hp StorageWorks

edge switch 2/24 product manager user guide

This guide provides an introduction and an overview of the StorageWorks Edge Switch 2/24 Product Manager. It also explains how to use the Product Manager to monitor, manage, and configure the switch.

hp invent

edge switch 2/24 product manager user guide
First Edition (January 2003)
Part Number: AA-RTDYA-TE

Contents

About This Guide

Product Manager Overview

Configuring the Switch

Using Logs

Using Maintenance Features

Optional Features

Product Manager Messages

Glossary

Index

Figures

Tables

About This Guide

This installation guide provides information to help you:

- Set up the Edge Switch 2/24.

- Configure the Edge Switch 2/24.

- Manage the Edge Switch 2/24.

- Contact technical support for additional assistance.

Intended Audience

This book is intended for use by administrators who are experienced with the following:

- Fibre Channel technology

- StorageWorks Fibre Channel Switches by Hewlett-Packard

Related Documentation

For a list of corresponding documentation included with this product, see the Related Documents section of the HP StorageWorks Edge Switch Release Notes.

For the latest information, documentation, and firmware releases, please visit the HP StorageWorks website:

http://h18006.www1.hp.com/storage/saninfrastructure.html

For information about Fibre Channel standards, visit the Fibre Channel Industry Association website, located at http://www.fibrechannel.org.

Document Conventions

The conventions included in Table 1 apply.

Table 1: Document Conventions

Element	Convention
Cross-reference links	Blue text: Figure 1
Key names, menu items, buttons, and dialog box titles	**Bold**
File names, application names, and text emphasis	*Italics*
User input, command names, system responses (output and messages)	`Monospace font` `COMMAND NAMES` are uppercase unless they are case-sensitive
Variables	`Monospace, italic font`
Website addresses	Sans serif font (http://thenew.hp.com)

Symbols in Text

These symbols may be found in the text of this guide. They have the following meanings.

> ⚠ **WARNING: Text set off in this manner indicates that failure to follow directions in the warning could result in bodily harm or loss of life.**

> △ **CAUTION:** Text set off in this manner indicates that failure to follow directions could result in damage to equipment or loss of information.

IMPORTANT: Text set off in this manner presents clarifying information or specific instructions.

NOTE: Text set off in this manner presents commentary, sidelights, or interesting points of information.

Symbols on Equipment

These icons may be located on equipment in areas where hazardous conditions may exist.

Any surface or area of the equipment marked with these symbols indicates the presence of electrical shock hazards. Enclosed area contains no operator serviceable parts.

WARNING: To reduce the risk of injury from electrical shock hazards, do not open this enclosure.

Any RJ-45 receptacle marked with these symbols indicates a Network Interface Connection.

WARNING: To reduce the risk of electrical shock, fire, or damage to the equipment, do not plug telephone or telecommunications connectors into this receptacle.

Any surface or area of the equipment marked with these symbols indicates the presence of a hot surface or hot component. If this surface is contacted, the potential for injury exists.

WARNING: To reduce the risk of injury from a hot component, allow the surface to cool before touching.

Power Supplies or Systems marked with these symbols indicate the equipment is supplied by multiple sources of power.

WARNING: To reduce the risk of injury from electrical shock, remove all power cords to completely disconnect power from the system.

Any product or assembly marked with these symbols indicates that the component exceeds the recommended weight for one individual to handle safely.

WARNING: To reduce the risk of personal INJURY or damage to the equipment, observe local occupational health and safety requirements and guidelines for manual material handling.

Rack Stability

⚠ **WARNING: To reduce the risk of personal injury or damage to the equipment, be sure that:**
- The leveling jacks are extended to the floor.
- The full weight of the rack rests on the leveling jacks.
- The stabilizing feet are attached to the rack if it is a single rack installations.
- The racks are coupled together in multiple rack installations.
- A rack may become unstable if more than one component is extended for any reason. Extend only one component at a time.

Getting Help

If you still have a question after reading this guide, contact an HP authorized service provider or access our website: http://thenew.hp.com.

HP Technical Support

In North America, call technical support at 1-800-652-6672, available 24 hours a day, 7 days a week.

NOTE: For continuous quality improvement, calls may be recorded or monitored.

Outside North America, call technical support at the nearest location. Telephone numbers for worldwide technical support are listed on the HP website under support: http://thenew.hp.com/country/us/eng/support.html.

Be sure to have the following information available before calling:

- Technical support registration number (if applicable)

- Product serial numbers

- Product model names and numbers

- Applicable error messages

- Operating system type and revision level

- Detailed, specific questions

HP Website

The HP website has the latest information on this product, as well as the latest drivers. Access storage at: http://thenew.hp.com/country/us/eng/prodserv/storage.html. From this website, select the appropriate product or solution.

HP Authorized Reseller

For the name of your nearest HP Authorized Reseller:

*   In the United States, call 1-800-345-1518

*   In Canada, call 1-800-263-5868

*   Elsewhere, see the HP website for locations and telephone numbers:
    http://thenew.hp.com.

1

Product Manager Overview

This chapter is an introduction and overview of the Edge Switch 2/24 Product Manager application. It is intended as a quick reference for using features available through the main Product Manager window.

Managing the Edge Switch 2/24

These options are available for managing the Edge Switch 2/24 through a user interface:

- The Product Manager application installed on an high-availability fabric manager (HAFM) server. Access to the Product Manager must be through the HAFM applications. These applications are installed on the HAFM server.

- The Embedded Web Server (EWS) interface. Using a browser-capable PC with an internet connection to the switch, you can monitor and manage the switch through the web server interface embedded in the switch firmware. The interface provides a Graphical User Interface (GUI) similar to the Product Manager application and supports switch configuration, statistics monitoring, and basic operation.

  To launch the Embedded Web Server interface, enter the switch's IP address as the internet uniform resource locator (URL) into any standard browser. Enter a user name and password at a the login screen. The browser then becomes a management console. Refer to the web server interface online help for details on use.

  NOTE: The default user name for the right to view status and other information is "operator." The default user name for the right to modify configuration data, perform maintenance tasks, or perform other options is "administrator." The default password for both user names is "password."

- The command line interface (CLI). The CLI allows you to access many HAFM and Product Manager functions while entering commands during a Telnet session with the switch. The primary purpose of the CLI is to automate management of a large number of switches using scripts. The CLI is not an interactive interface; no

checking is done for pre-existing conditions and no prompts display to guide users through tasks. Refer to the *hp StorageWorks CLI reference guide for director and edge switches*.

- Management using simple network management protocol (SNMP). An SNMP agent is implemented through the SDCM application that allows administrators on SNMP management workstations to access switch management information using any standard network management tool. Administrators can assign internet protocol (IP) addresses and corresponding community names for up to six SNMP workstations functioning as SNMP trap message recipients.

This manual provides details on the Product Manager application for the Edge Switch 2/24 only. Use this manual for the Product Manager installed on an HAFM server. This manual does not cover the Embedded Web Server interface or CLI.

Menu Options

This user guide provides information on the Edge Switch 2/24 Product Manager application only. Information on the HAFM application is provided in the *hp StorageWorks ha-fabric manager user guide*. Following are lists of options available from the menu bar in both applications. References are provided to the correct publication for detailed information on these options.

High-Availability Fabric Manager (HAFM)

Following are options available through the HAFM. For more information, refer to Chapter 3 of the *hp StorageWorks ha-fabric manager user guide*.

View Tabs

- Products
- Fabrics

Product Menu

- New
- Open
- Delete
- Modify
- Properties

- Logout
- Exit

Fabrics Menu

- Rename
- Persist Fabric Topology
- Unpersist Fabric Topology
- Export Fabric Topology
- Show Route
- Hide Route
- Show Zone Members
- Show View Port
- Show Fabric Tree
- Enterprise Fabrics Mode (active if SANtegrity features installed)
- Fabric Binding (active if SANtegrity features installed)

View Menu

- User Sessions
- Zoom
  - In
  - Out
  - Default
  - Fit in View
- Layout Icons
- Circular
- Spring
- Center in Topology
- Clear ISL Alert

- Clear All ISL Alerts
- Enable Fly Over Display

Configure Menu

- Users
- Nicknames
- Sessions
- Operating Parameters (Switch and Fabric)
- SNMP Agent
- Activate Zone Set
- Zoning Library
- Advanced Zoning

Logs Menu

- Audit Log
- Event Log
- Session Log
- Product Status Log
- Fabric Log

Maintenance Menu

- Configure E-Mail
- Test Remote Notification
- Configure Ethernet Events
- Configure Call Home Event Notification

Help

- Contents
- About

Product Manager

Following are options available through the Product Manager application for your switch. For more information on these options, refer to Menu Bar on page 1-14 in this manual.

View Tabs

- Hardware
- Node List
- Port List
- Performance
- FRU List

Product Menu

- Port (options available when port is selected)
  — Port Properties
  — Node Properties
  — Port Technology
  — Block Port
  — Enable Beaconing
  — Port Diagnostics
  — Channel Wrap
  — Swap Ports
  — Clear Link Incident Alert(s)
  — Reset Port
  — Port Binding
  — Clear Threshold Alerts(s)
- FRU
  — FRU Properties based upon which FRU was selected
- Clear System Error Light

- Enable Unit Beaconing
- Properties
- Close

Configure Menu

- Identification
- Operating Mode
- Operating Parameters
  — Switch
  — Fabric
- Switch Binding (option only available if SANtegrity features installed)
  — Change State
  — Edit Membership
- Ports
- SNMP Agent
- Management Server
- Features
- Date/Time
- Threshold Alert
- Export Configuration Report
- Enable Web Server
- Enable Telnet

Logs Menu

- Audit Log
- Event Log
- Hardware Log
- Link Incident Log
- Threshold Alerts Log

Maintenance Menu

- Port Diagnostics
- Data Collection
- IPL
- Set Online State
- Firmware Library
- Enable E-Mail Notification
- Enable Call Home
- Backup and Restore Configuration
- Reset Configuration

Help Menu

- Contents
- About

Product Manager Description

The Product Manager for the Edge Switch 2/24 is a Java-based graphical user interface (GUI) that provides in-depth management, configuration, and monitoring functions for individual switches and their field-replaceable units (FRUs). Although the Product Manager is accessed from the HAFM application, it is a separate application.

In contrast to the Product Manager, the HAFM enables administrators to monitor operational status for all products and Fibre Channel fabrics managed by an HAFM server. The HAFM also provides tools to administer user and product access to the HAFM and Product Manager. Refer to the *hp StorageWorks ha-fabric manager user guide* for more information about the HAFM application.

The Product Manager provides graphical views of switch hardware components and displays of component status. By positioning the cursor on icons, graphics, panels, and other visual elements in these views and clicking the left or right mouse button, you can quickly manage and monitor the switch on your network.

Access the switch Product Manager by double-clicking any product icon on the HAFM's **Products** or the **Topology Fabrics** views.

Figure 1–1 on page 1-8 illustrates switch management components. The figure shows the following elements:

You can install the HAFM and Product Manager applications on remote workstations, as shown in Figure 1–1, using any standard web browser. For instructions, refer to the appendix in the *hp StorageWorks ha-fabric manager user guide* that pertains to the operating system of your workstation.
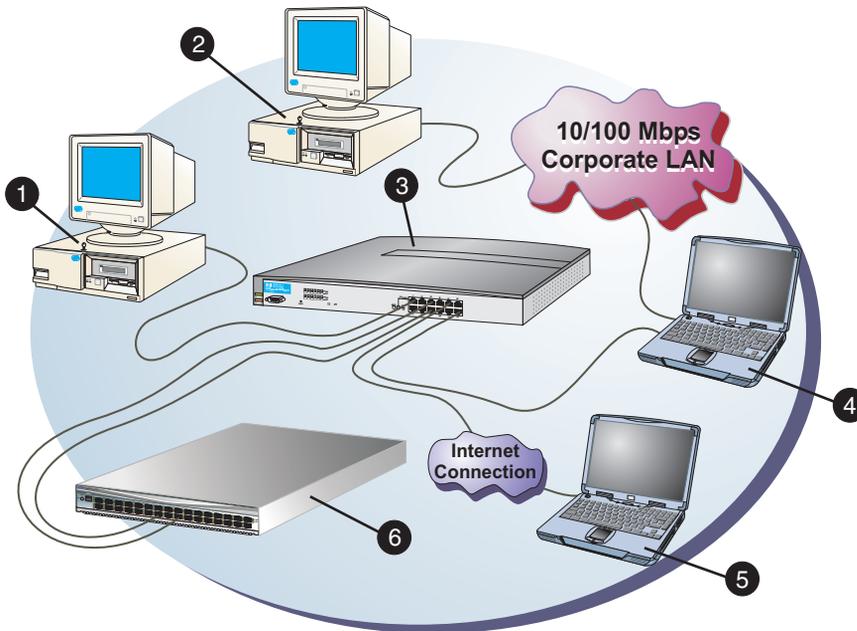
SHR-2314b

❶	SNMP management workstation	❹	HAFM server
❷	Remote user workstation	❺	Web browser
❸	HP Ethernet hub	❻	Switch

Figure 1–1: Switch management components on LAN

Using the Product Manager, you can:

• Back up and restore configuration data.

• Clear the system error indicator.

• Configure extended distance buffering for ports.

- Configure Fibre Channel operating parameters for the switch, such as BB_Credit, R_A_TOV, E_D_TOV, preferred domain ID, switch priority, and rerouting delay.

- Configure individual ports with a port name describing the node attached to the port.

- Configure keys for new features.

- Configure LIN alerts.

- Configure Port Binding.

- Configure Nickname to display instead of World Wide Name (WWN) for the switch and attached devices.

- Configure SNMP trap recipients and community names.

- Configure Open Systems Management Server Features (if installed).

- Configure the switch name, location, description, and contact person.

- Control individual Fibre Channel ports by blocking/unblocking operation, enabling link incident (LIN) alerts and WWN binding, setting data speeds, and running internal and external loopback diagnostics.

- Display FRU properties such as the FRU name, physical position in the switch (chassis slot number), active failed state, part number, and serial number.

- Display information for individual Fibre Channel ports, such as the port name, port number, Fibre Channel address, operational state, type of port, and login data.

- Display information on nodes attached to ports.

- Display port performance and statistics.

- Display vital product data for the switch, such as the system name, description, contact person, location, status, model number, firmware and EC level, and manufacturer.

- Enable beaconing for ports and the switch unit.

- Monitor the operational status of the switch and each of its hardware field-replaceable units.

- Perform an initial program load (IPL).

- Perform maintenance tasks for the switch including maintaining firmware levels, administering the call-home feature, accessing the switch logs, and collecting data to support failure analysis.

- Reset port operation.
- Run port diagnostics.
- Set the date and time on the switch.

Using the Product Manager

This section provides a general overview of the Product Manager and its functions. For details on performing specific tasks and using specific dialog boxes, refer to the appropriate chapters in this manual.

Using Dialog Boxes

Buttons such as **OK**, **Activate**, and **Close** or **Cancel** initiate functions in a dialog box. There is a difference between the **OK** and **Activate** buttons. The **OK** button saves the data you entered and closes the dialog box. The **Activate** button saves the data you entered without closing the dialog box, unless there is a **Close** button. In this case, **Activate** saves the information without closing the box. There is also a difference between the **Close** and **Cancel** buttons. The **Close** button closes the dialog box and saves the data you entered. The **Cancel** button cancels the operation and closes the dialog box without saving the information you entered.

Illustrations Used in this Manual

Figures containing HAFM and Product Manager screens in this manual are included for illustration purposes only. These illustrations may not match exactly what you see through your server or workstation. Title bars have been removed from the illustrations and fields in the illustrations may contain different data than in screens displayed on your system.

Keyboard Navigation

Use standard keyboard navigation in dialog boxes. For example, use the **Tab**, arrow, and backspace keys to move through dialog box fields and the **Enter** key to perform default button functions.

Log Into the HAFM

To open the Product Manager, you must first log into the HAFM.

1. Perform one of the following steps:

    — If you are using the HAFM server, the HAFM application automatically starts when you power on or reboot the HAFM server. If you reboot or switch on the HAFM server and the HAFM login screen displays, skip to step 3 to log in.

    — If you are using a remote user workstation, follow steps 2 through 5.

    — If the HAFM window displays already, skip to Opening the Product Manager on page 1-13.

2. Perform one of the following steps if you are using a remote user workstation (a network PC with a remote client installed), and the HAFM login screen or HAFM window is not displayed. If the login screen is displayed, go to step 3.

    — Start the HAFM and display the login screen by double-clicking the HAFM icon on the desktop.

Figure 1–2: HAFM Icon

    The HAFM login screen appears

    — If the HAFM window is open (Figure 1–3 on page 1-12) and you need to log in as another user or access a different HAFM server, select **Logout** from the Product menu on the menu bar to display the login screen. Go to step 3.

3. When the HAFM login screen displays, enter your user name and password. The default user name is *Administrator* and password is *password* unless changed by your system administrator.

NOTE: The default user name for the right to view status and other information is "operator." The default user name for the right to modify configuration data, perform maintenance tasks, or perform other options is "administrator." The default password for both user names is "password."

4. In the **HAFM Server** field on the login screen, select the HAFM server where which you want to connect. Note that if you are logging into an HAFM server locally, *localhost* is the HAFM server name. Type in the network address of the server if it is not in the list.

5. Click **Activate** or press the **Enter** key on your keyboard.

   The main HAFM window displays showing the **Product View**.
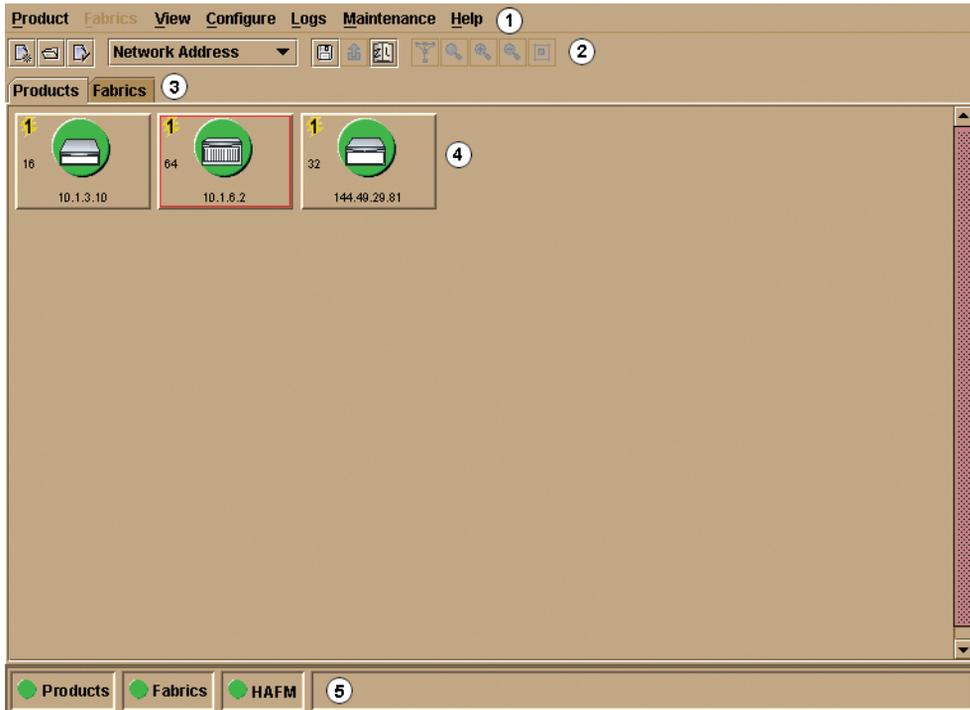
❶   Menu Bar   ❹   Main Panel
❷   Tool Bar   ❺   Status Panel
❸   View Tabs

Figure 1–3: Main HAFM window

Opening the Product Manager

To open the Product Manager, double-click the product icon in the **Product View** or right-click the icon and select **Open**.
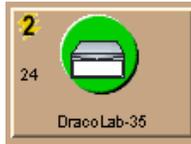
Figure 1–4: Edge Switch 2/24 icon

The Product Manager displays showing the default **Hardware View** (Figure 1–5).
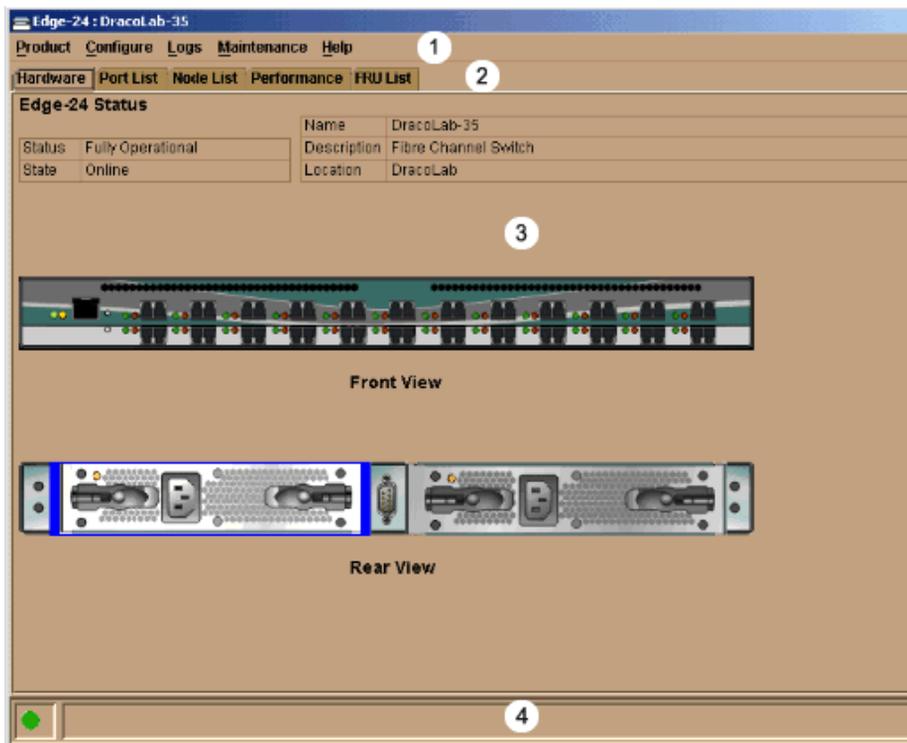
❶   Menu Bar   ❸   View Panel
❷   View Tabs   ❹   Status Bar

Figure 1–5: Edge Switch 2/24 Product Manager window (Hardware View)

NOTE: The HAFM window is still available as a separate window. You can drag the Product Manager window away from the HAFM window and view both windows on your PC desktop or minimize one or both of them to icons if desired. You can have a maximum of four Product Manager windows open concurrently.

Window Layout and Function

The main Product Manager window is divided into four main areas as shown in Figure 1–5 on page 1-13: menu bar, view tabs, view panel, and status bar. Use features in these panels to configure switch operation, monitor performance, and access maintenance features.

Menu Bar

The menu bar on the Product Manager window displays tabs for the following menus:

- Product
- Configure
- Logs
- Maintenance
- Help

Click one of the tabs to display a list of menu options. Click an option to open a dialog box that allows you to perform configuration and maintenance tasks and view logs. If a menu option contains a check box, click in the box to add a check mark and enable a function. Click a check box containing a check mark to remove the check mark and disable the function.

Product Menu

Select one of the following options from the **Product** menu.

Port

This provides a secondary port menu only when the **Hardware View**, **Port List View**, or **Performance View** displays in the view panel. To use this menu for a specific port, click a port in the **Hardware View**, a port's row in the **Port List View**, or a port's bar graph in the **Performance View**. The menu contains options which are identical to those that display when you right-click the port, port row, or port bar graph in those views. For detailed information on using these options, refer to Port Menu on page 2-16.

FRU

Click a power supply module or cooling fan module in the **Hardware View** only and select **FRU** from the **Product** menu to display the **FRU Properties** menu option. This displays the **FRU Properties** dialog box. The **FRU Properties** dialog box can also be displayed by double-clicking on the FRU in the **Hardware View**. These are the same menu option as when you double-click these components in the **Hardware View**. For details on these options refer to Displaying FRU Information on page 2-7.

Clear System Error Light

Select this to turn off the amber system error LED, located below the green power LED on the switch front bezel.

Enable Unit Beaconing

Click the check box to toggle unit beaconing on or off. When the check box has a check mark, unit beaconing is on, and the amber system error light on the switch front bezel blinks to help users locate the actual unit in an equipment room. When you click the check box to remove the check mark, unit beaconing is disabled and the amber LED goes out. You can only enable beaconing if there are no system errors (the system error light is off).

Properties

Click to display the **Switch Properties** dialog box. This dialog box contains the switch name, description, location, and contact person configured through the **Configure Identification** dialog box. Also included is other product information as detailed in switch Properties. You can also display this dialog box by double-clicking an area on the illustration in the **Hardware View**, away from a hardware component.

Close

Select this option to close the Product Manager window.

Configure Menu

Click on the **Configure** menu on the menu bar to display the following options. For detailed information on using these options, refer to Chapter 3, Configuring the Switch.

Identification

Select this option to display the **Configure Identification** dialog box. Enter the following information in this dialog box:

— **Name** - Assign a product name. Note that you can set this name as the nickname for the switch's WWN, using the **Set Name as Nickname** checkbox. The nickname then displays instead of the WWN in Product Manager views.

— **Description** - Assign a unique product description.

— **Location** - Describe the product's location.

— **Contact** - Assign a contact either by name, phone number, or e-mail address.

NOTE: This information displays in the identification table at the top of the *Hardware View* and in the HAFM *Product View,* if the *Product View* is configured to display names.

Switch Operating Parameters

Use this dialog box to set parameters on the switch for fabric operation. Set other fabric operating parameters, such as preferred domain ID (1 to 31) and Domain RSCNs. In addition, you can also enable the rerouting delay feature. Refer to Configure Switch Operating Parameters on page 3-3 for more information on configuring the switch priority and rerouting delay.

Fabric Operating Parameters

Use this dialog box to set parameters for fabric operation. In this dialog box, you can set the resource allocation time-out value (R_A_TOV) and error detect time-out value (E_D_TOV) in tenth-of-a-second increments, as well as other fabric operating parameters, such as switch priority level (Principal, Default, or Never Principal) and interop mode. You must take the switch offline through the **Set Online State** dialog box to configure these parameters. Refer to Configure Fabric Operating Parameters on page 3-6 for more information.

Switch Binding

This submenu provides two options if the SANtegrity feature is installed through the **Configure Feature Key** dialog box: **Change State** and **Edit Membership List**. Selecting **Change State** displays the **Switch Binding State Change** dialog box where you can activate Switch Binding according to a specific connection policy (Restrict E_Ports, Restrict F_Ports, or All Ports). **Edit Membership List** allows you to create a list of switches and devices that you want to allow exclusively to attach to switch ports. For details, refer to Configure Switch Binding on page 3-8.

Ports

Select this option to display the **Configure Ports** dialog box. For each port you can provide a name, block or unblock operation, configure extended distance buffering for 10 to 100km, enable LIN alerts for each port, enable Fabric Address Notification (FAN), define a type (G, F, E, Gx, and Fx), and enable port binding.

NOTE: Ports are automatically configured as Gx_Ports if no device is connected, F_Ports if a device is connected, E_Ports if a switch is connected and FL_Port if connected to a loop device.

SNMP Agent

Select this option to display the **Configure SNMP** dialog box. Use this dialog box to configure network addresses and community names for up to six SNMP trap recipients. Also authorize write permissions to enable SNMP management stations to modify writable MIB variables. In addition, you can enable authorization traps to be sent to management stations when unauthorized stations request access to switch SNMP data.

Features

Displays the **Configure Feature Key** dialog box. Use this dialog box to enter a feature key to enable optional features that you have purchased for the switch.

Date and Time

Select this option to display the **Configure Date and Time** dialog box. Use this option to set the current date and time in the switch. When the **Periodic Date/Time Synchronization** check box is checked, the **Date and Time** fields are greyed out (disabled), and the HAFM server date and time periodically synchronizes the switch date and time. If the **Periodic Date/Time Synchronization** check box is not checked, you can set the date and time in the dialog box fields manually.

Threshold Alert(s)

Select this option to configure threshold alerts for ports. A threshold alert notifies users when the transmit (Tx) or receive (Rx) throughput reaches specified values for specific switch ports or port types (E_Ports, F_Ports or FL_Ports). Using this option, you can configure:

- A name for the alert.

- A threshold type for the alert (Rx, Tx, or either).

- Active or inactive state of the alert.

- Threshold criteria. This criteria includes configuring the threshold as the percent of port traffic capacity utilized (% utilization). You must also configure the time interval during which the throughput is measured and the maximum cumulative time that the throughput percentage threshold can be exceeded during this time interval before an alert is generated.

Export Configuration Report

Select this option to display the **Export Configuration Report** dialog box, which enables you to specify a file name in which to save an ASCII text file containing all current user-definable configuration options in a printable format. Note that this file cannot be read back into the Product Manager in order to set configuration parameters.

Enable Web Server

To select this option, place a check mark in the check box to enable the Embedded Web Server interface on the switch. Select the option again to remove the check mark and disable the Embedded Web Server interface. When disabled, users at remote workstations cannot access the interface. If enabled, HP recommends changing the user names and/or passwords from their default values to prevent unauthorized access.

Enable Telnet

To select this option, place a check mark in the check box to enable telnet access to the switch. Select the option again to remove the check mark and disable telnet access. When disabled, users at remote workstations cannot access the switch through telnet to use the Command Line Interface (CLI) or perform other tasks. If enabled, HP recommends changing the user names and/or passwords from their default values to prevent unauthorized access.

Logs Menu

Click on the **Logs** menu from the menu bar to display the following options. For detailed information on using these dialog boxes, refer to Using Logs on page 4-1.

Audit Log

This log provides a record of all configuration changes made on the switch. Each entry displays the date and time of the change, a description of the change, the source of the change (such as the HAFM server or SNMP management station), and an identifier for the source, such as the IP address of the HAFM server or SNMP management station.

Event Log

Select this option to display the switch Event Log. This log provides a record of significant events that have occurred on the switch, such as hardware failures, degraded operation, and port problems. Each entry includes the date and time of the event, a reason code for the event, the severity level, a brief description, and up to 32 bytes of supplementary event data. Refer to the *hp StorageWorks edge switch 2/24 service manual* for more information.

Hardware Log

This log displays information on FRUs inserted and removed from the switch. Each log entry includes the name of the FRU inserted or removed, the slot position relative to identical FRUs installed, whether the FRU was inserted or removed, the FRU part number and serial number, and the date and time the FRU was inserted or removed.

Link Incident Log

The link incident (LIN) log displays the most recent incidents with their date and time, port number, and description of the incident. A link incident can be one of several conditions detected on a fiber optic link. For a list of events that may cause a link incident to be written to the log, refer to Link Incident Log on page 4-7.

Threshold Alert Log

This log provides notifications of threshold alerts. Besides the date and time that the alert occurred, it also displays information that was configured through the **Configure Threshold Alert(s)** option under the **Configure** menu. This includes the alert name, port for which the alert is configured. the type of alert (transmit throughput, receive throughput, or both), threshold utilization of traffic capacity, minutes the threshold was configured for, and the configured time interval for the threshold. For more details on this log, refer to Threshold Alert Log on page 4-8.

Maintenance Menu

Click on the **Maintenance** menu on the menu bar to display the following options. For detailed information on using these dialog boxes, refer to Chapter 5, Using Maintenance Features.

Port Diagnostics

This option displays the **Port Diagnostics** dialog box. Use this dialog box to run internal and external loopback tests on ports. Refer to the *hp StorageWorks edge switch 2/24 service manual* for instructions.

Data Collection

This option displays the **Save Data Collection** dialog box. Use this dialog box to collect maintenance data into a file. This file is used by support personnel to diagnose system problems. Refer to the *hp StorageWorks edge switch 2/24 service manual* for instructions.

IPL

Select this option to initiate an initial program load on the switch. A dialog box displays to allow you to confirm the IPL. Note that an IPL does not affect any configuration settings done through the Product Manager. Port operation is interrupted during the IPL.

Refer to Chapter 5, Execute an IPL for more information.

Set Online State

Select this option to display the **Set Online State** dialog box. Use this dialog box to change the online state of the switch to offline or online.

Firmware Library

Select this option to display the **Firmware Library** dialog box. This dialog box displays all firmware versions currently installed on the HAFM server that can be downloaded to Edge Switches. Use this dialog box to add a new firmware version to the HAFM server hard disk, modify the description displayed for an existing version, delete a version from the PC, or download (send) a version for operation on a switch. For additional information on using this option, refer to the *hp StorageWorks edge switch 2/24 service manual*.

Enable E-Mail Notification

The Simple Mail Transfer Protocol (SMTP) server and e-mail recipient addresses are configured in the HAFM application (not in the switch's Product Manager). E-mail notification is also initially enabled in the HAFM for all Edge Switches managed by the HAFM. Note, however, that the **E-Mail Notification** option on the Product Manager's **Maintenance** menu must be enabled (checked) for e-mail notification to occur for the specific switch.

The default setting for the **Enable E-Mail Notification** function is enabled (checked). To disable the function, select **Enable E-Mail Notification** from the **Maintenance** menu to clear the check box.

For additional information on using this option, refer to Enable E-Mail Notification on page 5-4.

Enable Call Home Notification

NOTE: The default setting for the *Enable Call Home Notification* function is disabled (unchecked).

Select **Enable Call Home Notification** from the **Maintenance** menu to enable the call-home function for the switch.

The parameters of the call-home feature are configured in Windows. Refer to the *hp StorageWorks HAFM server installation guide* for instructions.

Backup & Restore Configuration

Select this option to save the product configuration stored on the switch to the HAFM server hard disk or to restore the configuration data from the HAFM server. Only a single copy of the configuration is kept on the server.

This back up is primarily for single-CTP systems, where a back up is needed to restore the configuration data to a replacement CTP card. You cannot modify the location or the file name of the saved configuration.

For additional information on using this option, refer to Backing Up and Restoring Configuration Data on page 3-29.

NOTE: You can only restore the configuration to a switch with the same IP address.

Reset Configuration

Select this option to reset all switch configuration data back to the factory defaults. A confirmation dialog box displays with a warning upon selecting the option. For additional information on using this option, refer to Reset Configuration on page 5-7.

⚠️ **WARNING: This operation resets all configuration including any optional features that have been installed. You will need to re-enter your feature key to enable all optional features after resetting the configuration.**

Help Menu

Click on the **Help** menu on the menu bar to display the following options.

Contents

Select this option to display the **Help** window. The **Help** window contains **Contents**, **Index**, and **Glossary** buttons and hypertext- linked items to help you quickly navigate through information. Use the forward (**>**) and back (**<**) buttons to scroll forward and backward through the displayed help frames. Exit the help feature at any time by clicking the **Close** selection at the top of the **Help** window.

About

Select this option to display the version number for the Product Manager and copyright information.View Tabs

Click one of the view tabs across the top of the Product Manager window to display the following views in the **View** panel.

- Hardware

- Port List

- Node List

- Performance
- FRU List

View Panel

Views, selected from the view tabs, display under the tabs in the view panel.

Hardware View

The **Hardware View** is the default view that displays in the view panel when you open the switch Product Manager. To return to this view from another view, click the **Hardware View** tab. Refer to Figure 1–5 on page 1-13 for an example of this view.

In the **Hardware View**, colored indicators reflect the status of actual LEDs on the switch FRUs. The status bar displays a symbol to represent the most degraded status currently reported by any of the switch FRUs. For example, for a port failure, indicated by a blinking red and yellow diamond on a port, a yellow triangle displays on the status bar to indicate a degraded condition. However, if a blinking red and yellow diamond displays over both power supplies, the status bar displays a blinking red and yellow diamond, which indicates a failure requiring immediate attention. For an explanation of the different status symbols and the reasons they display in the **Hardware View** or **Port List View**, refer to the table under Monitoring Hardware Operation on page 2-4.

Switch Menu

Double-click the switch graphic away from a FRU to display the **Switch Properties** dialog box. Right-click a hardware graphic away from a FRU to display the following options:

- Switch Properties
- Enable Unit Beaconing
- Clear System Error Light
- IPL Switch
- Set Switch Date and Time
- Set Switch Online State

For details on menu options, refer to Switch Menu on page 2-13.

For details on navigating and monitoring via the **Hardware View**, refer to Hardware View on page 2-1.

Port Menu

Double-click a port to display the **Port Properties** dialog box. Right-click a port to display the following options:

- Port Properties
- Node Properties
- Port Technology
- Block Port
- Enable Beaconing
- Port Diagnostics
- Clear Link Incident Alert(s)
- Reset Port
- Port Binding
- Clear Threshold Alert(s)

Note that these same options are available when you click a port on the **Hardware View** and select the port secondary menu from the **Product** menu on the menu bar.

NOTE: For *Node Properties*, if a node is not logged in, a message box displays indicating that node information is not available.

For details on menu options, refer to Port Menu on page 2-16.

For details on navigating and monitoring via the **Hardware View**, refer to Hardware View on page 2-1.

Port List View

Select the **Port List** view tab. A table listing the port number, port name, block/unblock configuration, operating state, operating speed, port type, and alert condition displays in the view panel. Figure 1–6 shows an example of the **Port List View**.

Figure 1–6: Port List View

The **Port List View** displays information about all ports installed in the switch. All data is dynamic and updates automatically. Double-click any row in this view to display the **Port Properties** dialog box for the port.

Right-click a port row to display the same menu options that display when you right-click a port in the **Hardware View** or a port's bar graph in the **Performance View**. These include:

- Port Properties

- Node Properties

- Port Technology

- Block Port

- Enable Beaconing

- Port Diagnostics

- Clear Link Incident Alert(s)

- Reset Port

- Port Binding

- Clear Threshold Alert(s)

Note that these options are also available when you click a port row and select the **Port** secondary menu from the **Product** menu on the menu bar.

For details on these menu options, refer to Port Menu on page 2-16.

For details on navigating and monitoring via the **Port List View**, refer to Port List View on page 1-24.

Node List View

Select **Node List** from view tabs. Figure 1–7 on page 1-27 shows an example of the **Node List View**. This view displays a table with information about all node attachments or N_Ports that have logged into existing F_Ports on the switch. Only N_Ports display in the **Node List View** after nodes have logged in to the fabric. The columns that display in the table include: port number where the node is attached, node type, WWN of the attached node (device), and BB_Credit used by the attached node.

Double-click a port row to highlight it and display the **Node Properties** dialog box for that port.

Right-click a port row to display the following menu options:

- **Node Properties** - Displays the **Node Properties** dialog box.

- **Port Properties** - Displays the **Port Properties** dialog box.

- **Define Nickname** - Displays the **Define Nickname** dialog box, where you can define a nickname to display for the attached device instead of the device's 8-byte WWN.

- **Display options** - Allows you to display attached devices listed under the **Port WWN** column in the **Node List View** by the device's nickname configured through the **Define Nickname** menu option or the device's WWN.

Port #	Address	Node Type	Port WWN	Unit Type	BB_Credit
1	020513	N_Port	EMC-20:01:00:60:48:00:00:01	Reserved	4
2	020613	N_Port	Emulex-20:02:00:00:C9:00:00:01	Reserved	4
3	020713	N_Port	Emulex-20:03:00:00:C9:00:00:01	Reserved	4
5	020913	N_Port	Sun-20:05:08:00:20:00:00:01	Reserved	4
6	020A13	N_Port	EMC-20:06:00:60:48:00:00:01	Reserved	4
7	020B13	N_Port	JNI-20:07:00:E0:69:00:00:01	Reserved	4
9	020D13	N_Port	EMC-20:09:00:60:48:00:00:01	Reserved	4
10	020E13	N_Port	EMC-20:0A:00:60:48:00:00:01	Reserved	4
11	020F13	N_Port	Sun-20:0B:08:00:20:00:00:01	Reserved	4
13	021113	N_Port	Sun-20:0D:08:00:20:00:00:01	Reserved	4
14	021213	N_Port	Sun-20:0E:08:00:20:00:00:01	Reserved	4
15	021313	N_Port	JNI-20:0F:00:E0:69:00:00:01	Reserved	4
17	021513	N_Port	Sun-20:11:08:00:20:00:00:01	Reserved	4
18	021613	N_Port	EMC-20:12:00:60:48:00:00:01	Reserved	4
19	021713	N_Port	EMC-20:13:00:60:48:00:00:01	Reserved	4
21	021913	N_Port	Sun-20:15:08:00:20:00:00:01	Reserved	4
22	021A13	N_Port	Sun-20:16:08:00:20:00:00:01	Reserved	4
23	021B13	N_Port	Emulex-20:17:00:00:C9:00:00:01	Reserved	4
0	00000	NL_Port	Not Logged-In		

Figure 1–7: Node List View

Note that these options are also available when you click a port row, then select the **Port** secondary menu from the **Product** tab on the menu bar.

For details on navigating and monitoring via the **Node List View**, refer to Node List View on page 1-26.

Performance View

Select the **Performance** view tab. Figure 1–8 shows an example of the **Performance View**. This view provides a graphical display of performance for all 24 ports. The top portion of the **Performance View** displays bar graphs that show the level of transmit/receive activity for each port. This information updates every five seconds. Each bar graph also shows the percentage link utilization for the port. A red arrow marks the highest utilization level reached since the **Performance View** was opened. If the system detects activity on a port, it represents minimal activity with at least one bar.

When an end device (node) is logged into a port, moving the cursor over the port's bar graph in the **Performance View** highlights the graph and displays a message with the world-wide name of the connected node. If the connected node has more than one port, this is the world-wide name of the specific port on the node. When a port is functioning as an expansion port (E_Port), the message is E_Port. When a port is not logged into an end-device (not functioning as an F_Port) or to another switch (not functioning as an E_Port), the message is the port's current online state.
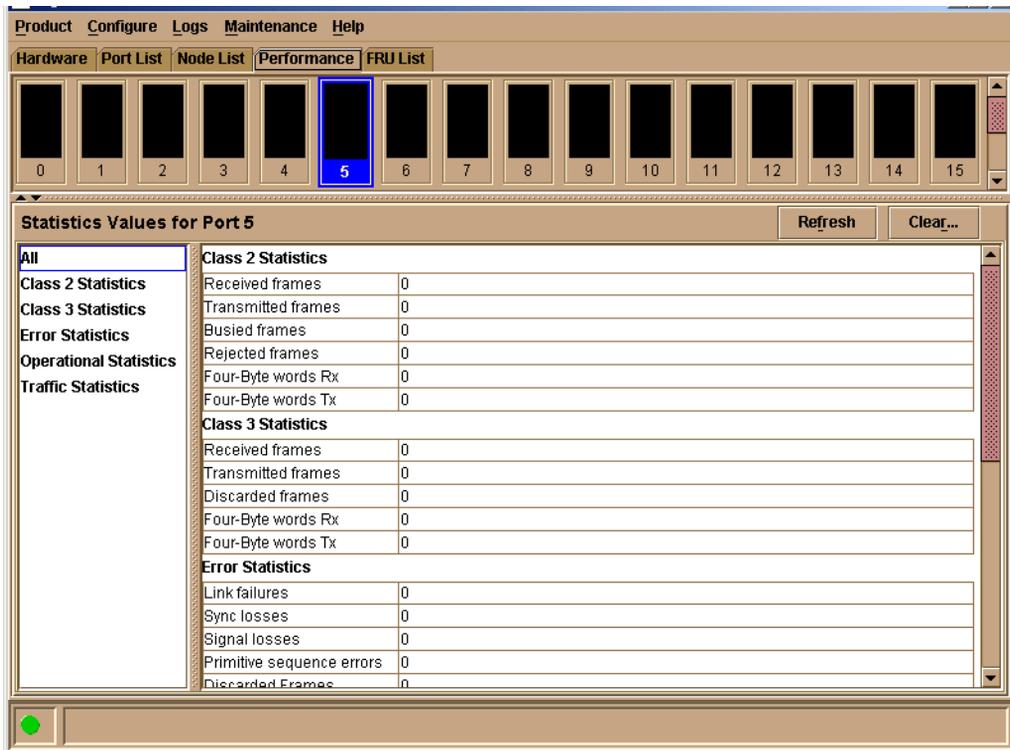
Figure 1–8: Performance View

Right-click a bar graph to display a menu of port-related actions. The options available
on this menu are the same as those that are available when you right-click a port in the
Hardware View or right-click a row in the **Port List View**. These include:

- Port Properties

- Node Properties

- Port Technology

- Block Port

- Enable Beaconing

- Port Diagnostics

- Clear Link Incident Alert(s)

- Reset Port

- Port Binding
- Clear Threshold Alert(s)

Note that these same options are also available when you click a port's graph, then select the **Port** secondary menu from the **Product** menu on the menu bar.

For details on menu options, refer to Port Menu on page 2-16.

The bottom portion of the **Performance View** displays cumulative statistical information for the port selected in the bar graph. Click the **Refresh** button to update the data with current data from the port.

Click the **Clear** button to clear all of the counters to zero for the selected port and to place an entry in the Audit Log indicating that statistics for the port have been cleared.

NOTE: Clearing the counters clears the statistics for all users.

For more information about the **Performance View**, including statistics descriptions, refer to Performance View on page 2-27.

FRU List View

Select the **FRU List** view tab. A table with information about each of the FRUs installed in the switch displays in the view panel. All data is dynamic and updates automatically. Figure 1–9 shows an example of the **FRU List View**.

Figure 1–9: FRU List View

For details on navigating and monitoring via the **FRU List View**, refer to Node List View on page 2-23.

Status Bar

The status bar is located along the bottom of the Product Manager window. This includes a symbol that displays at the left side of the bar and messages that display in the panel to the right of the symbol. The symbol indicates the current operating status of the switch and the messages display to provide more description of menu options as you move the cursor over the options under menu bar menus. Refer to Table 1–1 on page 1-30 for the meaning of these status symbols and of the corresponding alert text that displays in the Edge-24 **Status** table at the top of the **Hardware View** in the view panel.

If a gray square displays in the status bar (no Ethernet connection), a reason for the status displays in the **Status** table at the top of the **Hardware View**. Refer to No Link Status on page 2-2 for details.

Table 1–1: Operating Status - Status Bar and Switch Status

Symbol	Status Bar	Switch Status Table Text	Meaning
	Green Circle	Fully Operational	All components and installed ports are operational; no failures.
	Yellow Triangle	Redundant Failure	A redundant component has failed, such as a power supply, and the back up component has taken over operation.
		Minor Failure	A failure occurred which has decreased the switch's operational ability. Normal switching operations are not affected.
			One or more ports failed, but at least one port is still operational.
			A fan has failed or is not rotating sufficiently.

Table 1–1: Operating Status - Status Bar and Switch Status (Continued)

Symbol	Status Bar	Switch Status Table Text	Meaning
	Blinking Red and Yellow Diamond	NOT OPERATIONAL	A critical failure prevents the switch from performing fundamental switching operations. All fans failed. All installed ports failed. Both power supplies failed.
	Gray Square	Never Connected Link Timeout Protocol Mismatch Duplicate Session Unknown Network Address Incorrect Product Type	Switch status is unknown. This occurs if the Ethernet network connection between the HAFM server and the switch cannot be established or if the CTP fails. Refer to No Link Status on page 2-2 for details on the status table text.

Messages display to the right of the status symbol as you move the cursor over options under the menu bar menus. These messages provide additional details about tasks that you can perform through the menu option.

Closing the Product Manager

To close the Product Manager, use the following steps:

1. To close the Product Manager, do one of the following:

   — Select **Close** from the **Product** menu on the menu bar.

   — Click the X button at the top right corner of the Product Manager window.

   — Double-click the icon at the top left corner of the Product Manager window, or right-click the icon and select **Close** from the menu that displays.

2. Select **Logout** or **Exit** from the **Product** menu in the HAFM application.

— If you select **Logout**, the StorageWorks HA-Fabric Manager **Login** dialog box displays. You can now log in again using a user name and password. Log into a different HAFM server by selecting a different server from the **HAFM Server** field.

— If you select **Exit**, the **Product View** window closes.

User Rights

The HAFM's system administrator can assign levels of access, or "User Rights," to Product Manager users through the HAFM application.

NOTE: The HAFM's system administrator only has view rights while operating in a specific Product Manager application. Conversely, a Product Manager's product administrator only has view rights while operating in the HAFM application.

Detailed instructions concerning the assignment of user rights for both the HAFM and Product Manager applications appear in Chapter 3 of the *hp StorageWorks ha-fabric manager user guide*.

There are five levels of access or "user rights" that can be assigned to specific users:

• System Administrator

• Product Administrator

• Operator

• Maintenance

• View

By default, all users have view rights, which allow viewing configurations but not the changing configurations. View rights cannot be removed.

User(s) with system administrator rights can make all control and configuration changes implemented through the HAFM application.

User Rights for Specific Functions

Table 1–2 itemizes the specific functions available to Product Manager users that have been assigned "user rights" of product administrator, operator, or maintenance. If a user does not have the right to perform a specific operation, a not-authorized error box appears when the operation is attempted.

Table 1–2: User Rights for Product Manager Functions

Product Manager Rights	Product Administrator	Operator	Maintenance
Backup/Restore Configuration	X	X	X
Block Port	X	X	X
Change Online State	X		X
Clear Audit Log	X		
Clear Event Log			X
Clear Hardware Log	X		X
Clear LIN Alert	X	X	X
Clear LIN Log	X		
Clear System Error Light			X
Clear Threshold Alerts	X		
Configure Date/Time	X	X	X
Configure Feature Key	X		
Configure Identification	X		
Configure Management Server	X		
Configure Operating Mode	X		
Configure Operating Parameters	X		
Configure Port Binding	X	X	
Configure Ports	X	X	
Configure SNMP	X		
Configure Threshold Alerts	X		

Table 1–2: User Rights for Product Manager Functions (Continued)

Product Manager Rights	Product Administrator	Operator	Maintenance
Configure Zoning	X		
Data Collection			X
Date/Time Sync Configuration	X	X	X
Enable Call Home Notification	X		X
Enable E-Mail Notification	X		X
Enable Telnet	X		
Enable Web Server	X		
Export Configuration Report	X	X	X
IPL	X	X	X
Manage Firmware			X
Port Beaconing	X	X	X
Port Diagnostics			X
Reset Configuration			X
Reset Statistics Counters (Performance View)	X	X	
Reset Port	X		X
Set Online State	X	X	X
Unit Beaconing	X	X	X
View Event Log	X	X	X
View Firmware			X
View Hardware Log	X	X	X
View LIN Log	X	X	X
View SNMP	X		X

Backing Up and Restoring Product Manager Data

As long as a Zip® disk remains in the Zip drive of the HAFM server, critical information from both the Product Manager and HAFM applications automatically backs up to the Zip disk when the data directory contents change or when you reboot the HAFM server.

The application used for this function is Iomega® QuikSync, a separate application installed on the HAFM server. QuikSync is configured to automatically mirror the contents of the HafmData directory to the Zip drive when the contents are changed or when you reboot the HAFM server. This directory contains all HAFM and Product Manager data, so it can be copied back to a newly restored HAFM server to fully recover the preferred operating environment.

The mirroring operation will only occur while a user is logged in to Windows on the HAFM server PC (independent of the HAFM login).

The data contained in the HafmData directory and mirrored to the Zip disk includes the following:

- All HAFM configuration including:
    — Product definitions
    — User names, encrypted passwords, and user rights.
    — Nicknames
    — Session options
    — HAFM SNMP configurations
    — E-mail configuration
- All log files (both HAFM log files and individual Product Manager log files).
- Zoning library (all zone sets and zone definitions).
- Firmware library.
- Call-home configuration (including phone numbers and dialing options).
- Configuration data saved to the HafmData directory through the **Backup & Restore Configuration** option on the Product Manager **Maintenance** menu.

The QuikSync application will not back up certain Windows configurations that need to be reconfigured on a newly restored HAFM server, including the following:

- Windows user names and passwords.

- TCP/IP network configuration (such as IP address, gateway address, and DNS names).

The QuikSync application will be included on the HAFM Applications CD. It automatically installs on the HAFM server during the HAFM server install process. A blank Zip disk is required for each HAFM server and is included with the HAFM server deliverables.

Restoring Data to the HAFM server

To restore data to the HAFM server, copy the: HafmData directory from the zip disk to: C:\hafmdata on the C drive.

Using QuikSync

For information on using QuickSync, refer to the *hp StorageWorks ha-fabric manager user guide*.

2

Monitoring and Managing the Switch

This chapter describes how to use the features available in the Product Manager view panel to monitor and manage switch operation. These features include status indicators, menu options, and dialog boxes available through the **Hardware View**, **Port List View**, **Node List View**, **Performance View,** and **FRU List View**.

Hardware View

The **Hardware View** is the default view when you open the Product Manager. If another view displays, display the **Hardware View** by selecting **Hardware** from view tabs on the Product Manager window. Using this graphical view of the switch, you can view status symbols and simulated light emitting diode (LED) indicators, display data, and use mouse functions to monitor status and obtain vital product information for the switch and its hardware components.

Identifying FRUs

Move the cursor over parts of the switch graphic in the **Hardware View** to display labels identifying each hardware component and its slot position in the chassis relative to identical components installed in the switch. Components include:

- Power supply module. Note that each AC connector on the rear of the unit is the location of an internal power supply (two total).

- Ports (small form factor LC transceivers).

Monitoring Switch Operation

Monitor the operating status of the switch using the switch **Status** table on the **Hardware View** and the status indicator on the status bar at the bottom of the Product Manager window.

Switch Status Table

The **Status** table at the top of the **Hardware View** displays the switch's operational status, operational state, name, description, and location.

Status

Refer to Table 2–1 on page 2-35 for the meaning of the text that displays in the switch **Status** table and the corresponding status symbols that display on the status bar.

State

The **Status** field displays one of the following:

• OFFLINE

When the switch is "OFFLINE," all ports are offline. The ports cannot accept a login from an attached device or cannot connect to other switches. You can configure this state through the **Set Online State** dialog box. Refer to Set Online State on page 5–3 for instructions.

• Online

All unblocked ports are able to connect with devices. You can configure this state through the **Set Online State** dialog box. Refer to Set Online State on page 5–3 for instructions. Note that the switch automatically goes online after a power-up, an initial machine load (IML), or initial program load (IPL).

• Coming online

This is a transitional state that occurs just before the switch goes online. This state normally only happens briefly, unless there is a problem reaching the online state.

• Going offline

This is a transitional state that occurs just before the switch goes offline. This state normally only happens briefly, unless there is a problem reaching the offline state.

No Link Status

If the Ethernet network connection between the HAFM server and the switch is down, the **Hardware View** displays the front and rear of the unit without FRUs. The switch **Status** table at the top of the **Hardware View** changes to display the status (No Link) and reason with a yellow background. The name, description, and location fields are blank.

The **Reason** field on the switch **Status** table displays one of the following reasons when there are no links.

- Never Connected

  A network connection was never established between the switch and the HAFM server or if the CTP card has failed. Check the IP addresses, the Ethernet local area network (LAN) physical connection between the switch and HAFM server, and other network connection conditions.

  Note that the CTP card is not a FRU. If it fails, the switch must be replaced.

- Link Timeout

  The network connection that was established between the switch and HAFM server has been lost. Check the IP addresses, the Ethernet LAN physical connection between the switch and HAFM server, IP addresses, and other network components.

- Protocol Mismatch

  The switch and the HAFM server are not at compatible software release levels. Update the HAFM software version.

- Duplicate Session

  A link has previously been established between the switch and another instance of the HAFM server. Connect to the previously established HAFM server from the HAFM login screen.

- Unknown Network Address

  The address defined for the switch in the HAFM could not be found in the domain name server (DNS). Either the name was mistyped when the switch was added to the HAFM, or the name was not available from the DNS. Check the network IP address for the switch definition in the HAFM by right-clicking the product icon and selecting **Properties**. The IP address displays in the **Network Address** field.

- Incorrect Product Type

  The product at the configured network address is not a switch. Verify address, configuration, and product type.

Status Bar Status Indicator

The status bar displays a colored status symbol that indicates the overall operating status of the switch unit. The operating status depends on hardware component failures, which are indicated by status symbols that display over component graphics in the **Hardware View**. Refer to Hardware View on page 2–1 for the meanings of status symbols in the status bar.

The status bar indicates the switch operating status based on component failures. For example, for a single port failure, a blinking red and yellow diamond displays on the port connector in the **Hardware View**. At the same time, a yellow triangle displays in the status bar to indicate a degraded switch. However, if a blinking red and yellow diamond displays over both power supplies, the status bar displays a red and yellow diamond, indicating a failure that requires immediate attention.

Monitoring Hardware Operation

Determine hardware component operating status and states by the simulated light emitting diode (LED) indicators and status symbols, such as flashing red and yellow diamonds and yellow triangles, that appear on hardware components. These simulated LEDs and status symbols reflect the state of the actual hardware as changes occur. Corresponding or additional descriptions of hardware status and states also display when you double-click components to display **Properties** dialog boxes.

Figure 2–1 illustrates the Hardware View for the Edge Switch 2/24. The figure includes examples of symbols and LED indicators that display to help you monitor hardware operation. Numbers by each example are keyed to descriptions under Front View (following) and Rear View on page 2-7.
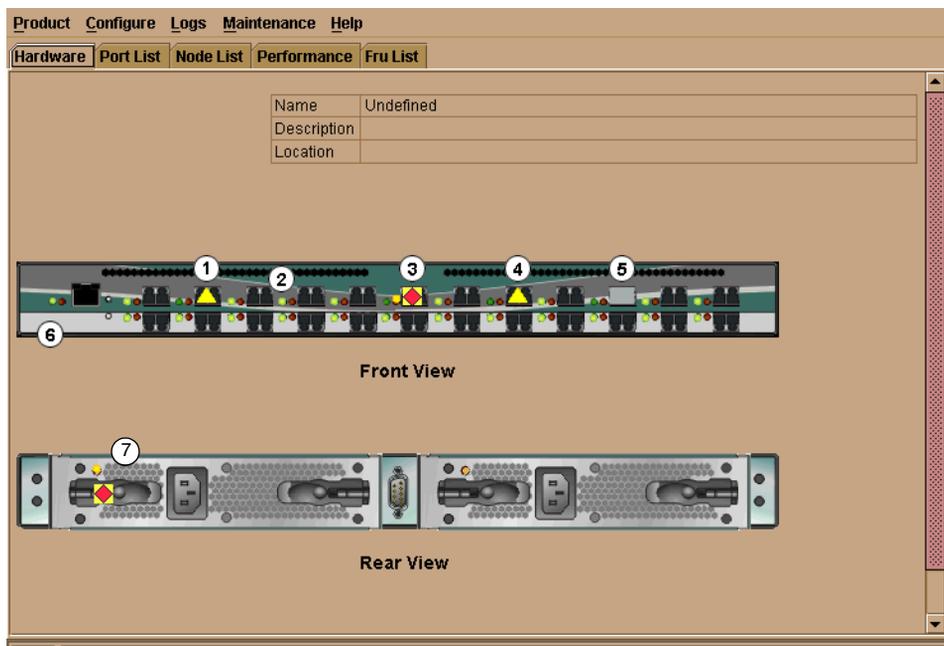
❶ Port Attention Indicator
❷ Port LED Indicator
❸ Port Failure Indicator
❹ Beaconing
❺ Not Installed
❻ Power, System Error, and Unit Beaconing Indicators
❼ Power Supply Status

Figure 2–1: Monitoring Hardware Operation - Edge Switch 2/24 Hardware View

Front View

1. Port Attention Indicator: The yellow triangle (⚠) indicates that a link incident occurred or that the port is not operational, in nonstandard mode of operation, or has other status. For a link incident, the status table at the top of the **Hardware View** changes to reflect the reason for the alert. You can also note the reason by displaying the **Port Properties** dialog box for the port. For details on status indicators, refer to Table 2–1 on page 2-35. For details on link incidents, refer to Link Incident Alerts on page 2–38.

2. Port LED Indicator: A green and amber indicator to the left of each port connector simulates LED operation on the actual switch port. When the green indicator illuminates, the port is online and operational. When the amber indicator remains illuminated, the port has failed. For details on port LED indicator operation, see Table 2–1 on page 2-35.

3. Port Failure Indicator: A blinking red and yellow diamond (🔴) below a port connector indicates that the port has failed. Refer to Table 2–1 on page 2-35 for details on port operating states and the status symbol and indicator operation.

4. Beaconing or Diagnostic Test: When a blinking amber LED indicator displays by a port and an attention indicator (🔶) displays below the port's connector, either diagnostic tests are running on the port or beaconing is enabled. Refer to Table 2–1 on page 2-35 for details on port operating states and the status symbol and indicator operation.

5. Not Installed. The port optics are not installed, or the feature that provides additional port function is not enabled.

6. Power, System Error, and Unit Beaconing Indicators: The green and amber indicators on the far right of the front view simulates the power and system error LEDs on the actual switch.

   • Power Indicator. The green indicator (**PWR**) simulates the power LED on the actual switch. When the indicator illuminates, the switch is connected to facility AC power and is operational. The indicator will be on if either power supply is operating.

   • System Error Indicator. The amber system error light indicator (**ERR**) simulates the system error light on the actual switch. When this indicator illuminates, an event has occurred requiring immediate attention, such as a system, fan, power supply, or port failure. View details of system errors by selecting **Event Log** from the **Logs** menu on the Product Manager menu bar. The indicator in the **Hardware View** and the LED on the actual unit remains illuminated until you clear the event by right-clicking on the front or rear view away from a hardware component and selecting **Clear System Error Light** from the menu.

   • Unit Beaconing Indicator. The amber indicator blinks if unit beaconing is enabled. Enable and disable unit beaconing by right-clicking on the front or rear view away from a hardware component and selecting **Enable Unit Beaconing** from the menu.

Rear View

7. Power Supply Status: Each AC power connector indicates the location of an internal power supply. An amber, service-required LED indicator is located in the upper left corner of each AC power connector. The indicator illuminates if the power supply has failed and requires service. The indicator is off if the power supply is active.

   When a blinking red and yellow diamond (◆) displays on a power connector, like in Figure 2–1 on page 2-5, the internal power supply for that connector failed. In this case, the green indicator to the top left of the connector will not illuminate. When the green indicator is on and no status symbol displays, the power supply is operational. Note that the switch operates with one power supply failure, however replace the power supply as soon as possible to retain redundancy.

Obtaining Hardware Information

This section explains how to access the **FRU Properties**, **Port Properties**, and **Switch Properties** dialog boxes.

Displaying FRU Information

Display the **FRU Properties** dialog box using one of the following methods:

- Double-click on a FRU, such as a power supply module illustrated in the **Hardware View**.

- Select a FRU in the **Hardware View**, then select **FRU** and **FRU Properties** from the **Product** menu.

- Double-click on a row in the **FRU List** view.

The **FRU Properties** dialog box displays FRU name; slot position relative to identical FRUs installed in the chassis and active or failed state.
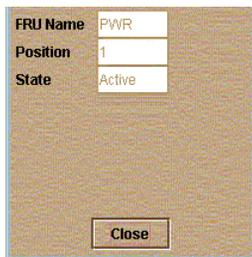
Figure 2–2: FRU Properties dialog box

Displaying Port Information

Double-click a port or right-click a port and select **Port Properties** from the menu to display the **Port Properties** dialog box. Also display this dialog box by:

- Double-clicking a row in the **Port List View** or right-clicking on a row and selecting **Port Properties** from the menu.

- Double-clicking a port's bar graph in the **Performance View** or right-clicking on the bar graph and selecting **Port Properties** from the menu.

- Right-clicking a port's row in the **Node List View** and selecting **Port Properties** from the menu

- Clicking a port, port row, or port bar graph in the preceding views and selecting the **Port** secondary menu from the **Product** menu on the menu bar.
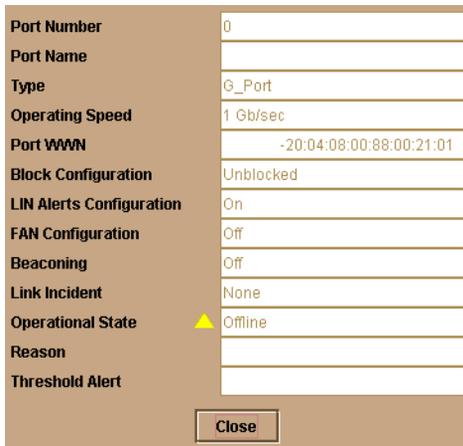
Port Number	0
Port Name	
Type	G_Port
Operating Speed	1 Gb/sec
Port WWN	-20:04:08:00:88:00:21:01
Block Configuration	Unblocked
LIN Alerts Configuration	On
FAN Configuration	Off
Beaconing	Off
Link Incident	None
Operational State ⚠	Offline
Reason	
Threshold Alert	

Close

Figure 2–3: Port Properties dialog box

The following paragraphs describe the fields in the **Port Properties** dialog box:

- Port Number

  The physical port number.

- Port Name

  User-defined port name or description. Refer to Configure Ports on page 3–9 for instructions.

- Type

  — Gx_port or G_port. This displays if nothing is logged into the port.

  — F_Port. This displays if a device is logged into the port.

  — E_Port. This displays if the port is connected to another switch's E_Port via an ISL.

  — FL_Port. This displays if a private loop device is logged into the port.

- Operating Speed

  This field displays the current data speed for the port as 1 Gb/sec, 2 Gb/sec, or Not Established. "Not Established" displays if **Negotiate** was set for the port through the **Configure Ports** dialog box and the data speed has not been resolved between the port and the attached device, or if the port and device are not communicating.

- Port WWN

  The port's 16-digit world wide name (WWN).

- Attached Port WWN

  The WWN of the node logged into the port.

- Block Configuration

  Blocked or unblocked. Operation can be blocked or unblocked through the **Configure Ports** dialog box. Refer to Configure Ports on page 3–9 for instructions.

- LIN Alerts Configuration

  This field indicates whether LIN alerts are enabled or disabled. LIN alerts can be configured through the **Configure Ports** dialog box. The default is for the LIN alerts to be enabled.

- FAN Configuration

  Indicates whether Fabric Address Notification (FAN) is On or Off when the port is operating as an FL_Port.

- Beaconing

  This field indicates the beaconing status for the port. To enable or disable beaconing, right-click the port and select **Enable Beaconing**.

- Link Incident

  Description of the last link incident that occurred on the port.

- Operational State

  Beaconing, inactive, invalid attachment, link incident, link reset, no light, not operational, online, offline, port failure, segmented E_Port, testing, or not installed. Refer to Table 2–1 on page 2-35 for definitions of operational states.

- Reason

  When the port operating state is "Segmented E_Port," "Invalid Attachment," or "Inactive," this field displays the reason for that state. When an E_Port is segmented, two fabrics are prevented from joining. This only occurs when the switch is connected to another switch. Reasons and probable causes are listed under Reason Field Messages below.

- Threshold Alert

  If a threshold alert exists for the port, an alert indicator (yellow triangle) will appear by the **Threshold Alert** field, and the configured name for the last alert received will appear in the field.

Reason Field Messages

The following messages display in the **Reason** field of the **Port Properties** dialog box if an Invalid Attachment, Segmented E_Port, or Inactive state occurs for the port.

Invalid Attachment Messages:

- `01 Unknown.` Invalid attachment reason cannot be determined.

- `02 ISL connection not allowed on this port.` Port is configured as an F_Port, but connected to Edge Switch or Director.

- `03 ELP rejected by the attached switch.` This Director/Edge Switch transmitted an exchange link protocol (ELP) frame that was rejected by the switch at the other end of the ISL.

- `04 Incompatible switch at the other end of the ISL.` Interop mode for this switch is set to Open Fabric mode and the switch at the other end of the ISL is a HP switch configured for Homogeneous Fabric mode.

- `05 External loopback adapter connected to the port.` A loopback plug is connected to the port and there is no diagnostic test running.

- `06 N_Port connection not allowed on this port.` The port type configuration does not match the actual port use. Port is configured as an E_Port, but attaches to a node device.

- `07 Non-HP switch at other end of the ISL`. The cable is connected to a non-HP switch and interop mode is set to Homogeneous fabric mode.

- `08 ISL connection not allowed on this port`. The port type configuration does not match the actual port use (the port is configured as an F_Port, but attaches to a Edge Switch or Director).

- `10 Port binding violation - unauthorized WWN`. The WWN entered to configure port binding is not valid or a nickname was used that is not configured through the Product Manager for the attached device.

- `11 Unresponsive node connected to port`. Possible causes are:

  — Hardware problem on switch or on a connected node where ELP frames are not delivered, the response is not received, or a fabric login in (FLOGI) cannot be received. There may be problems in switch SBAR.

  — Faulty or dirty cable connection.

  — Faulty host bus adapters that do not send out FLOGI within reasonable timeframe.

Segmented E_Port Messages:

- Incompatible operating parameters, such as resource allocation time-out values (R_A_TOV) or error-detect time-out values (E_D_TOV) are inconsistent. Refer to Configure Fabric Operating Parameters on page 3–6 for more information.

- Duplicate domain IDs. Refer to Configure Fabric Operating Parameters on page 3–6 for more information.

- Incompatible zoning configurations. Refer to sections on joining zoned fabrics in the *hp StorageWorks edge switch 2/24 service manual* and the *hp StorageWorks ha-fabric manager user guide* for details.

- Build fabric protocol error.

- No principal switch (no switch in fabric is capable of being principal switch).

- No response from an attached switch.

Displaying Switch Information

Double-click the switch illustration, away from a hardware component, to display the **Switch Properties** dialog box as shown in the following figure.
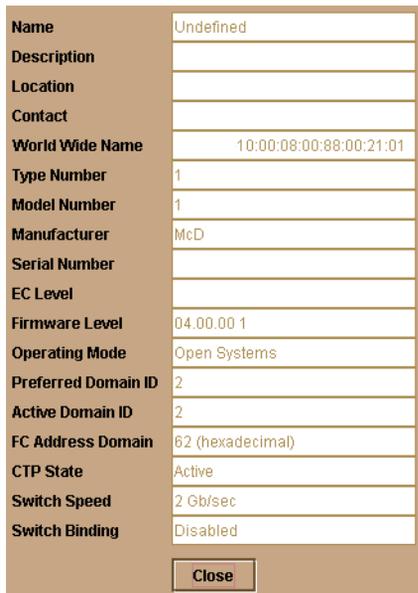
Name	Undefined
Description	
Location	
Contact	
World Wide Name	10:00:08:00:88:00:21:01
Type Number	1
Model Number	1
Manufacturer	McD
Serial Number	
EC Level	
Firmware Level	04.00.00 1
Operating Mode	Open Systems
Preferred Domain ID	2
Active Domain ID	2
FC Address Domain	62 (hexadecimal)
CTP State	Active
Switch Speed	2 Gb/sec
Switch Binding	Disabled

Close

Figure 2–4: Switch Properties dialog box

The following displays in this dialog box:

- Switch name, description, location, and contact (configured using the **Configure Identification** dialog box)

- Fibre Channel world wide name (WWN) identifier for the switch

- Product type number

- Product model number

- Product manufacturer

- Product serial number

- Engineering change (EC) level

- Firmware level

- Operating Mode (configured using the **Configure Operating Mode** dialog box)

- Preferred Domain ID (configured using the **Configure Switch Operating Parameters** dialog box)

- Active Domain ID (actual domain ID assigned to the switch)

- Fibre Channel Address Domain

- CTP State

- Switch Speed (always 2 Gb/sec)

- Switch Binding (enabled if the optional SANtegrity features are installed and enabled. Otherwise, disabled displays)

Using Menu Options

Right-click on various parts of the **Hardware View** to display menu options for displaying status and information and for controlling the switch and various hardware components.

Switch Menu

Right-click on any area of the switch illustration where a FRU hardware component is not installed to display the following menu options.

Switch Properties

Click to display the **Switch Properties** dialog box. This dialog box contains the switch name, description, location, and contact person configured through the **Configure Identification** dialog box. Also included is other product information as detailed in Displaying Switch Information on page 2-12. You can also display this dialog box by double-clicking an area on the illustration away from a hardware component.

Enable Unit Beaconing

Click the check box to toggle unit beaconing on or off. When the check box has a check mark, unit beaconing is on, and the system error light (**ERR**) on the switch blinks to help users locate the unit managed by the Product Manager. The amber indicator on the **Hardware View** also blinks when beaconing is enabled. When you click the check box to remove the check mark, the unit beaconing is disabled.

NOTE: You can only enable beaconing if there are no system errors (the system error light is off).

Clear System Error Light

Select this to turn off the amber system error light (**ERR**), located below the green power (**PWR**) LED on the switch. This also turns off the amber system error light indicator in the **Hardware View** (front view)

IPL Switch

Select this option to initiate an IPL on the switch. When the dialog box displays confirming the IPL, click **Yes**.

NOTE: An IPL is not intended for ordinary or casual use and should only be performed when directed by your support personnel.

Refer to Execute an IPL on page 5–1 for detailed procedures.

Set Switch Date and Time

Select this option to display the **Configure Date and Time** dialog box.

1. Click to display the **Configure Date and Time** dialog box.

   The dialog box displays with a check mark (the default) in the **Periodic Date/Time Synchronization** check box. If this field is checked, the HAFM server periodically sets the switch time to automatically synchronize with the HAFM server time. Daylight savings time automatically updates on the switch using this option.

   The current date and time display in the **Date** and **Time** fields. If the **Periodic Date/Time Synchronization** field is checked, the **Date** and **Time** fields are disabled (grayed out).

   To enable and disable **Periodic Date/Time Synchronization**, select the check box and then click **Activate**.
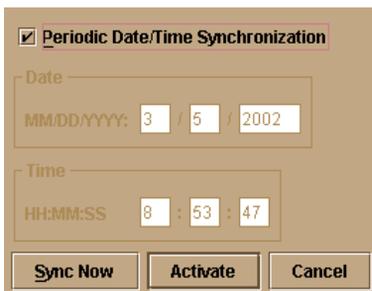
Figure 2–5: Configure Date and Time Periodic Synchronization dialog box

2. Perform one of the following steps:

— To immediately synchronize the switch date and time with the HAFM server, be sure the **Periodic Date/Time Synchronization** option is enabled and then click **Sync Now**.

NOTE: If you enable the *Periodic Date/Time Synchronization* feature and click *Activate*, the time will synchronize at the next update period.

— To set the switch with a specific date and time, make sure that the **Periodic Date/Time Synchronization** field is not selected. Refer to Figure 2–6. Enter the date and time and then click **Activate**.

Figure 2–6: Configure date and time manually

NOTE: Use the range of 0 to 23 for hours. Use the range of 0 to 59 for minutes and seconds.

Set Switch Online State

Click to display the **Set Online State** dialog box. The dialog box displays the current state (offline or online) and provides a button for changing the state.

⚠ **CAUTION:** Before setting the switch offline, warn administrators and users currently operating attached devices that the switch is going offline and that there will be a disruption of port operation. Also, request that the devices affected by an interruption of data flow be set offline.

1. Click the **Set Offline** or **Set Online** button to toggle between the states.

Figure 2–7: Set Online State dialog box (Offline)

Current state is ONLINE

| Set Offline | Cancel |

Figure 2–8: Set Online State dialog box (Online)

2. When the **Set Online** or **Set Offline** warning dialog box displays, click **OK** to set the switch online or offline.

    As the switch goes offline, the word, "OFFLINE," displays in the **State** field in the left corner of the **Hardware View**. As the switch goes online, the word, "ONLINE," displays in the **State** field in the left corner of the **Hardware View**. When going offline, LED indicators on all ports with attached devices stay green, but the switch sends offline sequences (OLS) to these devices.

Port Menu

While in the **Hardware View**, right-click on any port to display the following menu options.

Port Properties

Click this to display the **Port Properties** dialog box. This dialog box displays technical information about the port. See Displaying Port Information on page 2-8 for more information.

Node Properties

Click this to display the **Node Properties** dialog box. Note that if a node is not logged into the port, a message appears indicating that node information is not available. For details on information that displays in this dialog box, refer to Displaying Node Properties on page 2–25.

Port Technology

Click this to display the **Port Technology** dialog box. This dialog box displays the following information:

•   Port number.

•   Connector type: Always LC.

•   Transceiver type: Longwave laser LC or shortwave laser LC.

- Distance: General distance range for port transmission. This can be either short to long distances for the longwave laser LC transceiver or short distances for the shortwave laser LC transceivers.

- Media: The Fibre Channel mode and optic size. For the longwave laser LC transceiver, this would be singlemode 9-micron. For the shortwave laser LC transceiver, this would be multimode 50-micron or 62.5-micron.

- Speed: This will be either 1 Gbit per second or 1 Gbit, 2 Gbit per second.

Block Port

Click to display a check mark and block port transmission If blocked, a node attached to the port is prevented from logging into the switch or communicating with other devices attached to switch ports. A blocked port continuously transmits offline signals (OLS). Click to remove the check mark and unblock the port. If unblocked, a node attached to the port can communicate with the switch and communicate with other nodes attached to the switch.

Enable Beaconing

Click this to make the amber LED by the port blink on the actual switch and the amber indicator blink for the port in the **Hardware View**. This enables users to locate the unit where the port is located. When a blinking amber LED indicator displays by a port, an attention indicator ( ) displays below the port's connector in the **Hardware View** and in the port's row in the **Port List View**.

Port Diagnostics

Click this option to display the **Port Diagnostics** dialog box. Use this dialog box to run an internal loopback and external loopback test on the port. The **Port Diagnostics** option enables you to run internal and external loopback tests on any port. To use this option, follow the detailed steps in the *hp StorageWorks edge switch 2/24 service manual*.

Clear Link Incident Alert(s)

Click this to clear the attention indicator on the **Hardware View**, the **Port List View**, and the **Performance View**. In addition, the procedure clears the alert description in **Port Properties** dialog boxes. If there are no link incident alerts set for a port, no actions occur. Although you can manually clear link incidents, they may also be cleared by actions outside of the user interface, such as when rebooting the HAFM server.

Reset Port

Click to display a confirmation dialog box. Click **Yes** on that dialog box to reset the port. If a switch is attached to the port and online, this operation sends a link reset to the attached switch, otherwise this action disables port beaconing for the port. If the port is in a failed state, such as after failing a loopback test, the reset restores the port to an operational state, clearing the service required (amber) LED. The reset does not affect other ports in the switch.

Port Binding

Click to display the **Port Binding** dialog box (Figure 2–9). Use this dialog box to allow a device with a specific WWN or nickname to have exclusive connection to a port. To use this dialog box, refer to the following paragraphs.

Figure 2–9: Bind WWN dialog box

Port Binding dialog box parameters:

- **Port Binding**: Click this check box to place check mark in the box and enable WWN binding for the port. When enabled, only a specific device can community through the port. This device is specified by the WWN or nickname entered into the **Bound WWN** area (either the **Attached WWN** or **WWN** fields). With the check box cleared, any device can communicate through the port even if a WWN or nickname is specified in the **Bound WWN** field.

- **Attached WWN**: Click the radio button and, if a device is logged into the port, the device's WWN will display in the field. The device with this WWN or nickname will have exclusive communication privileges through the port if **Port Binding** is enabled.

NOTE: If you click this radio button to bind the port to a logged-in device and there are no devices logged in, the port is essentially bound to a WWN of "0." This prevents any device from logging in until this button is re-enabled to bind the WWN of a logged-in device or until you explicitly bind the WWN of a device by clicking the Detached WWN radio button and entering a WWN or nickname (see the following). Changes only take effect when you click the *Activate* button.

- **Detached WWN**: Click the radio button and enter a world wide name (WWN) in the proper format (xx.xx.xx.xx.xx.xx.xx.xx) or a nickname configured through the Product or HAFM applications. The device with this WWN or nickname will have exclusive communication privileges through the port if **Port Binding** is enabled.

  Note the following:

  — If you do not enter valid WWN or nickname in this field, but the **Port Binding** check box is checked (enabled), then no devices can communicate through the port.

  — If you enter a WWN or nickname in this field and do not place a check in the **Port Binding** check box, the WWN or nickname will be stored, and all devices can communicate through the port.

- **Activate**: Click this button to activate settings in this dialog box.

Warning and error message display:

- If one or more of the nodes logged into the port does not match the WWN or nickname configured in the field by the **WWN** radio button, a warning dialog box displays after you activate the configuration. This warning box displays a list of all nodes that will be logged off if you continue. If you click **Continue** on the warning box, these nodes will be logged off and the port can only communicate with the device with the WWN or nickname configured in the **WWN** field.

- An error message displays after you activate the configuration if the format for the WWN entered in the **WWN** field is not valid (not in xx.xx.xx.xx.xx.xx.xx.xx format) or if you have entered a nickname that was not configured through the Product Manager.

Clear Threshold Alert(s)

Click this to display the **Clear Threshold Alert(s)** dialog box. Select the appropriate option to clear alerts for the selected port only or all ports on the switch. This clears all attention indicators that notify users of threshold alerts in dialog boxes and views. This action also restarts the notification interval and the cumulative minutes for utilization % interval.
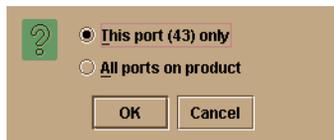
Figure 2–10: Clear Threshold Alert(s) dialog box

Port List View

Display the **Port List View** (Figure 2–11) in the view panel by selecting **Port List** from view tabs on the Product Manager window.

Product	Configure	Logs	Maintenance	Help

Hardware	Node List	Port List	Performance	FRU List

#	Name	Block Config	State	Type	Operating Speed	Alert
0		Unblocked	No Light	G_Port	1 Gb/sec	
1		Unblocked	No Light	G_Port	1 Gb/sec	
2		Unblocked	No Light	G_Port	1 Gb/sec	
3		Unblocked	No Light	G_Port	1 Gb/sec	
4		Unblocked	No Light	G_Port	1 Gb/sec	
5		Unblocked	No Light	G_Port	1 Gb/sec	
6		Unblocked	No Light	G_Port	1 Gb/sec	
7		Unblocked	No Light	G_Port	1 Gb/sec	
8		Unblocked	No Light	G_Port	1 Gb/sec	
9		Unblocked	No Light	G_Port	1 Gb/sec	
10		Unblocked	No Light	G_Port	1 Gb/sec	
11		Unblocked	No Light	G_Port	1 Gb/sec	
12		Unblocked	No Light	G_Port	1 Gb/sec	
13		Unblocked	No Light	G_Port	1 Gb/sec	
14		Unblocked	No Light	G_Port	1 Gb/sec	
15		Unblocked	No Light	G_Port	1 Gb/sec	

Figure 2–11: Port List View

The **Port List View** displays the following information on all ports that can be installed in the switch. All information is updated automatically.

- #

  Number of the port from 0 through 23.

- Name

  Displays the port name as configured through the **Configure Ports** dialog box.

- Block Config

  Indicates the blocked or unblocked configuration of the port as set through the **Configure Ports** dialog box.

Blocked states are:

— Blocked: Devices communicating with the port are prevented from logging into the switch or communicating with other devices attached to switch ports. A blocked port continuously transmits OLS.

— Unblocked: Devices communicating with the port can log in to the switch and communicate with devices attached to any other unblocked port in the same zone.

• State

The following port operational states may display in this table. For more information on these states and corresponding status symbol and LED indicator operations in the **Hardware View**, see FRU List View on page 2-34.

— No Light

— Online

— Offline

— Beaconing

— Link Reset

— Not Operational

— Not Installed

— Invalid Attachment

— Port Failure

— Segmented E_Port

— Link Incident

— Testing

— Inactive

• Type

The type of port. If the Port State is online, the available port types are F_Port, FL_Port, and E_Port. If the Port State is not online, the available port types are the configured type: Gx_Port, G_Port, Fx_Port, F_Port, and E_Port.

- Operating Speed

    This field displays the current data speed for the ports as 1 Gb/sec or 2 Gb/sec or Not Established.

- Alert

    This column displays a yellow triangle if a link incident occurs on the port or if the port's LED is beaconing. Blinking red and yellow diamonds display for port failures or for ports requiring service. Click on the row to display the reason for the alert in the **Port Properties** dialog box.

Double-click a row to display the **Port Properties** dialog box. For an explanation of the fields on the **Port Properties** dialog box, refer to Displaying Port Information on page 2–8.

Menu Options

Right-click a row to select it, highlight it, and display a menu with the following port-related action options. These are the same menu options that display when you right-click a port in the **Hardware View** and port bar graph in the **Performance View**. You can also display this menu by clicking on a port, port row, or port bar graph in the preceding views and selecting the **Port** secondary menu from the **Product** menu on the menu bar.

Refer to Port Menu on page 2–16 for details on these menu options.

- Port Properties
- Port Technology
- Block Port
- Enable Beaconing
- Port Diagnostics
- Clear Link Incident Alert
- Reset Port
- Port Binding
- Clear Threshold Alert(s)

Node List View

Display the **Node List View** in the view panel by selecting **Node List** from the view tabs on the Product Manager window. This view displays information about all node attachments to any F_Ports on the switch sorted by port number. All data is dynamic and updates automatically as devices log in and log out.

Hardware	Port List	**Node List**	Performance	FRU List		
Port #	Address	Node Type	Port WWN	Unit Type	BB_Credit	
1	020513	N_Port	EMC-20:01:00:60:48:00:00:01	Reserved	4	
2	020613	N_Port	Emulex-20:02:00:00:C9:00:00:01	Reserved	4	
3	020713	N_Port	Emulex-20:03:00:00:C9:00:00:01	Reserved	4	
5	020913	N_Port	Sun-20:05:08:00:20:00:00:01	Reserved	4	
6	020A13	N_Port	EMC-20:06:00:60:48:00:00:01	Reserved	4	
7	020B13	N_Port	JNI-20:07:00:E0:69:00:00:01	Reserved	4	
9	020D13	N_Port	EMC-20:09:00:60:48:00:00:01	Reserved	4	
10	020E13	N_Port	EMC-20:0A:00:60:48:00:00:01	Reserved	4	
11	020F13	N_Port	Sun-20:0B:08:00:20:00:00:01	Reserved	4	
13	021113	N_Port	Sun-20:0D:08:00:20:00:00:01	Reserved	4	
14	021213	N_Port	Sun-20:0E:08:00:20:00:00:01	Reserved	4	
15	021313	N_Port	JNI-20:0F:00:E0:69:00:00:01	Reserved	4	
17	021513	N_Port	Sun-20:11:08:00:20:00:00:01	Reserved	4	
18	021613	N_Port	EMC-20:12:00:60:48:00:00:01	Reserved	4	
19	021713	N_Port	EMC-20:13:00:60:48:00:00:01	Reserved	4	
21	021913	N_Port	Sun-20:15:08:00:20:00:00:01	Reserved	4	
22	021A13	N_Port	Sun-20:16:08:00:20:00:00:01	Reserved	4	
23	021B13	N_Port	Emulex-20:17:00:00:C9:00:00:01	Reserved	4	
0	00000	NL_Port	Not Logged-In			
1	00001	NL_Port	Not Logged-In			
2	00002	NL_Port	Not Logged-In			
3	00003	NL_Port	Not Logged-In			
4	00004	NL_Port	Not Logged-In			
5	00005	NL_Port	Not Logged-In			
6	00006	NL_Port	Not Logged-In			
7	00007	NL_Port	Not Logged-In			
8	00008	NL_Port	Not Logged-In			
9	00009	NL_Port	Not Logged-In			

Figure 2–12: Node List View

Information that displays for each node includes:

• Port #

  Number of the port, from 0 through 23.

• Fibre Channel Address

  The 3-byte Fibre Channel address for the node or the arbitrated loop physical address (ALPA) for private loop devices.

- Node Type

    — N_Port: The switch port is operating as an F_Port.

    — NL_Port: the switch port is operating as an FL_PortHub

- Port WWN

    The port WWN of the attached node (N_Port). The 16-digit WWN is a set of unique numbers assigned to the device attached to the port. The WWN is prefixed by the manufacturer's name of the host bus adapter that attaches to the device. If there is a nickname assigned, the nickname displays instead of the WWN. For private loop devices, "Not Logged In" displays.

    Unit Type

    The following information, if supported, is supplied by the attached device:

    — Converter

    — Gateway

    — HBA

    — Module

    — Other

    — Proxy-agent

    — Storage device

    — Software driver

    — Storage subsystem

    — Switch

    — Unknown

- BB_Credit

    The BB_Credit supported by the device. For private loop devices, this field will be blank.

NOTE: Private loop devices do not log into the fabric and do not provide any additional information other than their Arbitrated Loop Physical Address (ALPA) for private loop devices. The Port WWN field displays Not Logged In and the Unit Type field is blank for all private loop devices.

Double-click a row to display the **Node Properties** dialog box. For an explanation of the fields on the **Node Properties** dialog box, refer to Displaying Node Properties on page 2–25.

Menu Options

Right-click a row to select it, highlight it, and display a menu with the following port-related action options:

- Node Properties

    Select this option to display the **Node Properties** dialog box. Refer to Displaying Node Properties on page 2–25.

- Port Properties

    Select this option to display the **Port Properties** dialog box (refer to Figure 2–3 on page 2-8).

- Define Nickname

    Select this option to display the **Define Nickname** dialog box, where you can define a nickname to display for the attached device instead of the device's 8-byte WWN.

    The **Define Nickname** dialog box displays the world wide name (WWN) of the device attached to the port. To define a nickname, enter a name of up to 32 characters in the **Nickname** field and click **OK**. The nickname will display under the **Port WWN** column instead of the device's WWN.

- Display Options

    Select **Nickname** or **Worldwide Name** from the submenu. Selecting **Nickname** displays attached devices in the **Port WWN** column by the nickname configured through the **Define Nickname** menu option. Selecting **Worldwide Name** displays attached devices in the **Port WWN** column by the device's WWN.

Note that you can also display these menu options by clicking a port row, and selecting the **Port** secondary menu from the **Product** menu on the Product Manager menu bar.

Displaying Node Properties

Open the **Node Properties** dialog box by double-clicking a row in the **Node List View** or right-clicking a row and selecting **Node Properties** from the menu. You can also display this dialog box by right-clicking on a port in the **Hardware View**, right-clicking on a port's row in the **Port List View**, or right-clicking on a port's bar graph in the **Performance View** and selecting **Node List** from the menu that displays. In addition, you can display this dialog box by clicking to select a port, port row, or port bar graph in the preceding views and selecting **Node Properties** from the **Port** secondary menu on the **Product** menu of the menu bar.

NOTE: If a node is not logged in, a message appears indicating that node information is not available.

Port Number	1
Node Type	N_Port
Fibre Channel Address	020513
Port WWN	EMC-20:01:00:60:48:00:00:01
Port Nickname	
Node WWN	EMC-20:01:00:60:48:00:01:01
Node Nickname	
Unit Type	Reserved
Node Port Number	0
Buffer to Buffer Credit	4
Class of Service	Class 2
Data Field Size	10

Close

Figure 2–13: Node Properties dialog box

- Port Number

  The physical port number on the switch to which the node is connected.

- Fibre Channel Address

  The 3-byte address of the node or the ALPA for private loop devices.

- Port WWN

  Port worldwide name of the attached device.

- Port Nickname

  Nickname for the port WWN. Must be configured to display.

- Node WWN

  Node world-wide name of the attached device.

- Node Nickname

  Nickname for the node WWN. Must be configured to display.

- Node Port Number

  The physical port number field of the node port that is attached to the switch port (SB2- nodes only).

- Unit Type

  Type of unit as provided by the attached device.

- Class of Service

  Class of service. This can be class 2, class 3, or both.

- Data Field Size

  Data field size. This is the largest size of Fibre Channel frame the node will process. The size is negotiated with the attached device.

NOTE: Node Properties is also available from the menu that displays when you right-click a port's row in the **Port List View** or on a port's bar graph in the **Performance View**.

Performance View

Display the **Performance View** in the view panel by selecting **Performance** from the view tabs in the Product Manager window. This view displays a bar graph at the top of the view for each port. The lower portion of the view displays statistical values for the specific port's bar graph that you select.
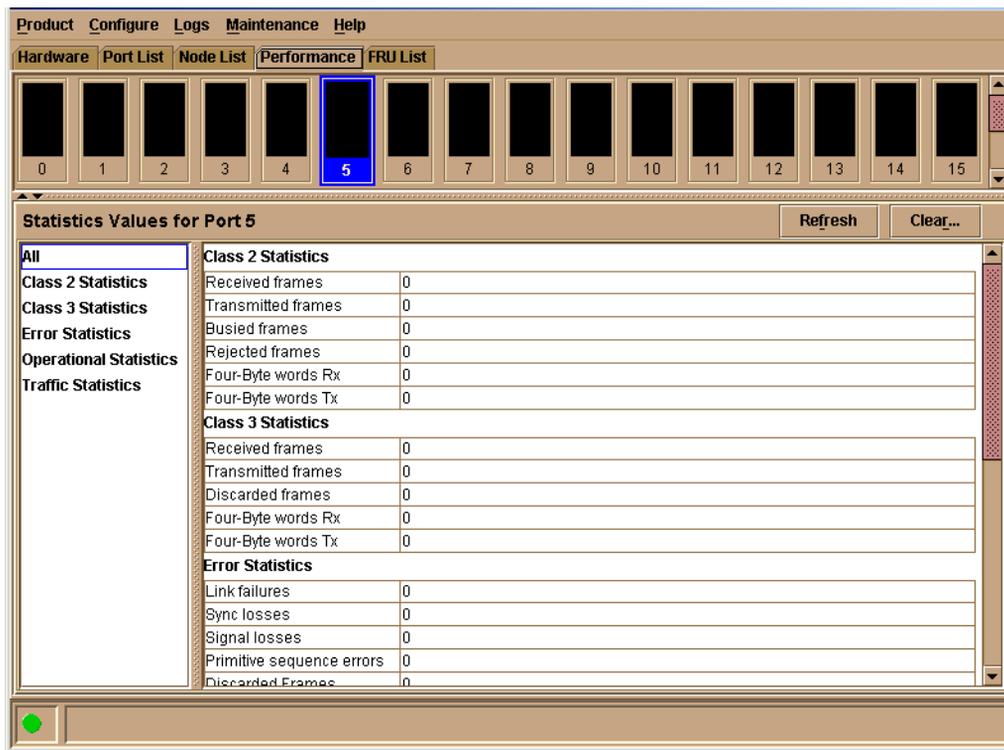

Figure 2–14: Performance View

Menu Options

Right-click any of the port bar graphs to display a menu with the following port-related action options. These are the same menu options that display when you right-click a port in the **Hardware View** or a port row in the **Port List View**. You can also display these options by clicking a port, port row, or port bar graph in the preceding views and selecting the **Port** secondary menu from the **Product** menu on the menu bar.

Refer to Port Menu on page 2–16 for an explanation of these menu options.

• Port Properties

• Node Properties

NOTE: If a node is not logged in, a message displays indicating that node information is not available.

• Port Technology

• Block Port

• Enable Beaconing

• Port Diagnostics

• Clear Link Incident Alert(s)

• Reset Port

• Port Binding

• Clear Threshold Alert(s)

Bar Graph Display

The **Performance View** provides a graphical display of performance for all ports. Each bar graph in the upper portion of the view panel displays the percentage of link utilization for the port. This information updates every five seconds. A red arrow marks the highest utilization since the opening of the **Performance View**. If the system detects activity on a port, it represents minimal activity with one bar.

When a port is operating as an F_Port and a device is logged on, moving the cursor over the port's bar graph displays a message with the attached port's WWN. If the port is an E_Port, the message reads, E_Port. If the port is an FL_Port, FL_Port displays. If the port is not logged in, the message displays the port's current operational state (refer to Table 2–1 on page 2-35).

Port Statistics

To select and display more detailed performance information for a port, click the port's bar graph. The bar graph for that port highlights with a darker background and the lower portion of the **Performance View** view panel displays the statistics values for the port's number and the WWN decoding. The **Statistics Values** tables contain cumulative port statistics and error statistics. For a description of the **Refresh** and **Clear** buttons, refer to Button Functions on page 2–34.

Statistics Description

The **Statistics Values** tables contain statistics in the following groups. To refresh tables with the latest data, click the **Refresh** button on the upper right portion of the **Statistics Values** panel or click the port's bar graph. Clear all counters for all users using the **Clear** button.

Traffic Statistics with Receive and Transmit Values

This section describes the types of statistics that display when you click a port's bar graph:

- Link utilization%

  There is a separate value for transmit and receive link utilization. The larger of these two values displays on the bar graph.

  The current link utilization for the port is expressed as a percentage. Each port can transmit or receive data at 100 Megabytes (MB) per second. This statistic shows the percentage of the maximum link utilization currently being used. Link utilization is calculated over one-second intervals. The maximum link utilization is 100%.

- Frames

  The number of frames that the port has received or transmitted.

- Transmitted Frames

  The number of Class 2 frames transmitted by the F-Port to its attached N_Port.

- Four Byte Words Rx

  The number of words that the port has received.

- Four Byte Words Tx

  The number of words that the port has transmitted.

- Offline sequences

  The number of offline sequence that the port has received or transmitted.

- Link resets

  The number of link reset protocol frames received/transmitted by this port from/to the attached switch. The switch transmits a link reset to initiate the link reset protocol or recover from a link timeout. The switch receives a link reset from an attached device if the device wishes to initiate the link reset or recover from a link timeout.

  There are not thresholds for these values. You may determine that a problem exists by the rate that the value changes.

- LIPS

  The number of Loop Initialization Primitives (LIPS) generated/detected by this port. These cause re-initialization of the port.

Class 2 Statistics

The **Class 2 Statistics** table includes:

- Received Frames

  The number of Class 2 frames received by this F_Port from its attached N_Port.

- Transmitted Frames

  The number of Class 2 frames transmitted by the F-Port to its attached N_Port.

- Busied Frames

  The number of F_BSY frames generated by this F_Port against Class 2 frames. This can occur if frames are received before the switch completes initialization or if the switch is servicing so many requests that it can not process a new request. The port generates frames if the switch is not ready to accept commands. This may indicate temporary congestion.

- Rejected Frames

  The number of F_RJT frames generated by this F_Port against Class 2 frames.

  These frames usually occur because of attached device errors. The device is expected to correct the error based on the reject code, then retry its request. If the device is able to recover, there is no cause for concern. If not, further

troubleshooting may be necessary. There are no thresholds for this value. Typically, this occurs because the destination is not available due to the device's action.

- Four Byte Words Received

  The number of four-byte words received.

- Four Byte Words Transmitted

  The number of four-byte words transmitted.

Class 3 Statistics

The **Class 3 Statistics** table includes:

- Received Frames

  The number of Class 3 frames received by this F_Port from its attached N_Port.

- Transmitted Frames

  The number of Class 3 frames transmitted by the F-Port to its attached N_Port.

- Discarded Frames

  The number of Class 3 frames discarded, including multicast frames with bad D_IDs.

  The switch increments this count when it discards a frame that cannot be routed. This occurs most frequently when a destination becomes unavailable without the source realizing the destination is unavailable. There are no thresholds for this value. Typically, this occurs when the destination is not available due to the destination device's action.

- Four Byte Words Received

  The number of four-byte words received.

- Four Byte Words Transmitted

  The number of four-byte words transmitted.

Error Statistics

Port errors indicate that a port is not operating correctly. Use this data to isolate problems with port and link operations. The statistics in this table include:

- Link failures

    A link failure was recorded in response to a not operational sequence (NOS), protocol timeout, or port failure. At the **Hardware View**, a yellow triangle appears to indicate a link incident, or a blinking red and yellow diamond appears to indicate a port failure.

- Sync losses

    A loss of synchronization was detected because the attached device was reset or disconnected from the port. At the **Hardware View**, a yellow triangle appears to indicate a link incident.

- Signal losses

    A loss of signal was detected because the attached device was reset or disconnected from the port. At the **Hardware View**, a yellow triangle appears to indicate a link incident.

- Primitive sequence errors

    An incorrect primitive sequence was received from the attached device, indicating a Fibre Channel link-level protocol violation. At the **Hardware View**, a yellow triangle appears to indicate a link incident.

- Discarded frames

    A received frame could not be routed and was discarded because the frame timed out (insufficient buffer-to-buffer credit) or the destination device was not logged into the switch.

- Invalid transmission words

    The number of times that the switch detected invalid transmission words from the attached device. This indicates that a frame or primitive sequence arrived at the switch's port corrupted. This corruption can be due to the attached device performing a reset, plugging or unplugging the link, bad optics at either end of the cable, bad cable, or a dirty or poor connection. Moving the connection around or replacing cables can isolate the problem.

Some number of invalid transmission words are expected and acceptable. Invalid transmission words within a frame are used to produce the bit-error threshold link incident. If one or more invalid transmission words are detected in 12 separate 1.5-second samples within five minutes, a bit-error threshold link incident is generated.

- CRC errors

  A received frame failed a cyclic redundancy check (CRC) validation, indicating the frame arrived at the switch's port corrupted. Frame corruption may be caused by device disconnection, an optical transceiver failure at the device, a bad fiber-optic cable, or a poor cable connection.

- Delimiter errors

  The number of times that the switch detected an unrecognized start-of-frame (SOF), an unrecognized end-of-frame (EOF) delimiter, or an invalid class of service. This indicates that the frame arrived at the switch's port corrupted. This corruption can be due to plugging/unplugging the link, bad optics at either end of the cable, bad cable, or dirty or poor connections. Moving the connection around or replacing cables can isolate the problem.

- Address ID errors

  A received frame had an unavailable or invalid Fibre Channel destination address, or an invalid Fibre Channel source address. This typically indicates the destination device is unavailable.

- Frames too short

  A received frame exceeded the Fibre Channel frame maximum size or was less than the Fibre Channel minimum size, indicating the frame arrived at the switch's port corrupted. Frame corruption may be caused by device disconnection, an optical transceiver failure at the device, a bad fiber-optic cable, or a poor cable connection.

Troubleshooting Tips

As a general rule, you should clear all counts after the system is stabilized. When looking at the **Performance View**, roughly keep track of the time interval when errors accumulate to judge the presence and severity of a problem. Also, recognize that there is a link recovery hierarchy implemented in Fibre Channel to handle some level of "expected anomalies." In general, only be concerned with error counts that increment very quickly.

Button Functions

The two buttons located at the right end of the title bar on the **Statistics Values** table are:

- Clear

  The **Clear** button clears all counters to zero. Selecting this button displays a **Clear Request Confirmation** dialog box. Confirming the request clears the statistics in the hardware at the physical port. Note that this also clears counters for other Product Manager users.

  An entry identifying when the statistics were cleared and by whom is saved in the **Audit Log**.

- Refresh

  The **Refresh** button updates the data in the statistics tables and enables you to compare values at any given time. Note that you can also refresh data by clicking the port's bar graph.

FRU List View

Display the **FRU List View** (Figure 2–15 on page 2-34) by selecting the **FRU List** view tab on the Product Manager window. This view displays information about all installed FRUs on the switch. All data is dynamic and updates automatically as the software detects changes.

FRU	Position	Status	Part Number	Serial Number
CTP	0	Active	470-000465-101	42360121
PWR	0	Active		
PWR	1	Active		

Tabs: Hardware | Port List | Node List | Performance | FRU List

Figure 2–15: FRU List View

Information on the **FRU List View** for each FRU includes:

- **FRU Name**: CTP (Control Processor) card and PWR (power-supply module). Note that the CTP card is an internal component and is not a FRU. If it fails completely, the entire switch must be replaced.

- **Position**: Slot position of FRU in the chassis relative to identical FRUs also installed in the chassis.

- These consist of one CTP card (position 0) and two power supply modules/fan (positions 0-1):

    — PWR - Power supply module/fan

    — CTP - Control processor

- **Status**: Active or failed. **Active** displays always unless the FRU fails. **Failed** displays if the FRU is not functional.

- **Part Number**: Part number of the FRU.

- **Serial Number**: Serial number of the FRU.

Port Operational States

Table 2–1 describes the port operational states and the LED and attention indicators that display in the **Hardware View** and **Port List View**.

Table 2–1: Port States and Indicators

Port State	Port Indicators		Alert Indicator[a]	Description
	Green/Blue	Amber		
Beaconing	Off or On	Blink	Yellow Triangle	The port is beaconing. The amber port LED blinks once every two seconds to enable users to find a specific port. Enable beaconing through the port's menu on the **Hardware View**, *P*ort **List View**, or **Performance View**.
Inactive	Off	Off	Yellow Triangle	The switch port is in an inactive state. Reasons for this state appear in the **Reason** field of the **Port Properties** dialog box. Note that if port optics have also failed, the amber LED will be on.

Table 2–1: Port States and Indicators (Continued)

Port State	Port Indicators		Alert Indicator[a]	Description
	Green/Blue	Amber		
Invalid Attachment	On	Off	Yellow Triangle	The switch port is in an invalid attachment state. Reasons for this state appear in the **Reason** field of the **Port Properties** dialog box.
Link Incident	Off	Off	Yellow Triangle	A link incident occurred on one of the ports and displays in the **Port List View** with a corresponding indicator displaying for the card in the **Hardware View**.
Link Reset	Off	Off	Yellow Triangle	The switch and the attached device are performing a link reset operation to recover the link connection. Ordinarily, this is a transient state that should not persist.
No Light	Off	Off	None	No signal (light) is being received on the switch port. This is a normal condition when there is no cable plugged into the port or when the power of the device attached to the other end of the link is off.
Not Operational	Off	Off	Yellow Triangle	The switch port is receiving the Fibre Channel not operational sequence (NOS), indicating that the attached device is not operational.
Online	On	Off	None	The attached device has successfully connected to the switch and is ready to communicate or is in the process of communicating with other attached devices. As long as the port remains in the online state, the green/blue port LED remains illuminated. Note that on the actual port in the unit, the green/blue LED blinks when there is active Fibre Channel traffic through the port.

Table 2–1: Port States and Indicators (Continued)

| Port State | Port Indicators | | Alert Indicator[a] | Description |
	Green/Blue	Amber		
Offline	Off	Off	None	The switch port was configured as "blocked" and is transmitting the Fibre Channel OLS to the attached device.
	Off	Off	Yellow Triangle	The switch port was configured as "Unblocked" and is receiving the Fibre Channel OLS, indicating that the attached device is offline.
Port Failure	Off	On	Red and Yellow Blinking Diamond	The switch port has failed and requires service. The amber LED for the port remains illuminated.
Segmented E_Port	On	Off	Yellow Triangle	The E_Port is segmented preventing the two fabrics from joining (this only occurs when two switches are connected to each other). Display the **Port Properties** dialog box to view the segmentation reason.
Testing	Off	Blink	Yellow Triangle	Port is executing an internal loopback test.
	On	Blink	Yellow Triangle	Port is executing an external loopback test.
				Note: For any loopback test, the amber LED blinks (beacons) to help users locate the port under test.
Not Installed	Off	Off	Yellow Triangle	The port optics are not installed or the feature that provides additional port function is not enabled.

a. The alert indicator displays on the port in the **Hardware View**. It indicates that a corrective action is required to return the port to a normal operating state.

Link Incident Alerts

A link incident is a problem detected on a fiber optic link, like the loss of light, invalid sequences, and other problems. When a problem occurs, a LIN alert is sent to the **Link Incident Log** in the switch Product Manager. LIN alerts warn you that there is a link incident being detected through a port connection that may require operator intervention to correct.

If LIN alerts are enabled for a port in the **Configure Ports** dialog box, a yellow triangle (attention indicator) displays by the port connector in the **Hardware View** or in the **Alert** column in the **Port List View**. A corresponding triangle displays for the card on the **Hardware View**. Double-clicking the port with the yellow triangle displays the **Port Properties** dialog box.

If LIN alerts have been enabled for a port in the **Configure Ports** dialog box, the **Port Properties** dialog box contains a short description of the latest incident in the **Link Incident** field. Or, if there are no active incidents, "None" displays. The system writes all link incidents to the **Link Incident Log**.

If you enable LIN alerts for a port in the **Configure Ports** dialog box, configure e-mail notification through the HAFM, and enable **E-Mail Notification** through the **Maintenance** menu, you will receive e-mail notification of LIN alerts.

NOTE: The e-mail notification of LIN alerts is available to all users; no user rights are imposed.

Although you can clear the attention indicator in the **Hardware View** and the alert description in the **Port Properties** dialog box manually, they may also be cleared by actions outside of your control; such as on HAFM server reboot.

You can clear the link incident indicator in the **Hardware View** and the description in the **Link Incident** field manually. To manually clear the attention indicator (yellow triangle), right-click the port with the yellow triangle and select **Clear Link Incident Alert(s)** from the menu. In the **Clear Link Incident Alert(s)** dialog box, select the appropriate option and click **OK**.

Be aware that clearing the incident indicator clears it for everyone using the system. If there are no link incident alerts enabled for a port, no actions occur.

Threshold Alerts

A threshold alert notifies Product Manager users when the transmit (Tx) or receive (Rx) throughput reaches specific values for switch ports or port types (E_Ports or F_Ports or FL_Ports).

Select the **Threshold Alerts** option on the **Configure** menu to display the **Configure Threshold Alerts** dialog box. Use this dialog box to configure criteria for generating a threshold alert. One criteria that you must configure is a throughput value that equals a specific percentage of the port's total throughput capacity. You also provide a time interval during which throughput is measured and a time interval during which that throughput value must remain constant. When throughput reaches the threshold value and remains constant for the specified time, an alert is generated.

Threshold alerts occur as the following in the Product Manager:

- An attention indicator (yellow triangle) that displays on the port in the **Port Card View**.

- An attention indicator (yellow triangle) that displays on the port card in the **Hardware View**.

- An attention indicator (yellow triangle) that displays in the **Alert** column of the **Port List View**.

- An attention indicator (yellow triangle) that displays by the **Threshold Alerts** field in the **Port Properties** dialog box.

- Detailed threshold alert data recorded in the **Threshold Alert Log**.

For detailed procedures to configure threshold alerts, refer to Configure Threshold Alerts on page 3–19.

3

Configuring the Switch

This chapter describes how to use the options that display on the Product Manager's **Configure** menu on the Product Manager menu bar.

Configure Identification

Use the procedure in this section to identify the switch by its name, description, location, and contact person. This information displays in the following Product Manager locations:

- Product Manager window title panel (name)

- **Switch Properties** dialog box (name, location, contact, description)

- Identification table at the top of the **Hardware View** (name, location, description)

The name also displays in the switch icon label in the HAFM **Product** tab if the product name is enabled through the HAFM **Display Options**.
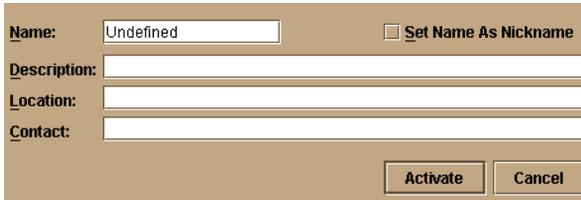
Data entered through the following procedure is saved in nonvolatile random access memory (NV-RAM) on the switch.

Procedure

To configure identification for the switch, use the following steps:

1. From the menu bar, select **Configuration > Identification**.

   The **Configure Identification** dialog box displays.

Figure 3–1: Configure Identification dialog box

2. Click in the name field and enter a name for the switch. The name could reflect the switch's Ethernet network domain name service (DNS) host name, if assigned.

3. Click in the **Description** field and enter a description of the switch.

4. Click in the **Location** field and enter the location of the switch.

5. Click in the **Contact** field and enter appropriate information about a contact person, such as a phone number, title, or e-mail address.

6. Click **Set Name as Nickname** and add a check mark to the check box if you want to use the name in the **Name** field as a nickname for the switch's WWN. The nickname will then display instead of the WWN in Product Manager views.

7. Click **Activate** to save the data and close the dialog box.

8. If you are finished configuring the switch, back up the configuration data. For more information, refer to Backup and Restore Configuration on page 5–6.

Configure Switch Operating Parameters

Use procedures in this section to set parameters on the switch for fabric operation through the **Configure Switch Parameters** dialog box. These operating parameters are stored in NV-RAM on the switch.

You can configure the following switch parameters as required by your fabric:

- Preferred Domain ID

  Use this field to set each switch in the fabric to a unique preferred domain ID. Fibre Channel addresses in the switch include this preferred domain ID, which creates a unique identification for the port in the fabric. The default value is 1. Set a preferred value from 1 through 31.

  The preferred domain ID must be unique for each switch in a fabric. If two switches have the same preferred domain ID, the E_Ports segment, causing the fabric to segment. For more information on domain ID, refer to the section on domain ID assignment for multi-switch fabrics in the *hp StorageWorks SAN high availability planning guide*.

- Insistent

  This option is not supported unless the SANtegrity feature is installed. Click the check box to remove or add a check mark. The default state is disabled (no check mark).

  When a check mark displays, the domain ID configured in the **Preferred Domain ID** field will become the active domain identification when the fabric initializes. See the following notes:

  — This option is required if Enterprise Fabric Mode (optional SANtegrity feature) is enabled. See Insistent Domain Identification (ID) on page 6–9 for more information.

  — If you enable Insistent Domain while the Edge Switch or Director is online, the Preferred Domain ID will change to the current active domain ID if the IDs are different.

> **CAUTION:** If a switch with a duplicate domain ID exists in the fabric, both switches' E_Ports will segment when they try to join.

- Rerouting Delay

  Placing a check mark in the check box to the left of the Rerouting Delay option enables rerouting delay. This option is only applicable if the configured switch is in a multi-switch fabric. The default state is disabled.

  Enabling the rerouting delay ensures that frames are delivered in order through the fabric to their destination. If there is a change to the fabric topology that creates a new path (for example, a new switch is added to the fabric), frames may be routed over this new path if its hop count is less than a previous path with a minimum hop count. This may result in frames being delivered to a destination out of order since frames sent over the new, shorter path may arrive ahead of older frames still in route over the older path.

  If rerouting delay is enabled, traffic ceases in the fabric for the time specified in the **E_D_TOV** field of the dialog box. This delay allows frames sent on the old path to exit to their destination before new frames begin traversing the new path.

- Domain RSCNs

  Use this check box to enable Domain register for state change notifications (domain RSCNs). Domain RSCNs are sent between end devices in a fabric to provide additional connection information to host bus adapters (HBA) and storage devices. As an example, this information might be that a logical path has been broken because of a physical event, such as a fiber optic cable being disconnected from a port. Consult with your HBA and storage device vendor to determine if enabling Domain RSCNs will cause problems with your HBA or storage products. If Enterprise Fabric Mode is enabled, this parameter is automatically enabled and cannot be disabled unless the director or switch is offline. Disabling Domain RSCNs also disables Enterprise Fabric Mode.

Procedure

To configure switch operating parameters:

1. The switch must be offline to change the Preferred Domain ID. If it is not, and you activate values in this dialog box,you are prompted to set the unit offline.

⚠ **CAUTION:** Setting the switch offline terminates all Fibre Channel connections.

To set the unit offline:

   a. From the Product Manager window menu bar, select **Maintenance** > **Set Online State**.

   b. When the **Set Online State** dialog box displays, click **Set Offline**.

   c. When the warning box displays asking to confirm the offline state, click **OK**.

2. Select **Configure** > **Operating Parameters** > **Switch Parameters**.

   The **Configure Switch Parameters** dialog box displays.
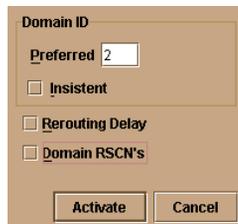
Figure 3–2: Configure Switch Parameters dialog box

NOTE: Ordinarily, you do not need to change values in this dialog box from their defaults. The only exception is the Preferred Domain ID. Change this value if the switch will participate in a multi-switch fabric.

3. Use the information described earlier in this section to change settings as required for parameters in this dialog box.

4. After you change settings, click the **Activate** button.

5. Set the switch online:

   a. Select **Set Online State** from the **Maintenance** menu on the menu bar.

   b. When the **Set Online State** dialog box displays, click the **Set Online** button.

Configure Fabric Operating Parameters

Use the procedures in this section to configure the following Fibre Channel operating parameters using the **Configure Fabric Parameters** dialog box. The operating parameters are stored in NV-RAM on the switch.

You can configure the following fabric operating parameters as required by your fabric:

- R_A_TOV

  Resource allocation time-out value. This variable is used to time out operations that depend on the maximum possible time that a frame can be delayed in a fabric and still be delivered. Adjust the value for R_A_TOV in tenths of a second (100 ms) increments over a range of 10 tenths (1 second) to 1200 tenths (120 seconds). The default value is 100 tenths (10 seconds).

NOTE: Set the same value for R_A_TOV on all switches on a multi-switch fabric. If the value is not the same on all units, the fabric segments. Also, the value for R_A_TOV must be greater than the value configured for E_D_TOV.

- E_D_TOV

  Error-detect time-out value: This defines the time that the switch waits for an expected response before declaring an error condition. Configure this value in tenths of a second (100 millisecond) increments in a range of 2 tenths of a second to 600 tenths (60 seconds). The default value is 20 tenths (2 seconds).

NOTE: Set the same value for E_D_TOV on all switches on a multi-switch fabric. If the value is not the same, the fabric segments.

- Switch Priority

  Setting this value determines the principal switch for the multi-switch fabric. Select either Principal (highest priority), Default, or Never Principal (lowest priority) from the **Switch Priority** drop-down list.

  Changed all this because of new switch priority options.

  If all switches are set to Principal or Default, the switch with the highest priority and the lowest WWN becomes the principal switch. Following are some examples of principal switch selection when switches have these settings.

  — If you have three switches and set all to Default, the switch with the lowest WWN become the principal switch.

  — If you have three switches and set two to Principal and one to Default, the switch with the Principal setting that has the lowest WWN becomes the principal switch.

— If you have three switches and set two to Default and one to Never Principal, the switch with the Default setting and the lowest WWN becomes the principal switch.

Note that at least one switch in a multi-switch fabric needs to be set as Principal or Default. If all of the switches are set to Never Principal, all of the interswitch links (ISLs) will segment. If all but one switch is set to Never Principal and the switch that was Principal goes offline, then all of the other ISLs will segment.

NOTE: We recommend configuring switch priority as Default. If you are considering changing this value to something other than the default, refer to sections on principal switch selection for multi-switch fabrics in the *hp StorageWorks SAN high availability planning guide* for details.

In the Audit Log, you may notice that the Principal setting maps to a number code of 1, Default maps to a number code of 254, and Never Principal maps to a number code of 255. The number codes 2-253 are no longer in use.

- Interop Mode

Select the interoperability mode for the switch:

— Homogeneous Fabric - Select this mode if the fabric contains only HP Edge Switches and Directors that are also operating in Homogeneous Fabric mode.

— Open Fabric 1.0 - Default. Select this mode if the fabric contains HP Directors and Edge Switches and other open-fabric compliant switches. Select this mode for managing heterogeneous fabrics.

Procedure

To configure fabric operating parameters

1. The switch must be offline to configure parameters in this dialog box. If it is not and you activate values in this dialog box, a dialog box displays prompting you to set the unit offline.

⚠ **CAUTION:** Setting the switch offline terminates all Fibre Channel connections.

To set the unit offline:

a. From the Product Manager window menu bar, select **Maintenance** > **Set Online State**.

b. When the **Set Online State** dialog box displays, click **Set Offline**.

    c.   When the warning box displays asking you to confirm the offline state, click **OK**.

2.   Select **Configure** > **Operating Parameters** > **Fabric Parameters**.

    The **Configure Fabric Parameters** dialog box displays.
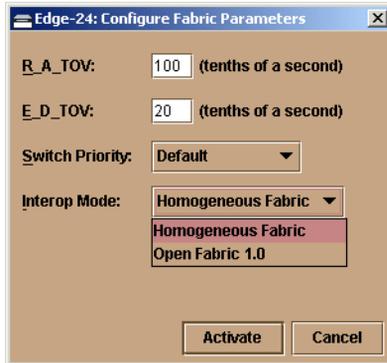
Figure 3–3: Configure Fabric Parameters dialog box

NOTE: Ordinarily, you do not need to change values in this dialog box from their defaults. Change this value if the switch will participate in a multi-switch fabric.

3.   Use information described earlier in this section to change settings as required for parameters in this dialog box.

4.   After you change settings, click the **Activate** button.

Configure Switch Binding

For complete procedures for configuring this optional feature, refer to Switch Binding on page 6–3.

Configure Ports

Use the procedures in this section to configure ports. Port configuration data is stored in NV-RAM on the switch.

Port information includes:

- Port #

  You cannot edit this field. This column identifies the port number. The port numbers range from 0 through 23.

- Name

  Enter a name for the port. The port names display in the **Port Properties** dialog box and elsewhere in the Product Manager to identify the port.

NOTE: To identify port numbers for which you want to provide names, place the cursor over the ports in the **Hardware View.** As you move over a port, a message displays that identifies the slot number where the port is installed.

- Blocked (open systems mode only)

  Placing a check mark in the check boxes of this column blocks the operation of the port.

- LIN Alerts

  A link incident (LIN) is a problem detected on a fiber optic link, such as the loss of light or invalid sequences. When a problem occurs, a LIN alert is sent to the **Link Incident Log** in the switch Product Manager. LIN alerts warn you that there is a link incident being detected through a port connection.

  Place or remove check marks in the check boxes in this column to enable or disable link incident alerts. The factory default is to enable LIN alerts.

  A link incident causes a yellow attention indicator (triangle) to display for the port in the **Hardware View** and in the alert column of the **Port List View**. Once a LIN occurs, you must acknowledge it by selecting the **Clear Link Incident Alert** option from the right-click menu for the port (**Hardware View**). A description of the alert displays in the **Link Incident** field of the **Port Properties** dialog box (refer to Figure 2–3).

  If the check boxes in this column are not selected, no link incident indicators display in the **Hardware View**. Also, the **Link Incident** field of the **Port Properties** dialog box is blank and a link incident is recorded in the **Link Incident Log**. LINs are always logged in the **Link Incident Log**, regardless of the configuration.

If LIN Alerts are enabled, you can receive e-mail notification when a LIN occurs. In order to receive e-mail notification, you must configure and enable this feature in the HAFM (**Maintenance** menu) and enable e-mail notification through the **Enable E-Mail Notification** option on the Product Manager's **Maintenance** menu.

For additional information about LIN alerts, refer to Link Incident Alerts on page 2-38.

- FAN

    Click to display a check mark in the check box and enable Fabric Address Notification for loop devices attached to the port. Right-click in this column to either clear all FANs for all ports or set all FANs for all ports.

- Type

    Select each port's type (G_Port, E_Port, F_Port, Fx_Port, or Gx_Port) in this column from the drop-down list. Right-click in this column to set all ports to either, E_Ports, F_Ports, Fx_Ports, G_Ports, or Gx_Ports.

- Port Binding

    Click this check box to display a check mark and enable Port binding for the port. This allows only a specific device to attach to the port. This device is specified by the WWN or nickname entered into the **Bound WWN** column. With the check box cleared, any device can attach to the port even if a WWN or nickname is specified in the **Bound WWN** column.

- Bound WWN

    Enter a world wide name (WWN) in the proper format (xx.xx.xx.xx.xx.xx.xx.xx) or a nickname configured through the HAFM application. The device with this WWN or nickname will have exclusive attachment to the port if **Port Binding** is enabled. If a valid WWN or nickname is not entered in this field, but the **Port Binding** check box is checked (enabled), then no devices can connect to the port. If you enter a WWN or nickname in this field and do not place a check in the **Port Binding** check box, the WWN or nickname will be stored, and all devices can connect to the port.

Procedure (open systems mode)

To configure ports in open systems mode, use the following steps:

1. Select **Ports** from the **Configure** menu on the menu bar.

   The **Configure Ports** dialog box displays.

Figure 3–4: Configure Ports dialog box

Ports are numbered from 0 through 23.

2. Click a **Name** field and type a name that reflects the end device connected through the port. For example, use "XYZ Server," where **XYZ** is the brand name of the server.

3. Block or unblock operation for a port by clicking the check box in the **Blocked** column. When a check mark displays, the port is blocked.

4. Enable or disable LIN alerts for the port by clicking the check box in the **LIN Alerts** column. When a check mark displays, LIN alerts are enabled.

NOTE: The factory default for LIN alerts is enabled.

5. Click the check box in the FAN column to enable Fabric Address Notification for loop devices.

6. Select a port type by clicking in the **Type** field and selecting from the list.

7. To bind a device with a specific WWN or nickname to the port, click the **Port Binding** check box to display a check mark. Then enter the WWN or configured nickname for the device into the **Bound WWN** column. The device that you bind to the port will have exclusive connection to that port.

   Notes:

   — If you have configured port binding and click **Activate**, a warning dialog box displays if one or more of the nodes attached to a port does not match the WWN or nickname configured in the **Bound WWN** column. This warning box displays a list of all attached nodes that will be logged off if you continue. If you click **Continue**, these nodes will log off and the port will only attach to the device with the WWN or nickname configured in the **Bound WWN** column.

   — If you have configured port binding and click **Activate**, an error message may display if the format for the WWN entered in the **Bound WWN** column is not valid (not in xx.xx.xx.xx.xx.xx.xx.xx format) or if you enter a nickname that has not been configured through the Product Manager.

8. Use the scroll bar on the right side of the **Configure Ports** dialog box table to display additional ports that you want to configure.

9. Activate changes and close the dialog box by clicking **Activate**.

10. If you are finished configuring the switch, back up the configuration data. For more information, refer to Backing Up and Restoring Configuration Data on page 3-29.

Configure SNMP

Use the procedures in this section to:

• Configure the SNMP agent that runs on the switch and implements the following MIBs:

   — MIB-II

   — Fabric Element MIB

   — Fibre Alliance (FCMGMT) MIB

   — Switch private MIB

For complete information on objects defined in MIBs and steps to download MIB variables to your SNMP workstation, refer to the *hp StorageWorks SNMP reference guide for directors and edge switches.*

- Configure network addresses and community names for up to six SNMP trap recipients.

  An SNMP trap recipient is a network management station that receives messages through SNMP for specific events that occur on the switch.

- Define SNMP community names that SNMP managers use for reading variables.

- Authorize write permissions for writable MIB variables.

NOTE: SNMP managers may request, but will not receive, traps and SNMP data through SNMP management stations that are not configured with community names.

Procedure

To configure SNMP traps and assign community names, use the following steps:

1. Select **SNMP** from the **Configure** menu on the menu bar.

   The **Configure SNMP** dialog box displays.

Figure 3–5: Configure SNMP dialog box

2. Click the **Enable Authorization Traps** field to enable authorization traps to be sent to SNMP management stations when unauthorized stations try to access SNMP information from the switch.

3. Click a field in the **Community Name** column to select the row. Enter the SNMP community name for the trap recipient. Enter up to 32 characters. This also defines community names from which SNMP managers can read MIB variables from or write MIB variables to the switch. Refer to the note under Configure SNMP on page 3-12 for more information about assigning community names.

4. Click the **Write Authorization** check box to enable write authorization for the community name. A check mark displays in the box to indicate that write authorization is enabled.

5. Enter the IP address for a trap recipient (SNMP management station) by clicking in the **Trap Recipient** column and entering an IP address.

NOTE: Step 6 usually is not necessary. If you do not wish to override the default UDP number, skip to step 7.

6. Enter user datagram protocol (UDP) port numbers in the **UDP Port Number** column. You can override the default UDP port number of 162 with any legal UDP port number (1 to 65535).

Figure 3–6: Configure SNMP dialog box

7. Click **Activate** to activate the data and close the dialog box.

    The SNMP configuration is stored in NV-RAM on the switch.

8. If you are finished configuring the switch, back up the configuration data. For more information, refer to Backup and Restore Configuration on page 5–6.

Configure Open Systems Management Server

Use these procedures to configure the open systems inband management program to function with the switch.

NOTE: The optional Open Systems Management Server feature must be enabled in order to perform this procedure.

Procedure

To configure the Open Systems Management Server, use the following steps:

1. Select **Management Server** from the **Configure** menu on the menu bar.

    The **Configure Open Systems Management Server** dialog box displays.

2. Enable the management server by clicking the **Enable Management Server** check box to add a check mark. (To disable the management server, click the check box again to remove the check mark.)

3. Click the check box in the **Host Control Prohibited** field to display a check mark and prohibit a host management program from changing configuration and connectivity parameters on the switch. In this case, the host program has read-only access to configuration and connectivity parameters. Clicking the check box when it contains a check mark removes the check mark and allows a host program to change configuration and connectivity parameters on the switch.

4. Activate changes and close the dialog box by clicking **Activate**.

5. If you are finished configuring the switch, you can back up the configuration data. For more information, refer to Backup and Restore Configuration on page 5-6.

Configure Feature Key

A feature key is a string of alphanumeric characters consisting of both uppercase and lowercase. The following is an example of a feature key format: XxXx-XXxX-xxXX-xX.

NOTE: The total number of characters may vary. The key is case-sensitive and must be entered exactly, including the dashes.

The feature key, which is encoded with a switch's serial number, can only be configured on the switch to which it is assigned.

To enable an optional feature on the switch, first set the switch offline, then enter the feature key into the **New Feature Key** dialog box.
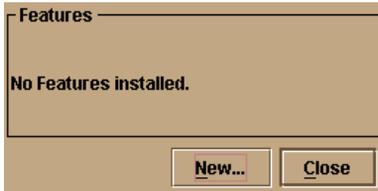
Display this dialog box by selecting **Feature** from the **Configure** menu on the menu bar.

Procedure

To configure a feature key, use the following steps:

1. Set the switch offline using the **Set Online State** dialog box. For help, refer to Set Online State on page 5-3.

2. Select **Features** from the **Configure** menu on the menu bar.

   The **Configure Feature Key** dialog box displays.

Figure 3–7: Configure Feature Key dialog box

3. Click **New** to add a new feature key.

4. In the **New Feature Key** dialog box, enter the switch's feature key and click **OK**.

   — Feature keys are only valid for a switch with a specific serial number. They cannot be interchanged between switches. If an error stating "Invalid serial number" displays, verify that you have entered the feature key that was assigned to the switch. To verify, check the serial number of the switch through the **Switch Properties** dialog box and compare it to the serial number listed in the documentation provided with your feature key. Refer to Displaying Switch Information on page 2-12 for instructions on displaying the **Switch Properties** dialog box.

   — The feature key is a string of alphanumeric characters with dashes. The key is case-sensitive, so enter the key exactly as printed in the documentation that you received for the feature. If an error stating "Invalid feature key" displays, verify that you have entered the feature key correctly.

   The **Enable Feature Key** dialog box displays with a warning, stating that this action will override the current set of features on the switch. The list in the left column of the dialog box is a list of features that are active on the switch. The list on the right is a set of features that come with the new feature key. All of the features that are active are included in the new feature list.

5. Click **Activate** to activate the new feature key.

   An IPL will occur, during which the Ethernet connection between the HAFM server and switch is momentarily interrupted.

NOTE: If you click **Activate**, all current features will be replaced with new features. That is, if there are features shown in the current list that are not shown in the new list, then those features will be removed from the switch.

6. Set the switch back online.

7. When you are finished configuring the switch, you can back up the configuration data. For more information, refer to Backing Up and Restoring Configuration Data on page 3-29.

Configure Date and Time

Use the procedures in this section to display and change the date and time set on the switch. You must set the current date and time on the switch using this dialog box so the correct time stamps display in the **Event Log**, **Audit Log**, **Hardware Log**, **Link Incident Log**, and **Threshold Alerts Log**.

Procedure

Set the switch date and time using the following steps:

1. Select **Date/Time** from the **Configure** menu on the menu bar.

   The **Configure Date and Time** dialog box displays.

   If the **Periodic Date/Time Synchronization** check box in the **Configure Date and Time** dialog box is selected, the HAFM server periodically synchronizes the switch time to the HAFM server, and daylight savings time automatically updates. When the **Periodic Date/Time Synchronization** option is selected, the **Date** and **Time** fields are disabled (grayed out).

   If the **Periodic Date/Time Synchronization** check box is not selected, you can set the HAFM server date and time manually.
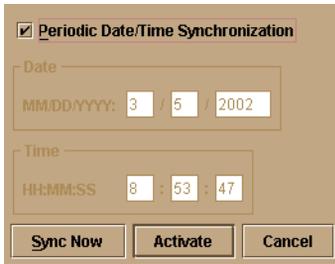
Figure 3–8: Configure Date and Time Periodic Synchronization dialog box

To disable **Periodic Date/Time Synchronization**, click the check box to remove the check mark, then click **Activate**. To re-enable **Periodic Date/Time Synchronization**, click the check box to display the check box, then click **Activate**.

NOTE: Click **Activate** to synchronize the date and time at the next update period. Click **Sync** *Now* to synchronize the date and time immediately.

2. Perform one of the following options:

   Option 1: To immediately synchronize the switch date and time with the HAFM server, click **Sync Now**. Make sure that a check mark is in the **Periodic Date/Time Synchronization** check box.

NOTE: If you click **Activate**, the date and time synchronize at the next update period.

   Option 2: To synchronize the switch date and time with a specific date and time that you enter:

   a. Make sure that **Periodic Date/Time Synchronization** is disabled (no check). Refer to Figure 3–9.
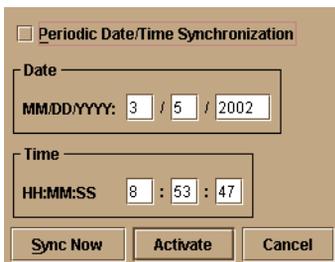
Figure 3–9: Configure date and time manually

   b. Click in a **Date** or **Time** field that you want to change.

    c. Delete characters and enter new ones as required or highlight the existing character by dragging the mouse cursor over the character and typing the new character.

NOTE: When entering the hours, use the range of 0 to 23, for minutes and seconds, use the range of 0 to 59.

    d. Click **Activate** to set the date and time on the switch.

3. If you are finished configuring the switch, back up the configuration data. For more information, refer to Backing Up and Restoring Configuration Data on page 3-29.

Configure Threshold Alerts

A threshold alert notifies users when the transmit (Tx) or receive (Rx) throughput reaches specified values for specific switch ports or port types, (E_Ports, F_Ports or FL_Ports).

You are notified of a threshold alert by:

- An attention indicator (yellow triangle) that displays on the port in the **Hardware View**.

- An attention indicator (yellow triangle) that displays in the **Alert** column of the **Port List View**.

   An attention indicator (yellow triangle) that displays by the **Threshold Alerts** field in the **Port Properties** dialog box.

- Detailed threshold alert data recorded in the **Threshold Alert Log**.

Use the **Threshold Alerts** option on the **Configure** menu to configure the following:

- Name for the alert.

- Type of threshold for the alert (Rx, Tx, or either).

- Active or inactive state of the alert.

- Threshold criteria:

  — Percent traffic capacity utilized. This is the percent of the port's throughput capacity achieved by the measured throughput. This setting constitutes the threshold value. For example the value of 50 means that the port's threshold is reached when throughput reaches 50% of port capacity.

  — Time interval during which throughput is measured and alert notification can occur.

  — The maximum cumulative time that throughput percentage can be exceeded during the set time interval before an alert is generated.

- Ports for which you are configuring threshold alerts.

You can configure up to 16 alerts, and any number of alerts can be active at one time.

Procedure

Use the following procedures to create a new threshold alert, or to modify, activate, deactivate, or delete an alert.

Create New Alert

1. Select **Threshold Alerts** from the **Configure** menu on the menu bar.

   The **Configure Threshold Alerts** dialog box displays.
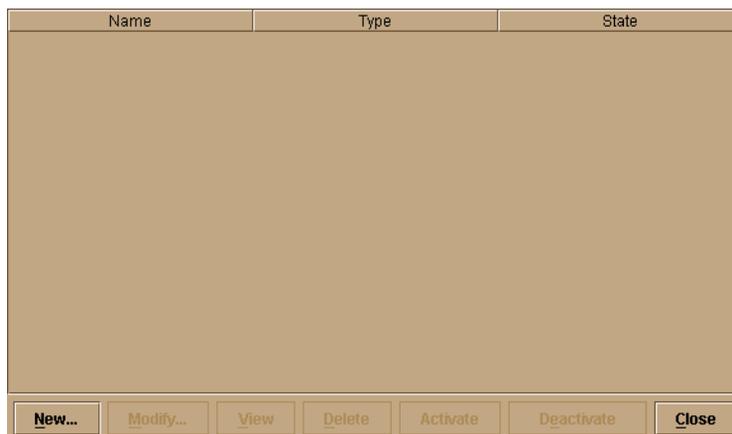
Figure 3–10: Configure Threshold Alerts dialog box

If alerts are configured, they will display in table format showing the name of the alert, type of alert (Rx, Tx, or Rx or Tx), and alert state (inactive or active).

2. Click **New**.

   The **New Threshold Alert** dialog box displays.

Figure 3–11: New Threshold Alerts dialog box - first screen

3. Enter a name from one to 64 characters in length. All characters in the ISO Latin-1 character set, excluding control characters, are allowed.

4. Select one of the following from the drop-down list under the **Name** field:

   — **Rx Throughput**. An alert will occur if the threshold set for receive throughput is reached.

   — **Tx Throughput**. An alert will occur if the threshold set for transmit throughput is reached.

   — **Rx or Tx Throughput**. An alert will occur if the threshold set for either receive or transmit throughput is reached.

5. Click **Next**.

   A new screen appears with additional parameters. The name configured for the alert appears at the top of the screen.

   (Click **Previous** if you need to return to the previous screen.)

Generate a Threshold Alert named "Port 15 Alert", if Tx Throughput reaches:

[15] % utilization

○ At any time

◉ For [4] cumulative minutes or more

during the [10] minute notification interval.

[<< Previous] [Next >>] [Finish] [Cancel]

Figure 3–12: New Threshold Alerts dialog box - second screen

6. Enter a percentage from 1 through 100 for **% utilization**. When throughput reaches this percentage of port capacity, a threshold alert will occur.

7. Enter the amount of cumulative minutes in which the **% utilization** should exist during the notification interval before an alert is generated. You can also select **At any time** if you want an alert to occur whenever the set **% utilization** is reached. The valid range is 1 to the interval set in step 8 (following).

8. Enter the interval in minutes in which throughput is measured and threshold notifications can occur. The valid range is 5 minutes to 70,560 minutes.

9. Click **Next**.

   A new screen appears for selecting ports for the alerts.
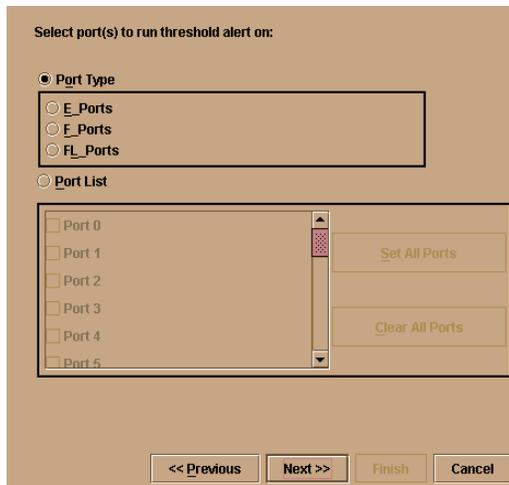
Figure 3–13: New Threshold Alerts dialog box - third screen

10. Either select Port Type or Port List.

   — If you select **Port Type**, selecting either E_Ports, F_Ports or FL_Ports will cause this alert to generate for all ports configured as E_Ports, F_Ports or FL_Ports respectively.

   — If you select **Port List**, you can select individual ports by clicking the check box by each port number or set all ports. Selecting **Set All Ports** places a check mark by each port number. Selecting **Clear All Ports** will clear the check marks by each port number.

11. Click **Next**.

   A final screen appears to provide a summary of your alert configuration. To make any changes, backwards and forwards through the configuration screens by selecting the **Previous** and **Next** buttons.
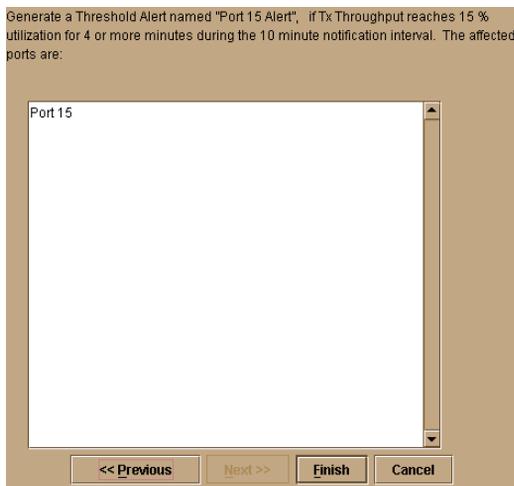
Figure 3–14: New Threshold Alerts dialog box - summary screen

12. Select **Finish**.

    The **Configure Threshold Alerts** dialog box appears listing the name, type, and state of the alert that you just configured.

13. At this point, the alert is not active. To activate the alert, select the alert information that displays in the **Configure Threshold Alerts** table and select **Activate**.
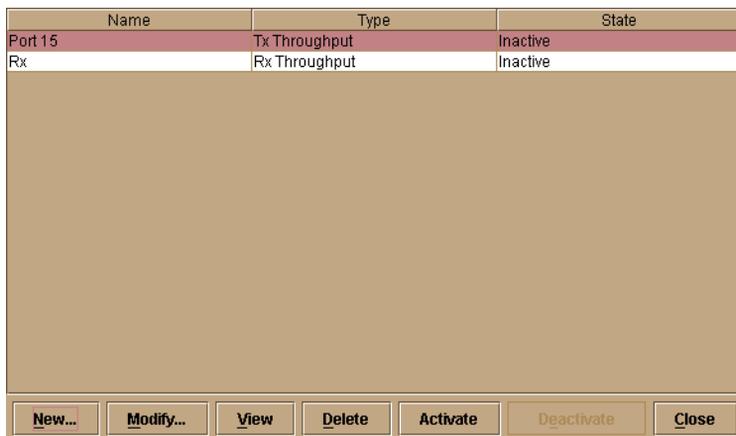
Figure 3–15: Configure Threshold Alerts dialog box - alert activated

Modify an Alert

Use the following steps to modify an existing threshold alert configuration.

1. Select **Threshold Alerts** from the **Configure** menu.

   The **Configure Threshold Alerts** dialog box displays.

2. Select the alert that you want to modify by clicking the alert information in the table.

3. If the alert is active, select **Deactivate**, then select the alert information in the table again.

4. Select **Modify**.

   NOTE: If the alert is active, an error message displays prompting you deactivate the alert.

   An initial **Modify Threshold** screen appears where you can change the threshold type.

5. Select a threshold type from the drop-down list.

6. Select **Next** when you are done. A **Modify Threshold** screen appears where you can change the % utilization, cumulative minutes for the threshold to occur before notification, and the time interval for measuring throughput and for alert notification.

7. Continue through the **Modify Threshold** screens until the summary screen appears displaying the alert configuration.

8. Perform either of the following steps:

   — If you need to change any parameters, select **Previous** and **Next** to display the desired **Modify Threshold** screen.

   — Select **Finish** when you are done.

Activate or Deactivate Alerts

Use the following steps to activate or deactivate existing threshold alerts. In the active state, notifications are generated for the alert. In the inactive state, notifications do not occur.

1. Select **Threshold Alerts** from the **Configure** menu.

   The **Configure Threshold Alerts** dialog box displays. The port's current state, deactive or active, is listed under the **State** column.

2. To change the state, select the alert by selecting the alert information in the table.

3. If the alert is active, select **Deactivate** to change to the deactive state. If the alert is deactive, select **Activate** to change to the active state.

Delete Alerts

Use the following steps to delete existing threshold alerts.

1. Select **Threshold Alerts** from the **Configure** menu.

   The **Configure Threshold Alerts** dialog box displays.

2. Select the alert that you want to delete by selecting the alert information in the table.

3. Select **Delete**.

   A message displays asking you to confirm the deletion.

4. Select Yes.

   The alert is removed from the dialog box.

Export Configuration Report

Use this option to save an ASCII file of all currently saved configuration data in switch NV_RAM to your hard drive or a diskette. Use any desktop publishing application to import this ASCII file for viewing or printing.

NOTE: This file cannot be used to set configuration parameters through the Product Manager.

Data in the file includes:

- Product identification

  Data input into the **Configure Identification** dialog box.

- Operating parameters

  Data input into the **Operating Parameters** dialog box.

- Port parameters

  Data input into the **Configure Ports** dialog box.

- SNMP parameters

  Data input into the **Configure SNMP** dialog box.

- Active zoning configuration

  This specifies the active zone and zone members, if set, and whether the default zone is enabled or disabled.

Procedure

To export a configuration report:

1. Select **Export Configuration Report** from the **Configure** menu on the menu bar.

   The **Export Configuration Report** dialog box displays.
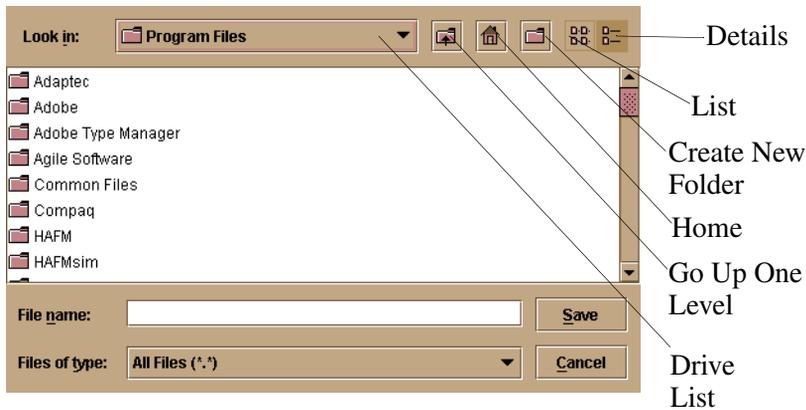
Figure 3–16: Export Configuration dialog box

2. Select the folder where you want to save the file.

3. Type in a file name and extension in the **File name** field.

4. Click **Save**.

   The file saves to the specified folder as an ASCII text file.

Enable Web Server

Select this option from the **Configure** menu on the menu bar to place a check mark in the check box to enable the Embedded Web Server interface on the switch. Select the option again to remove the check mark and disable the Embedded Web Server interface. When enabled, users at remote workstations cannot access the interface. If enabled, HP recommends changing the user names and/or passwords from the default values to prevent unauthorized access.

Enable Telnet

Select this option from the **Configure** menu on the menu bar to place a check mark in the check box to enable telnet access to the switch. Select the option again to remove the check mark and disable telnet access. When disabled, users at remote workstations cannot access the switch through telnet to use the Command Line Interface (CLI) or perform other tasks. When enabled, users at remote workstations cannot access the interface. If enabled, HP recommends changing the user names and/or passwords from the default values to prevent unauthorized access.

Backing Up and Restoring Configuration Data

You can back up the NV-RAM configuration, which includes all of the data you input through instructions in this chapter, using the **Backup and Restore Configuration** option. This option is available through the **Maintenance** menu. Selecting this option backs up the configuration data to a file on the HAFM server hard drive. The restore function writes this data back to NV-RAM on the switch. Using the restore function overwrites the existing configuration. For more information, refer to Backup and Restore Configuration on page 5-6.

In addition to the **Backup and Restore Configuration** option, the Iomega QuikSync application backs up configuration and other critical data from the HAFM server automatically. As long as a Zip disk remains in the Zip drive of the HAFM server, data backs up to the Zip disk whenever the directory contents change or you reboot the HAFM server. For more information, refer to Backup and Restore Configuration on page 5-6.

NOTE: We do not recommend changing the default QuikSync settings.

4

Using Logs

This chapter describes the Edge Switch 2/24 logs that you can access through the **Logs** menu on the Product Manager menu bar.

Using Logs

The Audit, Event, Hardware, Link Incident, and Threshold Alert logs store up to 1000 entries each. The most recent entry displays at the top of the log. After 1000 entries are stored, new entries overwrite the oldest entries.

Button Function

Button function is the same for all logs:

- **Clear**

  Clicking **Clear** clears all entries in the log for all users. A **Warning** dialog box displays requesting confirmation that you want to clear all entries in the log.

- **Refresh**

  Clicking **Refresh** reads the current data and refreshes the screen with the new display.

- **Close**

  Closes the log and displays the switch Product Manager window.

- **Export**

  Clicking **Export** on a log window displays the **Save** dialog box shown in Figure 4–1 on page 4-2. Click the **Home** icon to return to the files in your home directory. The folders that list in the display area of the **Save** dialog box after clicking the **Home** icon are those that are stored in your home directory. If you choose, you may create a folder for your home directory and save the file there.

To save a log file in American Standard Code for Information Exchange (ASCII) format to a location on your system's hard drive or to a diskette, use the following steps. You can open this file in any desktop publisher for viewing or printing.

Figure 4–1: Save dialog box

1. Click **Export** on the log window.

2. In the **Save** dialog box, select the folder where you want to save the file.

3. Type in a file name and extension in the **File name** field.

4. Click **Save**.

The file saves to the specified folder as an ASCII text file.

Expanding Columns

Expand columns in logs by placing the cursor over the line separating column headings until a double arrow appears, then click and drag to widen the column as necessary.

Sorting Entries

Sort log entries in columns by clicking a column heading. A down arrow displays in the heading, if sorting alphabetically in descending order. An up arrow indicates sorting in ascending order. Click once to sort. Click again to reverse the sort.

Audit Log

The Audit Log displays a history of all configuration changes applied to the switch from any source such as Product Manager, SNMP management stations, web server interface, host, or another switch.

Date/Time	Action	Source	Identifier
11/19/02 2:40:57 PM	Date/Time changed by automatic synchronization	HAFM	@16.117.74.207
11/14/02 8:01:35 PM	Zone Set disabled	HAFM	Administrator@16.117.100.95
11/14/02 6:18:42 PM	Zone Set enabled	HAFM	Administrator@16.117.100.95
11/14/02 4:44:27 PM	Zone Set enabled	Web Server	16.117.100.95
11/14/02 4:34:18 PM	Default Zone disabled	HAFM	Administrator@16.117.100.95
11/9/02 12:37:24 AM	Date/Time changed by automatic synchronization	HAFM	@16.117.74.207
11/8/02 6:42:53 PM(HAFM)	Call home enabled	HAFM	Administrator@16.117.74.207
11/8/02 11:39:13 PM	Switch Name changed	HAFM	Administrator@16.117.74.207
11/8/02 11:38:41 PM	Rerouting delay enabled	HAFM	Administrator@16.117.74.207
11/8/02 11:38:32 PM	Switch Contact changed	HAFM	Administrator@16.117.74.207
11/8/02 11:38:32 PM	Switch Location changed	HAFM	Administrator@16.117.74.207
11/8/02 11:38:32 PM	Switch Name changed	HAFM	Administrator@16.117.74.207
11/8/02 11:37:06 PM	Switch gateway address changed	Maintenance Port	
11/8/02 11:37:06 PM	Switch subnet mask changed	Maintenance Port	
11/8/02 11:37:06 PM	Switch IP Address changed	Maintenance Port	

Figure 4–2: Audit Log

- **Date/Time**

  The date and time of the change on the switch.

  Some actions, such as backing up configuration data and enabling automatic date/time synchronization, are performed only by the HAFM server without switch interaction. These actions are indicated by the string, (HAFM), following the Audit Log's stamp of the HAFM server's date and time (refer to Figure 4–2). If the string, (HAFM), is not displayed, the time stamp is from the switch.

- **Action**

  User action that caused the configuration change, such as offline status, port name change, or change of address.

- **Source**

  Identifies the user making the change through the switch Product Manager and IP or DNS host name address of the remote user's workstation.

  — Maintenance Port: Change was made by a user connected to the maintenance port.

  — HAFM: Change was made by an Product Manager user.

  — SNMP: Change was made by a remote SNMP management station.

— Fabric: Change was initiated by another switch in the fabric that is not managed by this HAFM server.

— Web server: Change was made by a user through the Embedded Web Server interface.

— Fibre Channel Host: Change was made inband by a Fibre Channel host through the Open Systems Management Server.

— Telnet: Change was made through a telnet connection.

- **Identifier** - Identifies the user making the change according to the source:

— Maintenance Port: No entry displays.

— HAFM: Includes user@address, where "user" is the Product Manager user name and "address" is the network address of the workstation (remote user workstation or HAFM server).

— SNMP: Contains the network address of the SNMP management station.

— Fabric: No entry displays.

— Web Server: The Identifier column contains user@address, where "user" is the web server user name and "address" is the network address of the web user.

— Fibre Channel Host: No entry displays.

— Telnet: Change was made through a telnet connection.

Event Log

The Event Log provides a record of significant events that have occurred on the switch, such as hardware failures, degraded operation, and port problems.

Date/Time	Event	Description	Severity	FRU-Position	
11/26/02 9:32:11 AM	510	SFP optics hot insertion initiated.	Informational	CTP-0	09 FF FF FF 2F FD 38 AA FF FF FF FF FF F
11/26/02 9:32:00 AM	513	SFP optics hot removed	Informational	CTP-0	09 FF FF FF 2F FD 0C 12 FF FF FF FF FF F
11/17/02 4:49:07 AM	410	CTP card reset.	Informational	CTP-0	00
11/8/02 11:33:36 PM	203	Power supply AC voltage recovery.	Informational	PWR-1	
11/8/02 11:33:26 PM	200	Power supply AC voltage failure.	Major	PWR-1	
11/8/02 11:33:23 PM	410	CTP card reset.	Informational	CTP-0	00

Figure 4–3: Event Log

All detected firmware faults and hardware failures are sent to the HAFM server for recording in the Event Log. The log provides a maximum of 1000 log entries before it wraps and overwrites the oldest entries.

For detailed information on event data and problem resolution, refer to the *hp StorageWorks edge switch 2/24 service manual*.

Each log entry includes the following:

- **Date/Time**

  The date and time of the event on the switch.

- **Event**

  Events are identified by a unique code.

  Event codes include:

000 - 199	System events
200 - 299	Power supply events
300 - 399	Fan module events
400 - 499	CTP events
500 - 599	Port events
800 - 899	Thermal events

- **Description**

  A short description of the event.

- **Severity**

  There are four classifications of severity that identify the importance of the event.

  — Informational

  — Minor

  — Major

  — Severe

- **FRU Position**

  The FRU involved in the event and the slot position in the chassis relative to identical FRUs installed.

- **Event Data**

  Up to 32 bytes of supplementary information for the event in hexadecimal format. For detailed information on event data and problem resolution, refer to the *hp StorageWorks edge switch 2/24 service manual*.

Hardware Log

The Hardware Log displays information on field replaceable units (FRUs) inserted and removed from the switch.

Date/Time	FRU	Position	Action	Part Number	Serial Number
2/14/02 9:09:18 AM	GSF2	1	Inserted	470-000396-201	121234561
2/14/02 9:09:18 AM	GSF2	0	Inserted	470-000396-201	121234560
2/14/02 9:09:18 AM	GXXL	13	Removed	470-000396-222	1012345613
2/14/02 9:09:18 AM	GSML	12	Removed	470-000396-201	912345612
2/14/02 9:09:18 AM	GLSL	11	Removed	470-000396-201	812345611
2/14/02 9:09:18 AM	GXXR	10	Removed	470-000396-201	1512345610
2/14/02 9:09:18 AM	GSMR	9	Removed	470-000396-201	141234569
2/14/02 9:09:18 AM	GLSR	8	Removed	470-000396-201	131234568
2/14/02 9:09:18 AM	GLSR	7	Removed	470-000396-222	131234567
2/14/02 9:09:18 AM	GLSR	6	Removed	470-000396-222	131234566

Export...   Clear   Refresh   Close

Figure 4–4: Hardware Log

Each log entry includes the following:

- **Date/Time**

  Date and time of the insertion or removal of the FRU.

- **FRU**

  The name of the inserted or removed FRU.

FAN	Fan module
PWR	Power supply module
SFP	SFP transceiver.
CTP	CTP card. Note that the CTP card is not a FRU. If it fails, the switch must be replaced.

- **Position**

  Slot position in the chassis relative to identical components installed.

- **Action**

  Inserted or removed.

- **Part Number**

  Part number of the component.

- **Serial Number**

  Serial number of the component.

Link Incident Log

The Link Incident Log displays a thousand of the most recent link incidents with the date each incident occurred, the time it occurred, and the port where it took place.

Date/Time	Port	Link Incident
3/31/02 12:21:56 PM	23	Loss-of-Signal or Loss-of-Synchronization.
3/22/02 4:09:11 PM	23	Not Operational primitive sequence (NOS) received.
3/22/02 4:09:11 PM	3	Not Operational primitive sequence (NOS) received.
3/22/02 4:07:38 PM	3	Not Operational primitive sequence (NOS) received.
3/22/02 4:07:10 PM	3	Loss-of-Signal or Loss-of-Synchronization.
3/22/02 3:06:09 PM	3	Not Operational primitive sequence (NOS) received.
3/22/02 3:06:09 PM	23	Not Operational primitive sequence (NOS) received.
3/21/02 4:34:52 PM	3	Loss-of-Signal or Loss-of-Synchronization.
3/21/02 4:30:11 PM	7	Not Operational primitive sequence (NOS) received.
3/21/02 4:29:13 PM	7	Loss-of-Signal or Loss-of-Synchronization.
3/21/02 4:19:41 PM	3	Not Operational primitive sequence (NOS) received.
3/21/02 3:47:51 PM	23	Not Operational primitive sequence (NOS) received.
3/21/02 10:28:38 AM	15	Not Operational primitive sequence (NOS) received.
3/21/02 10:28:28 AM	23	Loss-of-Signal or Loss-of-Synchronization.
3/21/02 10:27:03 AM	15	Loss-of-Signal or Loss-of-Synchronization.

| Export... | Clear | Refresh | Close |

Figure 4–5: Link Incident Log

Each log entry contains:

- **Date/Time**

  The date and time of the incident.

- **Port**

  The number of the port on which the incident occurred.

- **Link Incident**

  A short description of the incident. The following events may cause a link incident to be written to the log.

  — Implicit incident.

    The attached node detects a condition that may cause problems on the link.

    — Bit-error threshold exceeded.

    The number of code violation errors has exceeded threshold.

  — Loss-of-signal or loss-of-synchronization.

    This occurs if a cable is unplugged from an attached node.
    Loss-of-synchronization condition has persisted for longer than the resource allocation time out value (R_A_TOV).

— Not-operational (NOS) primitive sequence received. A NOS was recognized.

— Primitive sequence timeout.

   • Link reset protocol timeout occurred.

   • Timeout occurred for an appropriate response while in NOS receive state and after NOS is no longer recognized.

— Invalid primitive sequence received for the current link state.

   Either a link reset or a link reset response primitive sequence was recognized while waiting for the offline sequence.

Threshold Alert Log

This log provides details of threshold alert notifications. Besides the date and time that the alert occurred, the log also displays details about the alert as configured through the **Configure Threshold Alert(s)** option under the **Configure** menu.

Date/Time	Name	Port	Type	Utilization %	Alert Time	Interval
10/24/01 2:19:38 PM	a test	7	Rx Throughput	1	0	5
10/24/01 2:19:37 PM	a test	15	Rx Throughput	1	0	5
10/24/01 2:14:38 PM	a test	7	Rx Throughput	1	0	5
10/24/01 2:14:36 PM	a test	15	Rx Throughput	1	0	5
10/24/01 2:09:38 PM	a test	7	Rx Throughput	1	0	5
10/24/01 2:09:36 PM	a test	15	Rx Throughput	1	0	5
10/24/01 2:04:38 PM	a test	7	Rx Throughput	1	0	5
10/24/01 2:04:36 PM	a test	15	Rx Throughput	1	0	5
10/24/01 1:59:38 PM	a test	7	Rx Throughput	1	0	5
10/24/01 1:59:36 PM	a test	15	Rx Throughput	1	0	5
10/24/01 1:54:37 PM	a test	7	Rx Throughput	1	0	5
10/24/01 1:54:36 PM	a test	15	Rx Throughput	1	0	5
10/24/01 1:49:37 PM	a test	7	Rx Throughput	1	0	5
10/24/01 1:49:36 PM	a test	15	Rx Throughput	1	0	5
10/24/01 1:44:37 PM	a test	7	Rx Throughput	1	0	5
10/24/01 1:44:36 PM	a test	15	Rx Throughput	1	0	5
10/24/01 1:39:36 PM	a test	7	Rx Throughput	1	0	5
10/24/01 1:39:35 PM	a test	15	Rx Throughput	1	0	5
10/24/01 1:34:36 PM	a test	7	Rx Throughput	1	0	5
10/24/01 1:34:35 PM	a test	15	Rx Throughput	1	0	5
10/24/01 1:29:35 PM	a test	15	Rx Throughput	1	0	5
10/24/01 1:29:35 PM	a test	7	Rx Throughput	1	0	5
10/24/01 1:24:34 PM	a test	15	Rx Throughput	1	0	5
10/24/01 1:24:34 PM	a test	7	Rx Throughput	1	0	5
10/24/01 1:19:34 PM	a test	15	Rx Throughput	1	0	5
10/24/01 1:19:34 PM	a test	7	Rx Throughput	1	0	5
10/24/01 1:14:34 PM	a test	15	Rx Throughput	1	0	5

Export... Clear Refresh Close

Figure 4–6: Threshold Alert Log

- **Date/Time**

  Date and time stamp for when the alert occurred.

- **Name**

  Name for the alert as configured through the **Configure Threshold Alerts** dialog box.

- **Port**

  Port number where the alert occurred.

- **Type**

  The type of alert: transmit (Tx) or receive (Rx).

- **Utilization %**

  Percent usage of traffic capacity. This is the percent of the port's throughput capacity achieved by the measured throughput. This setting constitutes the threshold value and is configured through the **Configure Threshold Alerts** dialog box. For example, a value of 25 means that threshold occurs when throughput reaches 25 percent of the port's capacity.

- **Alert Time**

  The maximum cumulative time that the throughput threshold percentage must exist before an alert is generated.

- **Interval**

  The time interval during which the throughput is measured and an alert can generate. This is set through the **Configure Threshold Alerts** dialog box.

5

Using Maintenance Features

This chapter describes how to use the options that display from the **Maintenance** menu on the Product Manager menu bar.

Run Port Diagnostics

The **Port Diagnostics** option enables you to run internal and external loopback tests on any port. To use this option, follow the detailed steps in the *hp StorageWorks edge switch 2/24 service manual*.

Collect Maintenance Data

The **Data Collect** option enables you to collect maintenance data that can help support personnel diagnose system problems. Save this data to a zip file on a Zip disk (or other medium with the appropriate capacity), and forward it to technical support personnel.

To use this option, follow the detailed steps in the *hp StorageWorks edge switch 2/24 service manual*.

Execute an IPL

> ⚠ **CAUTION:** The Ethernet connection between the HAFM server and switch is interrupted momentarily during an IPL.

> ⚠ **CAUTION:** An initial program load (IPL) is not intended for ordinary or casual use and should only be performed if the control processor (CTP) card is suspected to be faulty. Do not use this option unless directed by your support representative or if you need to reset a failed CTP card. An IPL will disrupt port operations. Before using this option, make sure administrators of device(s) attached to ports quiesce Fibre Channel traffic through the switch and take the device offline. Note that the CTP card is not a FRU. If it fails, the switch must be replaced.

If it is necessary for you to execute an IPL on the switch, use the following steps:

1. Select **IPL** from the **Maintenance** menu on the menu bar.

   A dialog box displays confirming the IPL.

Figure 5–1: IPL Confirmation dialog box

2. Click **Yes**.

Selecting **IPL** from the **Maintenance** menu causes Ethernet connection between the switch and HAFM server to drop momentarily and the following to occur in the Product Manager window:

- As the network connection drops, the switch **Status** table on the **Hardware View** turns yellow.

- The **Status** field in the table displays "No Link" and the **State** field displays the reason for no link.

- A grey square displays in the status bar. Refer to Table 1–1 on page 1-30 for an explanation of this status bar display.

- The FRUs illustrated in the **Hardware View** do not display. They display again as the connection is re-established.

An IPL initiates the following functions in the switch:

- Restarts the operational firmware on the CTP card, executes abbreviated power on system tests (POSTs) and then, if no POST errors are encountered, the switch resumes the active role that it had before the IPL. Note that the CTP card is an internal component and is not a FRU.

- Resets the Ethernet interface on the CTP card, causing the connection to the HAFM server to drop momentarily. The status symbol for the switch in the Product View will change to a gray square until the connection is re-established.

- Stops normal switching functions for ports (functions resume after the IPL).

After the IPL:

- All Fabric services databases containing information about current Fabric logins, name server registrations, and other data remain intact, making the operation transparent to attached devices.

- The switch returns to the online state, even if it was offline before the operation.

- All ports configured as blocked will remain blocked.

- Modifications made to an active zone set configuration that have not been enabled will be automatically enabled.

Set Online State

Use the procedure in this section to display the current switch operating state (offline or online) and change the state as required.

> ⚠ **CAUTION:** Before setting the switch offline, warn administrators and users currently operating devices that are attached to the switch that it is going offline and that there will be a disruption of communications. Make sure administrators of device(s) attached to ports quiesce Fibre Channel traffic through the switch.
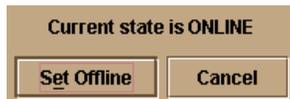
To set the switch online or offline (depending on current state), use the following steps:

1. Right-click on the switch in the **Hardware View** and select **Set Online State** in the menu, or select **Set Online State** from the **Maintenance** menu on the menu bar.

   One of the following dialog boxes displays, depending on the current operating state.

Figure 5–2: Set Online State dialog box (Offline)

Figure 5–3: Set Online State dialog box (Online)

2. Click **Set Offline** or **Set Online**, depending on the operating state you want to set.

3. When a warning box displays requesting you to confirm the offline or online state, click **OK**.

As the switch goes offline, "OFFLINE" displays in the **State** field of the **Switch Status** table in the **Hardware View**. LED indicators on all ports with attached devices stay green, but the switch is sending offline sequences (OLSs) to these devices.

Manage Firmware Versions

Firmware refers to the internal operating code for the switch. You can maintain up to eight firmware versions on the HAFM server for downloading to an switch. To use the **Firmware Library** option to manage firmware versions, follow the steps in the *hp StorageWorks edge switch 2/24 service manual.*

Enable E-Mail Notification

E-mail addresses and the simple mail transfer protocol (SMTP) server address for e-mail notification of switch events must be configured through the HAFM application. Refer to the *hp StorageWorks ha-fabric manager user guide* for instructions on configuring e-mail.

NOTE: E-mail recipients are configured in the HAFM through the **Configure E-Mail** dialog box. A valid SMTP address is configured in this dialog box.

Use the **Enable E-Mail Notification** function on the Product Manager to enable e-mail notification for events that occur on a selected switch. The default state is disabled.

To enable e-mail notification, use the following steps:

1. Select **Enable E-Mail Notification** from the **Maintenance** menu on the menu bar.

2. To enable e-mail notification, select the option to add a check mark to the check box.

3. To disable e-mail notification, select the option to remove the check mark from the check box.

Enable Call-Home Notification

The call-home feature enables the HAFM server to automatically dial out to a support center to report system problems. The support center server accepts calls from the HAFM server, logs reported events, and notifies one or more support center representatives.

You must enable Call-Home Event Notification through the StorageWorks HAFM application Maintenance Menu before enabling this function through the Product Manager for individual Edge Switches. Two call-home options are available but only one can be used when HAFM is installed:

- In legacy HP environments, call-home notification for directors and switches requires installation of Proactive Service software. This service is offered at no additional charge for subsystems covered under an on-site warranty or on-site storage hardware support contract. To register or order Proactive Services software, contact your HP customer service representative.

- In classic HP environments, configure telephone numbers and other information for the call-home feature through the Windows dial-up networking application. Refer to the *hp StorageWorks HAFM server installation guide* for details.

Use the **Enable Call Home Notification** function on the Product Manager to enable call-home notification for events that occur on the selected switch. The default state is disabled.

To enable call-home notification for system problems, use the following steps:

1. Select **Enable Call Home Notification** from the **Maintenance** menu on the menu bar to enable and disable call-home notification.

   A check mark displays next to the menu option to indicate that call-home notification is enabled.

2. Click the check box to add or remove the check mark.
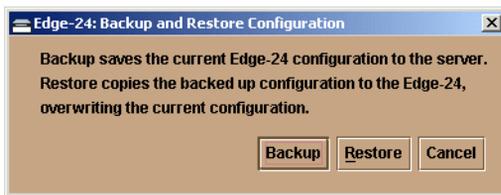
Backup and Restore Configuration

Select this option from **Maintenance** menu to save the product configuration stored on the switch to the HAFM server hard disk or to restore the product configuration from the HAFM server. Only a single copy of the configuration is kept on the server.

The purpose of the back up is primarily for restoring configuration data to a replacement switch. You can also use this feature for a special purpose configuration or for temporary testing of a configuration. You cannot modify the location and file name of the saved configuration.

NOTE: You can only restore the configuration to a switch with the same IP address.

Backup

1. Select **Backup and Restore Configuration** from the **Maintenance** menu on the menu bar to display the **Backup and Restore Configuration** dialog box.

Figure 5–4: Backup and Restore dialog box

The **Backup and Restore** dialog box consists of a short description of the features performed when you select **Backup** or **Restore**.

Following is a list of configurations that are backed up to the HAFM server:

- Identification data (switch name, description, and location).

- Port configuration data (port names, blocked states, and extended distance settings).

- Operating parameters for fabric (E_D_TOV, R_A_TOV, switch priority, interop mode) and for switch (preferred domain ID, rerouting delay, and domain RSCNs).

- SNMP configuration (trap recipients, community names, and write authorizations).

- Zoning configuration (active zone set and default zone state).

2. To back up data, click **Backup**.

3. When the dialog box appears confirming that the back up of configuration is complete, click **OK**.

    If the back up fails, a dialog box displays to inform you that the back up to the server failed.

Restore

1. Set the switch offline before performing the restore function. For instructions, refer to Set Online State on page 5-3.

2. Click **Restore** on the **Backup and Restore Configuration** dialog box to restore the backed up configuration to the nonvolatile random access memory (NV-RAM) on the switch.

    Set the switch to offline before performing the restore function. If you select **Restore** and the switch is online, a message dialog displays requesting that you turn the switch offline. No action takes place when you close the dialog box. For instructions on setting the switch offline or online, refer to Set Online State on page 5-3.

    If the switch is already offline and you click **Restore**, a confirmation dialog box displays indicating that the restore will overwrite any existing configuration already on the switch. The dialog box also displays the date of the restored back up. Click **OK**

    Note that the restore operation initiates an IPL.

3. Set the switch back online when the restore completes.

Reset Configuration

NOTE: You must have maintenance authorization rights to access this feature.

This option resets all configuration data input through options in the **Configure** menu, zoning configurations, and switch addressing to factory-default values. Since the current IP address for the switch may not match the factory default address, the Ethernet link between the switch and the service processor may drop and not reset. Before using this option, record the switch's current IP address which displays below the switch's icon in the HAFM's Product View (view **Display Options** set to **Network Address**). You can also find the current IP address through the Embedded Web Server interface.

After resetting the configuration, you must reset the original address on the switch through the maintenance port or the Embedded Web Server interface to maintain LAN connections and communication with the service processor.

Procedure

1. Set the switch offline. For instructions, refer to .

2. Select **Reset Configuration** from the **Maintenance** menu on the menu bar. The following warning displays:

> ⚠ **WARNING: This operation will reset all switch configuration data and non-volatile settings to factory default values. All optional features will also be disabled. The switch must be offline to continue.**

NOTE: If you have enabled features that add additional port function since the switch was shipped from the factory, these features will be disabled (factory default) when the configuration is reset. Only those ports that were enabled at the factory will function. You will have to enable the additional port function features again through the **Configure Feature Key** dialog box.

Factory-default values may vary, depending on the firmware release installed in your switch. For a list of values, refer to the *hp StorageWorks edge switch 2/24 service manual*.

6

Optional Features

This chapter provides detailed information on using, administering, and configuring optional features through High Availability Fabric Manager application.

- "Keyed" features, requiring feature keys to be purchased and enabled through the **Configure Feature Key** dialog box in the product's Product Manager application.

- Features not requiring feature keys themselves, but requiring that specific keyed features be enabled before they can be accessed through HAFM or Product Manager applications

Configure Open Systems Management Server

Use these procedures to configure the open systems inband management program to function with the switch.

The optional Open Systems Management Server feature must be enabled in order to perform this procedure.

Procedure

To configure the Open Systems Management Server, use the following steps:

1. Select **Management Server** from the **Configure** menu on the menu bar.

   The **Configure Open Systems Management Server** dialog box displays.

2. Enable the management server by clicking the **Enable Management Server** check box to add a check mark. (To disable the management server, click the check box again to remove the check mark.)

3. Click the check box in the **Host Control Prohibited** field to display a check mark and prohibit a host management program from changing configuration and connectivity parameters on the switch. In this case, the host program has read-only access to configuration and connectivity parameters. Clicking the check box when it contains a check mark removes the check mark and allows a host program to change configuration and connectivity parameters on the switch.

4. Activate changes and close the dialog box by clicking **Activate**.

5. If you are finished configuring the switch, you can back up the configuration data. For more information, refer to Backup and Restore Configuration on page 5–6.

SANtegrity Features

SANtegrity includes a set of features that enhance security in Storage Area Networks that contain a large and mixed group of fabrics and attached devices. Through these features you can allow or prohibit switch attachment to fabrics and device attachment to switches. These features are enabled by purchasing a feature key, then enabling the key through the **Configure Feature Key** dialog box. For general instructions in enabling a feature key, refer to Configure Feature Key on page 3–15.

SANtegrity features include:

• Fabric Binding

• Switch Binding

Enterprise Fabric Mode - Although this is not a keyed feature the SANtegrity Fabric Binding and Switch Binding must be installed before you can use Enterprise Fabric Mode function through the HAFM **Fabrics** menu.

Fabric Binding

This feature is managed through the Fabric Binding option, available through the **Fabrics** menu in the HAFM when the **Fabrics** tab is selected. Using Fabric Binding, you can allow specific switches to attach to specific fabrics in the SAN. This provides security from accidental fabric merges and potential fabric disruption when fabrics become segmented because they cannot merge.

Enable/Disable and Online State Functions

In order for Fabric Binding to function, specific operating parameters and optional features must be enabled. Also, there are specific requirements for disabling these parameters and features when the Director or Edge Switch is offline or online. Be aware of the following:

- Because switches are bound to a fabric by world wide name (WWN) and domain ID, the Insistent Domain ID option in the **Configure Switch Parameters** dialog box is automatically enabled if Fabric Binding is enabled. You cannot disable Insistent Domain ID while Fabric Binding is active and the switch is online.

- If Fabric Binding is enabled and the switch is online, you cannot disable Insistent Domain ID.

- If Fabric Binding is enabled and the Director or Edge Switch is offline, you can disable Insistent Domain ID, but this will disable Fabric Binding.

- You cannot disable Fabric Binding or Switch Binding if Enterprise Fabric Mode is enabled. However, if Enterprise Fabric Mode is disabled, you can disable Fabric Binding, Switch Binding, or both.

For More Information

To enable, disable, and configure this option, refer to the Fabric Binding section of Chapter 8, "Optional Features," in the *hp StorageWorks ha-fabric manager user guide*.

Switch Binding

This feature is managed through the **Switch Binding** submenu options available on the Product Manager **Configure** menu. Using Switch Binding, you can specify devices and switches that can attach to switch ports. This provides security in environments that include a large number of devices by ensuring that only the intended set of devices attach to a Edge Switch or Director.

Configuring Switch Binding - Overview

To configure switch binding, you must first activate the feature using the **Switch Binding State Change** dialog box while selecting the type of port where you want to restrict connection (connection policy). Possible selections are E_Ports, F_Ports, or all types.

If the switch is online, activating switch binding populates the Membership List in the **Switch Binding - Membership List** dialog box (Product Manager) with the following WWNs currently connected to the switch, depending on the connection policy set in the **State Change** dialog box:

• WWNs of devices connected to F_Ports (F_Port connection policy). The WWN is the WWN of the attached device's port.

• WWNs of switches connected to E_Ports (E_Port connection policy). The WWN is the WWN of the attached switch.

• WWNs of devices connected to F_Ports and switches connected to E_Ports (all-ports connection policy).

Note the following:

• When the Switch Binding feature is first installed and has not been enabled, the Switch Membership List is empty. When you enable Switch Binding, the Membership List is populated with WWNs of devices, switches, or both that are currently connected to the switch.

• If the Edge Switch is offline and you activate switch binding, the Membership List is not automatically populated.

• Edits to the Switch Binding Membership List will be maintained when you enable or disable Switch Binding.

After enabling Switch Binding, you prohibit devices and/or switches from connecting with switch ports by removing them from the Membership List in the **Switch Binding Membership List** dialog box. You allow connections by adding them to the Membership List. You can also add detached nodes and switches as well.

Enable/Disable Switch Binding

1. Select the **State Change** option from the **Configure** menu's **Switch Binding** submenu. The **Switch Binding State Change** dialog box displays.

2. Perform one of the following steps:

• To disable Switch Binding (a check mark appears in the **Enable Switch Binding** check box), click the **Enable Switch Binding** check box to remove the check mark, then click **Activate**.

• To enable Switch Binding (check mark is not in the **Enable Switch Binding** check box), click the **Enable Switch Binding** check box to add a check mark. Go on to step 3 to set the Connection Policy.

3. Click one of the **Connection Policy** radio buttons.

- **Restrict E_Ports**. Select if you want to restrict connections from specific switches to Director E_Ports. Switch WWNs can be added to the Switch Membership List to allow connection and removed from the Membership List to prohibit connection. Devices are allowed to connect to any F_Port.

- **Restrict F_Ports**. Select if you want to restrict connections from specific devices to Director F_Ports. Device WWNs can be added to the Switch Membership List to allow connection and removed from the Membership List to prohibit connection. Switches are allowed to connect to any E_Port.

- **Restrict All**. Select if you want to restrict connections from specific devices to Director F_Ports and Edge Switches to Edge Switch E_Ports. Device and switch WWNs can be added to the Switch Membership List to allow connection and removed from the Membership List to prohibit connection.

4. Click **Activate** to enable the changes and close the dialog box.

5. Edit the Switch Membership List through the **Switch Binding Membership List** dialog box to add or remove switches and devices that are allowed to connect with the switch. Refer to following section for procedures.

Editing the Switch Membership List

1. Select the **Edit Membership List** option from the **Configure** menu's **Switch Binding** submenu in the Product Manager. The **Switch Binding Membership List** dialog box displays. The WWNs of devices and/or switches that can currently connect to switch ports are listed in the **Switch Membership List** panel.

NOTE: Refer to Configuring Switch Binding - Overview on page 6–3 for information on how the Switch Membership List is populated with WWNs according to options set in the *Switch Binding State Change* dialog box.

2. If nicknames are configured for WWNs through the HAFM and you want these to display instead of WWNs in this dialog box, click the **Display Options** button at the bottom of the dialog box. When the **Display Options dialog box** displays, click **Nickname**, then **OK**.

3. To prohibit connection to a switch port from a WWN currently in the Membership List, click the WWN or nickname in the Membership List, then click the **Remove** button. The WWN or nickname will move to the **Node List** panel. WWNs can only be removed from the fabric if any of the following is true:

- The switch is offline.

- Switch Binding is disabled.

- The switch or device with the WWN is not connected to the switch.

- Switch Binding is not enabled for the same port type as enabled for the Connection Policy in the **Switch Binding State Change** dialog box. For example, a WWN for a switch attached to an E_Port can be removed if the Switch Binding Connection Policy was enabled to Restrict F_Ports.

- The switch or device with the WWN is connected to a port that is blocked.

- The switch or device with the WWN is not currently connected to the Director (detached node).

4. WWNs can be added to the Switch Membership List (and thereby allowed connection) when Switch Binding is either enabled or disabled. To allow connection to a switch port from a WWN in the **Node List** panel, select the WWN or nickname in the **Node List** panel, click the **Add** button. The WWN or nickname will move to the **Membership List** panel.

5. To add a WWN for a device or switch not currently connected to the Director, click the **Detached Node** button. When the **Add Detached Node** dialog box appears, enter the appropriate WWN or nickname (if configured through the HAFM) and click **OK**. The WWN or nickname appears in the Switch Membership List.

6. Click **Activate** to enable the changes and close the dialog box.

Enable/Disable and Online State Functions

In order for Switch Binding to function, specific operating parameters and optional features must be enabled. Also, there are specific requirements for disabling these parameters and features when the Director or Edge Switch is offline or online. Be aware of the following:

- Switch Binding can be enabled or disabled whether the Edge Switch is offline or online.

- Enabling Enterprise Fabric Mode automatically enables Switch Binding.

- You cannot disable Switch Binding if Enterprise Fabric Mode is enabled.

- If Enterprise Fabric Mode is enabled and the Director or Edge Switch is online, you cannot disable Switch Binding. However, if Enterprise Fabric Mode is disabled, you can disable Fabric Binding, Switch Binding, or both.

- If Enterprise Fabric Mode is enabled and the Director or Edge Switch is offline you can disable Switch Binding, but Enterprise Fabric Mode will also disable.

- WWNs can be added to the Switch Membership List when Switch Binding is enabled or disabled.

- WWNs can only be removed from the Switch Membership List if any of the following are true:

  — The switch is offline.

  — Switch Binding is disabled.

  — The switch or device with the WWN is not connected to the switch.

  — Switch Binding is not enabled for the same port type as enabled for the Connection Policy in the **Switch Binding State Change** dialog box. For example, a WWN for a switch attached to an E_Port can be removed if Switch Binding Connection Policy was enabled to Restrict F_Ports.

  — The switch or device with the WWN is connected to a port that is blocked.

  — The switch or device with the WWN is not currently connected to the Director or Edge Switch (detached node).

- If the Director or Edge Switch is online and Switch Binding is not enabled, all nodes and switches attached to the switch are automatically added to the Switch Membership List.

Zoning with Switch Binding Enabled

Note that SANtegrity has no effect on existing zoning configurations. However, note that if a device WWN is in a specific zone, but the WWN is not in the Switch Membership List, the device cannot log in to the Director or Edge Switch port and cannot connect to other devices in the zone with Switch Binding enabled.

Enterprise Fabric Mode

Enterprise Fabric Mode is an option available on the **Fabrics** menu in the HAFM application if the SANtegrity feature key is installed. This option automatically enables the following features and operating parameters that are necessary in multi-switch Enterprise Fabric environments. Note that there are specific requirements for disabling these parameters and features when the Director or Edge Switch is offline or online.

Features and Parameters Enabled

Fabric Binding

This is a SANtegrity feature enabled through the **Fabrics** menu in the HAFM that allows or prohibits Edge Switches and Directors from merging with a selected fabric. Refer to Enable/Disable and Online State Functions on page 6–3 for details on enabling/disabling Fabric Binding with Enterprise Fabric Mode enabled.

Switch Binding

This is a SANtegrity feature enabled through the **Configure** menu in the Product Manager that allows or prohibits Edge Switches and/or Directors from connecting to switch E_Ports, devices from connecting to F_Ports. Refer to Enable/Disable and Online State Functions on page 6–3 for details on enabling/disabling Switch Binding with Enterprise Fabric Mode enabled.

Rerouting Delay

Rerouting delay is a parameter in the **Configure Switch Parameters** dialog box, available from **Configure** menu in the Product Manager application.

Rerouting Delay ensures that frames are delivered through the fabric in order to their destination. If there is a change to the fabric topology that creates a new path (for example, a new switch is added to the fabric), frames may be routed over this new path if its hop count is less than a previous path with a minimum hop count. This may result in frames being delivered to a destination out of order since frames sent over the new, shorter path may arrive ahead of older frames still in route over the older path. If Rerouting Delay is enabled, traffic ceases in the fabric for the time specified in the E_D_TOV field of the **Configure Fabric Parameters** dialog box (**Configure** menu). This delay enables frames sent on the old path to exit to their destination before new frames begin traversing the new path.

If Enterprise Fabric Mode is enabled, this option is automatically enabled and cannot be disabled unless the switch is offline. In this case, disabling Rerouting Delay also disables Enterprise Fabric Mode.

Domain RSCNs

This is a parameter in the **Configure Switch Parameters** dialog box, available from **Configure** menu in the Product Manager application. Domain register for state change notifications (domain RSCNs) are sent between end devices in a fabric to provide additional connection information to host bus adapters (HBA) and storage devices. As an example, this information might be that a logical path has been broken because of a physical event, such as a fiber optic cable being disconnected from a port.

If Enterprise Fabric Mode is enabled, this parameter is automatically enabled and cannot be disabled unless the switch is offline. In this case, disabling Domain RSCNs also disables Enterprise Fabric Mode.

Insistent Domain Identification (ID)

This is a parameter in the **Configure Switch Parameters** dialog box, available from **Configure** menu in the Product Manager application. Enabling this option sets the domain ID configured in the **Preferred Domain ID** field in the **Configure Switch Parameters** dialog box as the active domain identification when the fabric initializes. A static and unique domain identification is required by the Fabric Binding feature because the feature's Fabric Membership list identifies switches by WWN and Domain ID. If a duplicate preferred domain ID is used, then insisted, warnings occur when Directors and Edge Switches are added to a Fabric Membership List.

If Fabric Binding or Enterprise Fabric Mode is enabled, this option is automatically enabled and cannot be disabled unless these options are disabled when the switch is offline. If the switch is online, disabling Insistent Domain ID will disable Enterprise Fabric Mode and Fabric Binding.

A

Product Manager Messages

This appendix lists and explains messages that may display in message boxes as you use the Product Manager. Solutions to problems implied by each message are included when applicable.

Table A–1: StorageWorks Edge Switch 2/24 Product Manager Messages

Message	Description	Action
Activating this configuration will overwrite the current configuration.	Confirmation to activate a new address configuration.	Click Yes to confirm activating the new address configuration or No to cancel the operation.
All configuration names must be unique.	All address configurations must be saved with unique names.	Save the configuration with a different name that is unique to all saved configurations.
All port names must be unique.	A duplicate port name was entered. Every configured port name must be unique.	Reconfigure the port with a unique name.
Another Product Manager is currently performing a firmware install.	Only one firmware install to a specific switch can take place at a time.	Wait for the current firmware install to complete and try again.
Are you sure you want to delete firmware version?	Requesting confirmation to delete the firmware version. Firmware library can hold only eight firmware versions.	Click Yes to confirm the firmware deletion or No to cancel the operation.
Are you sure you want to delete this address configuration?	Confirmation to delete the selected address configuration.	Click Yes to confirm the deletion of the address configuration or No to cancel the operation.

Table A–1: StorageWorks Edge Switch 2/24 Product Manager Messages (Continued)

Message	Description	Action
Are you sure you want to send firmware version?	Confirmation to add a firmware version to the firmware library. The firmware library can hold eight firmware versions.	Click Yes to confirm adding the firmware version to the firmware library, or no to cancel the operation.
Cannot disable Switch Binding while Enterprise Fabric Mode is active and the switch is Online.	User attempted to disable switch binding through the Switch Binding Change State dialog box, but Enterprise Fabric Mode is enabled.	You must either disable Enterprise Fabric Mode using the Enterprise Fabric Mode dialog box in the HAFM application or set the switch offline before you can disable Switch Binding.
Cannot disable Insistent Domain ID while Fabric Binding is active.	User attempted to disable the Insistent Domain ID parameter through the Configure Switch Parameters dialog box, but Fabric Binding is enabled.	Disable Fabric Binding through the Fabric Binding dialog box before disabling these parameters.
Cannot enable beaconing on a failed FRU.	Occurs when selecting Enable Beaconing option for a failed FRU.	Replace FRU and enable beaconing again or enable beaconing on operating FRU.
Cannot enable beaconing while the system error light is on.	Beaconing cannot be enabled while the system error light is on.	Select Clear System Error Light from Product menu to clear error light, then enable beaconing.
Cannot have spaces in field.	Spaces are not allowed in this field.	Remove the spaces or retype the field without spaces.
Cannot install firmware to a switch with a failed CTP card.	Firmware cannot be installed on a switch with a defective CTP card.	Note that the CTP card is not a FRU. If it fails, the switch must be replaced. After replacement, retry the firmware install to the switch.

Table A–1: StorageWorks Edge Switch 2/24 Product Manager Messages (Continued)

Message	Description	Action
Cannot perform this operation while the switch is offline.	This operation cannot take place while the switch is offline.	Configure the switch offline through the Set Online State dialog box then retry the operation.
Cannot retrieve current SNMP configuration.	The current SNMP configuration cannot be retrieved. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot retrieve diagnostics results.	Diagnostics results cannot be retrieved. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot retrieve information for port.	Information for the port cannot be retrieved. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot retrieve port configuration.	Port configuration cannot be retrieved. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot retrieve port information.	Port information cannot be retrieved. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot retrieve port statistics.	Port statistics cannot be retrieved. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot retrieve switch date and time.	Switch date and time cannot be retrieved. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot retrieve switch state.	Switch state cannot be retrieved. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot run diagnostics on a port that is failed.	Port diagnostics cannot be performed on a port that has failed.	Run diagnostics only on an operational port.
Cannot run diagnostics on an active E-port.	Port diagnostics cannot be performed on an active E-port.	Run diagnostics on an E-port only when it is not active.

Table A–1: StorageWorks Edge Switch 2/24 Product Manager Messages (Continued)

Message	Description	Action
Cannot run diagnostics. The port is not installed.	Port diagnostics cannot be performed when the port is not installed.	Run diagnostics only on a port that is installed.
Cannot save port configuration.	Port configuration cannot be saved. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot save SNMP configuration.	SNMP configuration cannot be saved. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot set all ports to Negotiate due to port speed restriction on some ports.	Displays if you try to set all ports to Negotiate through the Configure Ports dialog box and some ports do not support speed configuration.	Replace ports that do not support speed configuration with those that do support more than one speed configuration.
Cannot set Fibre Channel parameters.	Fibre Channel parameters cannot be set. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot set switch date and time.	Switch date and time cannot be set. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot set switch state.	Switch state cannot be set. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot set write authorization without defining a community name.	A community name was not defined in the Configure SNMP dialog box for the write authorization selected.	Provide a name in the name field where write authorization is checked.
Cannot start data collection.	Data collection cannot be started. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot start port diagnostics.	Port diagnostics cannot be started. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.

Table A–1: StorageWorks Edge Switch 2/24 Product Manager Messages (Continued)

Message	Description	Action
Cannot swap an uninstalled port.	A port swap cannot be performed when the port is not installed.	Perform a swap only on a port that is installed.
Click OK to remove all contents from log.	Requesting confirmation that you want all contents removed from the log.	Click OK to continue or Cancel to cancel the operation.
Continuing may overwrite host programming. Continue?	Configurations sent from the host may be overwritten by HAFM.	Continuing will activate the current configuration.
Could not export log to file.	A file I/O error occurred. The log file could not be saved to the specified destination.	Ensure filename and drive are correct.
Could not find firmware file.	Firmware file selected was not found in the FTP directory.	Ensure file name and directory are correct.
Could not find firmware file.	The selected file is not a firmware file.	Obtain a valid firmware file from your service representative.
Could not remove dump files from server.	Dump files could not be removed from server. Link may be down or switch may be busy.	Retry the operation later. If the condition persists, contact support personnel.
Could not stop port diagnostics.	Port diagnostics could not be stopped. Link may be down or switch may be busy.	Retry the operation later. If the condition persists, contact support personnel.
Could not write firmware to flash.	Firmware could not be written to flash memory.	Try again. If problem persists, contact support personnel.
CUP name and port name are identical.	Within the address configuration, one or more of the port names are the same as the CUP name.	Make sure all names are unique for the ports and CUP name.
Date entered is invalid.	Date entered incorrectly.	Verify that the number of days in the month is valid.

Table A–1: StorageWorks Edge Switch 2/24 Product Manager Messages (Continued)

Message	Description	Action
Device applications should be terminated before starting diagnostics. Press NEXT to continue.	Device application is not terminated.	Terminate device application before running port diagnostics.
[device WWN] cannot be removed from the Switch Membership List while participating in Switch Binding. The device must be isolated from the switch, or Switch Binding deactivated before it can be removed.	User attempted to remove a device WWN from the Switch Membership List (SANtegrity feature) while Switch Binding is enabled.	Remove the device from the switch by blocking the port, setting the director offline, or disabling Switch Binding through the Switch Binding Change State dialog box before removing devices form the Switch Membership List.
Disabling Insistent Domain ID will disable Fabric Binding. Do you want to continue?	Fabric Binding is enabled through the HAFM and user attempted to disable Insistent Domain ID in the Configure Switch Parameters dialog box.	Click Yes if you want to continue and disable Fabric Binding.
Disabling Switch Binding will disable Enterprise Fabric Mode. Do you want to continue?	User attempting to disable Switch Binding through the Switch Binding State Change dialog box, but Enterprise Fabric Mode is enabled	Disable Enterprise Fabric Mode using the Enterprise Fabric Mode dialog box in the HAFM before disabling Switch Binding.
Do you want to continue with IPL?	Requesting confirmation to proceed with an IPL.	Click Yes to confirm the IPL or Cancel to cancel the operation.
Duplicate community names require identical write authorizations.	Duplicate community names exist that have conflicting or different write authorizations.	Verify community names and whether a community name is duplicated with different write authorizations.

Table A–1: StorageWorks Edge Switch 2/24 Product Manager Messages (Continued)

Message	Description	Action
Enterprise Fabric Mode will be disabled if any of the following parameters are disabled: Insistent Domain ID, Rerouting Delay, Domain RSCN's. Do you want to continue?	User attempted to disable these parameters in the Configure Switch Parameters dialog box while the Edge Switch was online, but Enterprise Fabric Mode (SANtegrity feature) is enabled.	Click Yes if you want to continue, and disable Enterprise Fabric Mode.
Error retrieving port information.	An error occurred while retrieving port information. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Error retrieving port statistics.	An error occurred while retrieving port statistics. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Error stopping port diagnostics.	An error occurred while attempting to stop the port diagnostics from running. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Error transferring files <message>.	An error occurred while attempting to download files.	Retry the operation. If the condition persists, contact support personnel.
Field cannot be blank.	A blank field is not allowed in this dialog.	Enter the required information in the blank field.
File transfer aborted.	User has stopped the file transfer.	N/A. An informational message.
File transfer is in progress.	Firmware or data collection is being transferred.	N/A. An informational message.
Firmware download timed out.	The switch did not respond in the time allowed. The status of the firmware install operation is unknown.	Retry the operation. If the problem persists, contact support personnel.
Firmware file I/O error.	Firmware file input/output error occurred.	Contact support personnel.
Firmware file not found.	Firmware file deleted from the HAFM server.	Add firmware to library.

Table A–1: StorageWorks Edge Switch 2/24 Product Manager Messages (Continued)

Message	Description	Action
Incorrect product type.	When configuring a new product through the New Product dialog box, an incorrect product was selected for the network address.	Select the correct product type for the product with the network address.
Installing this feature key, while online, will cause an IPL operation on the switch and a momentary loss of LAN connection. This operation is non-disruptive to the Fibre Channel traffic. Do you wish to continue installing this feature key?	If the Edge Switch is online, installing the new feature key will cause an internal program load (IPL). The LAN connection to the HAFM server will be lost momentarily, but Fibre Channel traffic will not be affected.	Select Yes to install the feature key or No to not install.
Internal file transfer error received from switch.	Switch detected an internal file transfer error.	Contact support personnel.
Invalid character in field.	Invalid character in the input field.	Re-enter the field information.
Invalid configuration name.	Attempted to save an address configuration name with an invalid name.	Use up to 24 alphanumeric characters, including spaces, hyphens and underscores.
Invalid feature key.	The feature key was not recognized.	Re-enter the feature key noting the key is case-sensitive and to include the dashes.
Invalid firmware file.	Selected file is not a firmware file.	Select the correct firmware file.
Invalid network address.	Network address specified is not known by the domain name server.	Check the input address and specify the correct network address.
Invalid port number.	Port number must be within the range of ports for the specific switch model.	Enter a port number within the correct range.

Table A–1: StorageWorks Edge Switch 2/24 Product Manager Messages (Continued)

Message	Description	Action
Invalid port number. Valid ports are (0 - 23).	Port number must be within the range of ports for the specific switch model. For this model, the valid port numbers are 0 - 23.	Enter a port number within the correct range.
Invalid port swap.	Port swap selection is not allowed.	Ensure that each port selected for swap has not been previously swapped.
Invalid response received from switch.	The switch returned an invalid response.	Resend the firmware. If the condition persists, contact support personnel.
Invalid serial number for this feature key.	The serial number and the feature key did not match.	Ensure that the feature key being installed is specifically for this switch serial number.
Invalid UDP port number.	UDP port number must be an integer from 1 through 65535.	Enter a port number from 1 through 65535.
Invalid value for day (1 - 31).	Value for day must be an integer from 1 through 31.	Enter a value from 1 through 31.
Invalid value for E_D_TOV.	Value for E_D_TOV must be an integer from 2 through 600, measured in tenths of a second.	Enter a value from 2 through 600.
Invalid value for hour (0 - 23).	Value for hour must be an integer from 0 through 23.	Enter a value from 0 through 23.
Invalid value for minute (0 - 59).	Value for minute must be an integer from 0 through 59.	Enter a value from 0 through 59.
Invalid value for month (1 - 12).	Value for month must be an integer from 1 through 12.	Enter a value from 1 through 12.
Invalid value for R_A_TOV.	Value for R_A_TOV must be an integer from 10 through 1200. Measured in tenths of a second.	Enter a value from 10 to 1200.
Invalid value for second (0 - 59).	Value for second must be an integer from 0 through 59.	Enter a value from 0 through 59.

Table A–1: StorageWorks Edge Switch 2/24 Product Manager Messages (Continued)

Message	Description	Action
Invalid value for year.	Value for year must be a four-digit year after 1980.	Enter a correct four-digit value for the year.
Invalid World Wide Name.	World wide name must have eight two-digit hexadecimal numbers separated by colons (xx:xx:xx:xx:xx:xx:xx:xx).	Enter a worldwide name using eight two-digit hexadecimal numbers separated by colons in the format given in the message.
Link dropped.	Connection between HAFM server and the switch has been lost.	Wait for the connection to re-establish. Link re-connects are attempted every 30 seconds.
Log is currently in use.	Log is in use by another Product Manager.	Retry the operation later.
Loopback plug(s) must be installed on ports being diagnosed. Press Next to continue.	External loopback diagnostics require an optical loopback plug to be installed.	Ensure that an optical loopback plug is installed in port optical transceiver before running external wrap diagnostic testing.
Maximum number of versions already installed.	The maximum number of firmware versions has been reached.	Delete a firmware version before adding a new firmware version.
No file was selected.	Action requires you to select a file	Select a file.
No firmware version file was selected.	A file was not selected in the Firmware Library dialog box before an action, such as modify or send was performed.	Click a firmware version in the dialog box to select it, then perform the action again.
No firmware versions to delete.	There are no firmware versions in the firmware library to delete.	N/A. An informational message.

Table A–1: StorageWorks Edge Switch 2/24 Product Manager Messages (Continued)

Message	Description	Action
Non-redundant switch must be offline to install firmware.	Since the switch has only a single CTP card, it must be offline to initiate a firmware installation. Note that the CTP card is an internal component and not a FRU.	Take switch offline and try again.
Not all of the optical transceivers are installed for this range of ports.	Some ports in the specified range do not have optical transceivers installed.	Use a port range that is valid for the ports installed.
Performing this operation will change the current state to Offline.	This operation causes the switch to go offline.	N/A. An informational message.
Performing this operation will change the current state to Online.	This operation causes the switch to go online.	N/A. An informational message.
Performing this action will overwrite the date/time on the switch.	Warning that occurs when configuring the date and time through the Configure Date and Time dialog box, that the new time or date will overwrite the existing time or date set for the switch.	Verify that you want to overwrite the current date or time.
Periodic Date/Time synchronization must be cleared before enabling switch clock alert.	Action cannot be performed because Periodic Date/Time Synchronization option is active.	Click Periodic Date/Time Synchronization check box in Configure Date and Time dialog box (Configure menu) to clear check mark and disable periodic date/time synchronization.
Port binding was removed from attached devices that are also participating in Switch Binding.	Informational message. User has removed Port Binding from attached devices, but one or more of these devices is still controlled by Fabric Binding.	Review the Switch Binding Membership List to determine if the devices should be members.

Table A–1: StorageWorks Edge Switch 2/24 Product Manager Messages (Continued)

Message	Description	Action
Port cannot swap to itself.	Port addresses entered in the Swap Ports dialog box are the same.	Make sure that address in the first and second port address fields are different.
Port diagnostics cannot be performed on an inactive port.	This displays when port diagnostics is run on a port in an inactive state.	Run the diagnostics on an active port.
Port speeds cannot be configured at a higher rate than the director/switch speed.	This displays when you configure a port to 2 GB/sec and the switch speed is set to 1 Gb/sec.	Set the port speed to 1 Gb/sec in the Configure Ports dialog box.
Product Manager error <number>.	The switch Product Manager encountered an internal error and cannot continue.	Report the problem to support personnel.
Product Manager instance is currently open.	A Product Manager window is currently open.	Informational message only.
R_A_TOV must be greater than E_D_TOV.	R_A_TOV must be greater than E_D_TOV.	Change one of the values so that R_A_TOV is greater than E_D_TOV.
Resource is unavailable.	The specified operation cannot be performed because the product is unavailable.	Verify that the HAFM server-to-product link is up. If the link is up, the HAFM server may be busy. Try the operation again later.
SANtegrity Feature not installed. Please contact your sales representative.	The user selected Switch Binding from the Configure menu, but the optional SANtegrity feature is not installed.	Install the SANtegrity key through the Configure Feature Key dialog box before using Switch Binding features.
Send firmware failed.	Send firmware operation has failed.	Retry the operation. If the condition persists, contact support personnel.
SNMP trap address not defined.	An SNMP trap address must be defined if a community name is defined.	Define an SNMP address.

Table A–1: StorageWorks Edge Switch 2/24 Product Manager Messages (Continued)

Message	Description	Action
Stop diagnostics failed. The test is already running.	Diagnostics for the port was not running and the Stop was selected on the Port Diagnostics dialog box. Diagnostics quit for the port for some reason, but the Stop button remains enabled.	Verify port operation. Retry diagnostics for port and select Stop from the dialog box. If problem persists, contact your service representative.
Stop diagnostics failed. The test was not running.	The action to stop diagnostics failed because the test was not running.	Informational message.
Switch Binding was removed from attached devices that are also participating in Port Binding. Please review the Port Binding Configuration.	The device WWNs were removed from the Switch Membership List (SANtegrity Switch Binding feature), but you should note that one or more of these devices still has security control in port binding.	Verify that the security level for each device is as required by reviewing the Bound WWN list in the Configure Ports dialog box.
System diagnostics cannot run. The Operational Status is invalid.	System diagnostics cannot run on switches with failed ports.	Replace failed ports.
The add firmware process has been aborted.	User has ended the add firmware process.	N/A. An informational message.
The data collection process failed.	An error occurred in the data collection process.	Contact support personnel.
The data collection process has been aborted.	User has ended the data collection process.	N/A. An informational message.
The following parameters cannot be disabled while Enterprise Fabric Mode is active: Insistent Domain ID, Rerouting Delay, Domain RSCN's.	User attempted to disable these parameters in the Configure Switch Parameters dialog box while Enterprise Fabric Mode is enabled.	Disable Enterprise Fabric Mode through the Enterprise Fabric Mode dialog box in the HAFM, then disable the parameters.
The firmware file is corrupted.	A firmware file has corrupt data.	Contact support personnel.

Table A–1: StorageWorks Edge Switch 2/24 Product Manager Messages (Continued)

Message	Description	Action
The firmware version already exists.	Firmware version already exists in the database.	N/A. An informational message.
The HAFM server is busy processing a request from another Product Manager	The HAFM server could not process the current request because it is busy handling a request from another Product Manager.	Retry the operation later. If the condition persists, contact support personnel.
The link to the switch is not available.	The link from the HAFM server to the switch is not available.	Check Ethernet connection.
The maximum number of address configurations has been reached.	The maximum number of saved address configurations has been reached.	Delete configurations no longer needed to allow new configuration to be saved.
The optical transceiver is not installed.	No information available for a port that is not installed.	Ensure the optical transceiver is installed and fully seated.
The switch did not accept the request.	The switch did not handle the action.	Try action again. If problem persists, contact your support representative.
The switch did not respond in the time allowed.	A time out was reached waiting for the switch to respond to the action.	Try action again.
The switch is busy saving maintenance information.	switch is busy with a maintenance operation.	Retry the operation later. If the condition persists, contact support personnel.
The switch must be offline to configure.	A configuration changed was attempted for a configuration requiring offline changes.	Take the appropriate actions to set the switch offline before attempting the configuration change.
This feature has not been installed. Please contact your sales representative.	Indicator that the feature has not been installed on this switch.	Contact your sales representative to obtain the desired feature.

Table A–1: StorageWorks Edge Switch 2/24 Product Manager Messages (Continued)

Message	Description	Action
This feature key does not include all of the features currently installed and cannot be activated while the switch is online.	The feature set currently installed for this system contains features that are not being installed with the new feature key. To activate the new feature key, you must set the Edge Switch offline. Activating the new feature set, however, will remove current features not in the new feature set.	Set the Edge Switch offline through the Set Online State dialog box, then activate the new feature key using the Configure Feature Key dialog box.
This feature key does not include all of the features currently installed. Do you want to continue with feature key activation?	The feature set currently installed for this system contains features that are not being installed with the new feature key.	Click Yes to activate the feature key and remove current features not in the new feature set or No to cancel.
Threshold alerts are not supported on firmware earlier than 01.03.00.	Threshold alerts are not supported in firmware releases before 1.03.00.	Informational message.
Unable to change to incompatible firmware release.	The user tried to download a firmware release that is not compatible with the current product configuration.	Refer to the release notes or contact customer support.
Unable to save data collection file to destination.	Could not save data collection file to the specified drive (hard drive, network).	Retry the operation. If the condition persists, contact support personnel.
You do not have rights to perform this action.	User does not have the rights to perform this action.	An informational message.

Glossary

The following cross-references are used in this glossary:

Contrast with. This refers to a term that has an opposite or substantively different meaning.

See. This refers the reader to another keyword or phrase for the same term.

See also. This refers the reader to definite additional information contained in another entry.

access control
List of all devices that can access other devices across the network and the permissions associated with that access. *See also* persistent binding and zoning.

active FRU
A field-replaceable unit that is currently operating as the active and not the back up FRU.

active zone set
Single zone set that is active in a multi-switch fabric. It is created when you enable a specified zone set. This zone set is compiled by checking for undefined zones or aliases.

agent
Software that processes queries on behalf of an application and returns replies.

alarm
SNMP message notifying an operator of a network or device problem.

ANSI
American National Standards Institute: an organization that provides voluntary standards in the United States.

application-specific integrated circuit (ASIC)
A circuit designed for a specific application or purpose, such as implementing the lower-layer Fibre Channel protocol (FC-0). ASICs differ from general purpose devices such as memory chips or microprocessors.

alias server
Fabric software facility that supports multicast group management.

arbitrated loop
One of the three connection topologies offered by Fibre Channel. Up to 126 node ports and one fabric port can communicate without the need for a separate switched fabric. *See also* point to point.

arbitration
Process of selecting one device from a collection of devices that request service simultaneously.

Audit Log
Log summarizing actions (audit trail) made by the user.

authentication
Verification of identity for a person or process.

backplane
The backplane provides 48 VDC power distribution and connections for all logic cards.

back up FRU
When an active FRU fails, an identical back up FRU takes over operation automatically (failover) to maintain switch and Fibre Channel link operation.

beaconing
Use of light-emitting diodes on ports, port cards, field-replaceable units, and switches to aid in the fault-isolation process; when enabled, active beaconing will cause LEDs to flash for faulty components.

BB_Credit
Also known as Buffer-to-Buffer Credit. Indicates the maximum number of frames a port can transmit without receiving a receive ready signal from the receiving device.

ber
See bit error rate.

bidirectional
In Fibre Channel, the capability to simultaneously communicate at maximum speeds (100 Mbps) in both directions over a link.

bit error rate
A comparison of the number of bits received incorrectly by a device to the total number of bits transmitted.

blocked port
Devices communicating with the port are prevented from logging into the switch or communicating with other devices attached to the switch. A blocked port continuously transmits the offline sequence.

bridge
Device that connects and passes packets between two network segments that use the same communications protocol.

broadcast
Send a transmission to all N_Ports on a fabric.

broadcast frames
Data packet, also known as a broadcast packet, whose destination address specifies all computers on a network. *See also* multicast.

buffer
Storage area for data in transit. Buffers compensate for differences in processing speeds between devices. *See also* BB_Credit.

CHPID
See channel path identifier.

call-home
Product feature which enables the HAFM server to automatically dial out to a support center and report system problems. The support center server accepts calls from the HAFM server, logs reported events, and can notify one or more support center representatives.

channel
Point-to-point link that transports data from one point to the other.

channel path
A single interface between a central processor and one or more control units along which signals and data can be sent to perform I/O requests.

channel path identifier
In a channel subsystem, a value assigned to each installed channel path of the system that uniquely identifies that path to the system.

class of Fibre Channel service
Defines the level of connection dedication, acknowledgment, and other characteristics of a connection.

Class F Fibre Channel service
Used by switches to communicate across interswitch links (ISLs) to configure, control, and coordinate a multi-switch fabric.

Class 2 Fibre Channel service
Provides a connectionless (not dedicated) service with notification of delivery or nondelivery between two N_Ports. In-order delivery of frames is not guaranteed.

Class 3 Fibre Channel service
Provides a connectionless (not dedicated) service without notification of delivery or nondelivery between two N_Ports. Also known as datagram.

community profile
Information that specifies which management objects are available to what management domain or SNMP community name.

concurrent firmware upgrade
The CTP card provides two nonvolatile memory regions. Because two firmware versions can be stored on the card, firmware is upgraded without disrupting switch operation. Note that the CTP card on this switch is an internal component and not a FRU.

concurrent maintenance
Ability to perform maintenance tasks, such as removal or replacement of field-replaceable units, while a hardware product is operating.

configuration data
Configuration data includes: identification data, port configuration data, operating parameters, SNMP configuration, and zoning configuration. A configuration back up file is required to restore configuration data if the CTP card in a nonredundant switch or switch is removed and replaced.

configuration report
An ASCII text file containing all current user-definable configuration options.

connectionless
Nondedicated link. Typically used to describe a link between nodes which allows the switch to forward Class 2 or Class 3 frames as resources (ports) allow. Contrast this to the dedicated bandwidth that is required in a Class 1 Fibre Channel Service point-to-point link.

connector
See optical fiber connector.

control processor card
Circuit card that contains the switch microprocessor. The CTP card also initializes hardware components of the system after power-on. Note that the CTP card on this switch is not a FRU.

control unit
A hardware unit that controls the reading, writing, or displaying of data at one or more input/output units.

control unit port
An internal port on the CTP card that communicates with the attached IBM S/390 or similar processor channels to report error conditions and link initialization.

CRC
See cyclical redundancy check.

CTP
See control processor card.

CUP
See control unit port.

cyclical redundancy check
System of error checking performed at both the sending and receiving station using the value of a particular character generated by a cyclic algorithm. When the values generated at each station are identical, data integrity is confirmed.

DASD
Direct access storage device such as a disk drive.

data directory
Critical information for all managed products (including Directors and Edge Switches). Information stored here includes: all HAFM configuration data (product definitions, user names, passwords, user rights, nicknames, session options, SNMP trap recipients, e-mail recipients, and Ethernet event notifications); all log files (HAFM logs and individual Product Manager logs); zoning library (all zone sets and zone definitions); firmware library; call-home settings (phone numbers and dialing options); configuration data for each managed switch (stored on the HAFM server and in NV-RAM on each switch).

datagram
See Class 3 Fibre Channel service.

default
Pertaining to an attribute, value, or option that is assumed when none is explicitly specified.

default zone
Contains all attached devices that are not members of a separate zone.

destination address
Address identifier that indicates the targeted destination of a data frame.

device
Product, connected to a managed switch, that is not controlled directly by the Product Manager. *See also* node.

diagnostics
Procedures used by computer users and service personnel to diagnose hardware or software error conditions.

dialog box
Dialog box is a window containing informational messages or data fields to be modified or filled in with desired options.

D_ID
See destination address.

director
An intelligent Fibre Channel switching device providing any-to-any port connectivity between nodes (end devices) on a switched fabric. The director sends data transmissions (data frames) between nodes in accordance with the address information present in the frame headers of those transmissions.

DNS name
Domain name system or domain name service. Host or node name for a device or managed product that is translated to an IP address through a domain name server.

domain ID
Number (1 through 31) that uniquely identifies a switch in a multi-switch fabric. A distinct domain ID is automatically allocated to each switch in the fabric by the principal switch.

E_Port

See expansion port.

E_D_TOV

See error-detect time-out value.

Embedded Web Server

A management interface embedded on the switch's code which offers features similar to, but not as robust as, the HAFM and Product Manager.

error-detect time-out value

E_D_TOV defines the time the switch waits for an expected response before declaring an error condition.

error message

Indication that an error has been detected. *See also* information message and warning message.

Ethernet

A widely implemented local area network (LAN) protocol that uses a bus or star topology and serves as the basis for the IEEE 802.3 standard, which specifies the physical and software layers. Baseband LAN allows multiple station access to the transmission medium at will without prior coordination and which avoids or resolves contention.

ethernet hub

A device used to connect the HAFM server and the switches it manages.

event code

A numeric code that displays in the Event Log. This code provides information on system failures, such as hardware failures, failure locations, or general information on normal system events.

Event Log

Record of significant events that have occurred on the switch, such as FRU failures, degraded operation, and port problems.

expansion port

Physical interface on a Fibre Channel switch within a fabric that attaches to an expansion port (E_Port) on another Fibre Channel switch to form a multi-switch fabric. *See also* segmented E_Port.

explicit fabric login
Data field size, supported by an F-Port, that is agreed upon during fabric login.

fabric
Entity that interconnects N_Ports and is capable of routing (switching) Fibre Channel frames using the destination ID information in the Fibre Channel frame header accompanying the frames.

fabric element
Any active switch or node in a switched fabric.

fabric port
Physical interface within the fabric that connects to an N_Port through a point-to-point full duplex connection.

fabric services
Fabric services implements the various Fibre channel services that are described in the standards. These services includes the Fabric controller (login server), name server, and management server.

failover
Automatic and nondisruptive transition of functions from an active FRU that has failed to a back up FRU.

FCC-IOC
See Fibre Channel I/O controller.

FE-MIB
See Fibre Channel Fabric Element.

feature key
A string of alphanumeric characters consisting of both uppercase and lowercase. The following is an example of a feature key format: XxXx-XXxX-xxXX-xX.

fiber optics
Branch of optical technology concerned with the transmission of light pulses through fibers made of transparent materials such as glass, fused silica, and plastic.

fibre
Physical media types supported by the Fibre Channel specification, such as optical fiber, twisted pair, and coaxial cable.

Fibre Channel

Integrated set of standards recognized by ANSI which defines specific protocols for flexible information transfer. Logically, a point-to-point serial data channel, structured for high performance.

Fibre Channel fabric element

Any device linked to a fabric. Information about these devices is recorded in a management information base (MIB) which can be accessed by fabric management software.

Fibre Channel I/O controller

Controls the embedded Fibre Channel port and configures the ports' ASICs.

fibre port module card

Each fiber port module card provides four Fibre Channel connections through duplex small form factor pluggable (SFP) fiber-optic transceivers.

field-replaceable unit

Assembly removed and replaced in its entirety when any one of its components fails.

firmware

Embedded program code that resides and executes on the switch.

FLASH memory

A computer chip with a read-only memory that retains its data when the power is turned off and that can be electronically erased and reprogrammed without being removed from the circuit board.

F_Port

See fabric port.

FPM card

See fiber port module card.

frame

A variable-length packet of data that is transmitted in frame relay technology.

FRU

See field-replaceable unit.

gateway

A multi-homed host used to route network traffic from one network to another, and to pass network traffic from one protocol to another.

gateway address

A unique string of numbers (in the format xxx.xxx.xxx.xxx) that identifies a gateway on the network.

GBIC

GigaBit Interface Converter. A removable module that converts an electrical serial data stream to an optical or amplified electrical serial data stream. Contains connector for attaching fiber optic cable.

generic port

Also known as G_Port. Physical interface on a switch that can function either as a fabric port (F_Port) or an extension port (E_Port) depending on the port type to which it connects.

G_Port

See generic port.

GUI

Graphical User Interface.

HAFM Product Manager

The applications provide a graphical user interface (GUI) and management services, and implement web and other server functions.

HAFM server

PC shipped with a product to run the HAFM and Product Manager applications.

Hardware Log

Record of FRU insertions and removals in the switch.

HBA

See host bus adapter.

heterogeneous fabric

A fabric with both HP and non-HP products.

homogeneous fabric

A fabric consisting of only HP products.

hop count

The number of hops a unit of information traverses in a fabric.

hexadecimal
A number system with a base of 16.

high availability
A performance feature characterized by hardware component redundancy and hot-swappability (enabling non-disruptive maintenance). High-availability systems maximize system uptime while providing superior reliability, availability, and serviceability.

hop
Data transfer from one node to another node.

hop count
ISL connections.

host bus adapter
Logic card that provides a link between the server and storage subsystem, and that integrates the operating systems and I/O protocols to ensure interoperability.

hot-swapping
Removing and replacing a device's components while the device continues to operate normally.

hub
In Fibre Channel, a device that connects nodes into a logical loop by using a physical star topology.

IML
See initial machine load.

inband management
Management of the switch through Fibre Channel connection to a port card.

information message
Message telling a user that a function is performing normally or has completed normally. *See also* error message and warning message.

initial machine load
Also known as IML. Hardware reset for the CTP card on the switch. It does not affect other hardware. It is initiated by pushing the reset (RST) button on the machine's front panel.

initial program load
Process of initializing the device and causing the operating system to start. Initiated through a menu in the Product Manager.

interface
Hardware, software, or both, linking systems, programs, or devices.

Internet Protocol
The TCP/IP standard protocol that defines the IP datagram as the unit of information passed across an internet and provides the basis for connectionless, best-effort packet delivery service. IP includes the ICMP control and error message protocol as an integral part.

internet protocol address
Unique string of numbers (in the format xxx.xxx.xxx.xxx) that identifies a device on a network.

interoperability
Ability to communicate, execute programs or transfer data between various functional units over a network.

interswitch link
Also known as ISL. Physical E_Port connection between two switches in a fabric.

I/O configuration
See input/output configuration.

IOCDS
A data set that contains an I/O configuration definition built by the IOCP.

IOCP
See input/output configuration program.

IP address
See internet protocol address.

IPL
See initial program load.

ISL
See interswitch link.

jumper cable
Optical cable that provides physical attachment between two devices or between a device and a distribution panel. *Contrast with* trunk cable.

laser
Light Amplification through Simulated Emissions of Radiation. A device that uses the oscillation of atoms or molecules between energy levels to generate a narrow, finely focused beam of light. The light has a single wavelength or narrow spectrum of wavelengths and is matched in phase and frequency.

latency
When used in reference to a Fibre Channel switching device, latency refers to the amount of time elapsed between receipt of a data transmission at a switch's incoming F_Port (from the originating node port) to retransmission of that data at the switch's outgoing F_Port (to the destination N_Port). The amount of time it takes for data transmission to pass through a switching device.

LED
Light-emitting diodes (LEDs) on switch FRUs and the front bezel that provide visual indicators of hardware status or malfunctions.

LIN
See link incident.

link
Physical connection between two devices on a switched fabric.

link incident
A link incident is a problem detected on a fiber optic link, like the loss of light, invalid sequences and other problems.

link incident alerts
A user notification, such as a graphic symbol in the Hardware View that indicates that a link incident has occurred.

load balancing
Ability to evenly distribute traffic over multiple interswitch links within a fabric. Load balancing on HP switches takes place automatically.

log
A record, as of the performance of a machine or the progress of an undertaking.

logical unit number
Also known as LUN. In Fibre Channel addressing, a logical unit number is a number assigned to a storage device which, in combination with the storage device's node port's world-wide name, represents a unique identifier for a logical device on a storage area network.

loopback plug
In a fiber optic environment, a type of duplex connector used to wrap the optical output signal of a device directly to the optical input.

loopback test
Test that checks attachment or control unit circuitry, without checking the mechanism itself, by returning the output of the mechanism as input.

LUN
See logical unit number.

MAC address
See Media Access Control address.

maintenance port
Connector on the switch operator panel where a PC running an ASCII terminal emulator can be attached or dial-up connection made for specialized maintenance support.

managed product
Hardware product that can be managed with the Product Manager. For example, the Edge Switch 2/24 and Edge Switch 2/32 are managed products. *See also* device.

management information base
Related set of software objects (variables) containing information about a managed device and accessed via SNMP from a network management station.

management session
Management session exists when a user logs on to the HAFM. HAFM can support multiple concurrent management sessions. The user must specify the network address of the HAFM's server at logon time.

Media Access Control address
Hardware address of a node (device) connected to a network.

MIB
See management information base.

multicast

Delivery of a single transmission to multiple destination N_Ports. Can be one to many or many to many. All members of the group are identified by one IP address.

multi-switch fabric

Fibre Channel fabric created by linking more than one fabric switching device within a fabric.

name server

Program that translates names from one form into another. Domain name servers (DNS) translate domain names into IP addresses.

name server zoning

N_Port access management that allows N_Ports to communicate if and only if they belong to a common name server zone.

network address

Name or address that identifies a managed product, such as the Edge Switch 2/24 and Edge Switch 2/32, on a TCP/IP network. The network address can be either an IP address in dotted-decimal notation (containing four three-digit octets in the format xxx.xxx.xxx.xxx), or a domain name (as administered on a customer network).

nickname

Alternate name assigned to a worldwide name for a node or switch in the fabric.

node

In Fibre Channel terminology, mode refers to an end device (server or storage device) that is or can be connected to a switched fabric.

node port

Physical interface within an end device which can connect to an F_Port on a switched fabric or directly to another N_Port (in point-to-point communications).

nondisruptive maintenance

Ability to service FRUs (including maintenance, installation, removal and replacement) while normal operations continue without interruption. *See also* concurrent maintenance.

N_Port

See node port.

offline sequence

Sequence sent by the transmitting port to indicate that it is attempting to initialize a link and has detected a problem in doing so.

offline state

When the switch is in the offline state, all the installed ports are offline. The ports transmit an OLS (offline sequence) and they cannot accept a login for connection from an attached device. *Contrast with* online state.

OLS

See offline sequence.

online state

When the switch is in the online state, all of the unblocked ports are allowed to login to the fabric and begin communicating. Devices can connect to the switch if the port is not blocked and can communicate with another attached device if both devices are in the same zone or if the default zone is enabled. *Contrast with* offline state.

Open Systems Management Server

An optional feature that can be enabled on the Director or Edge Switch through the Product manager application. When enabled, host control and management of the Director or Edge Switch are provided through an open systems interconnection (OSI) device attached to a Director or Edge Switch port.

operating state (switch)

The operating states are described as follows:

   Online - when the switch is set online, an attached device can log in to the switch if the port is not blocked. Attached devices can communicate with each other if they are configured in the same zone.

   Offline - when the switch is set offline, all ports are set offline. The switch transmits the offline sequence (OLS) to attached devices, and the devices cannot log in to the switch.

operating state (port)

Can be beaconing, invalid attachment, link incidents, link resets, no light, not operational, online, offline, segmented E_Port, port failure, or testing.

operating status (switch)

Can be online, offline, coming online, or going offline.

optical cable

Fiber, multiple fibers, or a fiber bundle in a structure built to meet optical, mechanical, and environmental specifications. *See also* jumper cable, optical cable assembly, and trunk cable.

optical cable assembly

Optical cable that is connector-terminated. *See also* jumper cable and optical cable.

optical fiber connector
Hardware component that transfers optical power between two optical fibers or bundles and is designed to be repeatedly connected and disconnected.

out-of-band management
Transmission of management information using frequencies or channels other than those routinely used for information transfer.

packet
Logical unit of information (usually in the form of a data frame) transmitted on a network. It contains a header (with all relevant addressing and timing information), the actual data, and a trailer (which contains the error checking function, usually in the form of a cyclic redundancy check), and frequently, user data.

panel
The main Product Manager window is divided into four view panels: title panel, menu bar, status bar, and view panel. Use features in these panels to configure switch operation, monitor performance, and access maintenance features.

password
Unique string of characters known to the computer system and to a user who must specify it to gain full or limited access to a system and to the information stored within it.

path
In a network, any route between any two ports.

persistent binding
A form of server-level access control that uses configuration information to bind a server to a specific Fibre Channel storage volume (or logical device) using a unit number.

point-to-point
A Fibre Channel topology which involves a dedicated link that connects only two stations. *See also* arbitrated loop.

port
Receptacle on a device to which a cable leading to another device can be attached.

port name
Name that the user assigns to a particular port through the Product Manager.

POST
See power-on self-test.

power-on self-test
Series of self-tests executed each time the unit is booted or reset.

preferred domain ID
Domain ID that a switch is assigned by the principal switch in a switched fabric. The preferred domain ID becomes the active domain ID except when configured otherwise by the user.

principal switch
In a multi-switch fabric, the switch that allocates domain IDs to itself and to all other switches in the fabric. There is always one principal switch in a fabric. If a switch is not connected to any other switches, it acts as its own principal switch.

product manager
Application that implements the management user interface for the switch.

product name
User-configurable identifier assigned to a managed product. Typically, this name is stored on the product itself. For the switch, the product name can also be accessed by an SNMP manager as the system name.

protocol
A standard procedure for regulating data transmission between computers.

PSP bucket
See preventive service planning bucket.

R_A_TOV
See resource allocation time-out value.

redundancy
Performance characteristic of a system or product whose integral components are backed up by identical components to which operations will automatically failover in the event of a component failure. Redundancy is a vital characteristic of virtually all high-availability (24 hr./7 days per week) computer systems and networks.

redundant FRU
SFP LC transceivers, power supplies, and cooling fans that can be removed or replaced without disrupting switch or Fibre Channel link operation.

remote access link
Connection to a device or program on a computer network via a (geographically) remote workstation.

remote notification

A process by which a system is able to inform remote users and/or workstations of certain classes of events that occur on the system. E-mail notification and the configuration of SNMP trap recipients are two examples of remote notification programs that can be implemented.

remote user workstation

Workstation, such as a PC, using HAFM and Product Manager software that can access the HAFM server over a LAN connection.

rerouting delay

Enabling rerouting delay ensures that frames are delivered in order through the fabric to their destination. If there is a change to the fabric topology that creates a new path (for example, a new switch is added to the fabric), frames may be routed over this new path if its hop count is less than a previous path with a minimum hop count. This may result in frames being delivered to a destination out of order since frames sent over the new, shorter path may arrive ahead of older frames still in route over the older path.

resource allocation time out value

R_A_TOV is a value used to time out operations that depend on the maximum possible time that a frame could be delayed in a fabric and still be delivered.

SAN

See storage area network.

SC

Subscriber connectors.

segmented E_Port

E_Port that has ceased to function as an E_Port within a multi-switch fabric due to an incompatibility between the fabrics that it joins. *See also* expansion port.

SEL

System error light.

SFP transceivers

See small form factor transceivers.

small form factor pluggable (SFP) transceivers

Laser-based optical transceivers for a wide range of networking applications requiring high data rates. The transceivers, which are designed for increased densities, performance, and reduced power, are well-suited for Fibre Channel applications.

simple mail transfer protocol
The standard e-mail protocol on the Internet. It is a TCP/IP protocol that defines the message format and the message transfer agent, which stores and forwards the mail.

SMTP
See simple mail transfer protocol.

SNMP
Simple Network Management Protocol. Specifies a mechanism for network management that is complete, yet simple. Information is exchanged between agents, which are the devices on the network being managed, and managers, which are the devices on the network through which the management is done.

SNMP community
Also known as SNMP community string. SNMP community is a cluster of managed products (in SNMP terminology, hosts) to which the server or managed product running the SNMP agent belongs.

SNMP community name
The name assigned to a given SNMP community. Queries from an SNMP management station to a device running an SNMP agent will only elicit a response if those queries are addressed with the correct SNMP community name.

SNMP management station
An SNMP workstation console used to oversee the SNMP network.

SSP
See system services processor.

status bar
This bar is at the bottom on the screen and displays a status symbol that indicates the current state of the switch.

storage area network
A high-performance data communications environment that interconnects computing and storage resources so that the resources can be effectively shared and consolidated.

StorageWorks HA-Fabric Manager

Software application that is the system management framework providing the user interface for managing HP Fibre Channel connectivity products. The HAFM can run both locally on the HAFM server and remotely on a user workstation.

subnet mask
A method of representing the portion of the IP network address that is devoted to subnet addresses (as opposed to the portions of the address that refer to individual hosts or to the organizational network overall).

switchover
Changing a back up FRU to the Active state, and the active FRU to the Backup state.

switch priority
Value configured into each switch in a fabric that determines its relative likelihood of becoming the fabric's principal switch.

system services processor
Controls the RS-232 maintenance port and the Ethernet port of a Fibre Channel switch.

topology
Logical and/or physical arrangement of stations on a network.

trap
Unsolicited notification of an event originating from a SNMP managed device and directed to an SNMP network management station.

trap host
SNMP management workstation that is configured to receive traps.

trunk cable
Cable consisting of multiple fiber pairs that do not directly attach to an active device. This cable usually exists between distribution panels and can be located within, or external to, a building. *Contrast with* jumper cable.

unblocked port
Devices communicating with an unblocked port can log in to the switch and communicate with devices attached to any other unblocked port (assuming that this is supported by the current zoning configuration).

unicast

Communication between a single sender and a single receiver over a network. Compare to *multicast* (communication between a single sender and multiple receivers) and *anycast* (communication between any sender and the nearest of a group of receivers). Similar in meaning to *point-to-point communication*.

universal port module card

Each fiber port module card provides four Fibre Channel connections through duplex small form factor pluggable (SFP) fiber-optic transceivers. 1 or 2 gigabits per second enabled.

uniform resource locator

A standard way of specifying the location of an object, typically a web page, on the Internet. URLs are the form of address used on the world-wide web. They are used in HTML documents to specify the target of a hyperlink which is often another HTML document (possibly stored on another computer).

UPM card

See universal port module card

URL

See uniform resource locator.

user rights

The HAFM's system administrator can assign levels of access, or "User Rights," to Product Manager users through the HAFM application.

vital product data

System-level data stored by the backplane in the electrically erasable programmable read-only memory. This data includes serial numbers and identifies the manufacturer.

VPD

See vital product data.

warning message

Indication that a possible error has been detected. *See als*o error message and information message.

window

A scrollable viewing area on screen. A window may refer to a part of the application, such as the scrollable index window or the text window in the electronic versions of this database, or it may refer to the entire application in a window.

world-wide names
Eight byte address that uniquely identifies a switch, or a node (end device), even on global networks.

wrap plug
See loopback plug.

WWN
See world-wide names.

zone
Set of devices that can access one another. All connected devices may be configured into one or more zones. Devices in the same zone can see each other. Those devices that occupy different zones cannot.

zone member
Specification of a device to be included in a zone. A zone member can be identified by the port number of the switch to which it is attached or by its device (or HBA) world wide name. In multi-switch fabrics, identification of end-devices/nodes by world wide name is preferable.

zone set
See zone.

zoning
Grouping of several devices by function or by location. All devices connected to a connectivity product, such as the switch, may be configured into one or more zones. *See also* zone.

Index

S

SANtegrity feature 6–2
    fabric binding 6–2
SANtegrity features
    switch binding 6–3
save data collection dialog box 1–20
save dialog box 4–2
segmented E_Port messages 2–11
server platform
    customer-supplied 1–1
set online state dialog box 1–20
setting online state 5–3
signal losses, error statistics 2–32
SMTP server address 1–21
SNMP
    configuring 3–13
    introduction 1–2
SNMP agent option 1–17
software licensing 1–10
square, gray, meaning of 1–30
statistics on ports 1–29, 2–29
status bar 1–30
    status symbols 2–4
status symbols 2–4
status table 2–2
switch
    displaying information 2–12
switch binding 6–3, 6–8
    enable and disable 6–4
    membership list 6–5
    state change dialog box 6–4
    zoning function 6–7
switch binding membership list dialog box 6–5
switch menu 1–23
switch parameters
    configuring 3–3
switch priority, default value 3–6

switch properties 2–13
switch properties dialog box 1–23, 2–12, 2–13
switch status 2–4
switch status table 2–2
system error indicator 2–6

T

telnet, enabling 3–28
threshold alert
    configuring 3–19
    log 4–8
    port properties dialog box 2–10
threshold alerts 1–18
triangle, port, meaning for 2–5
triangle, yellow
    meaning of 1–30

U

unit beaconing indicator 2–6
user rights 1–32
username, default 1–1, 1–11

V

versions, firmware 1–21
view menu
    FRU list view 2–23
    node list view 2–23
    performance view 2–27
    port list view 2–20
view panel 1–23
view tabs 1–22

W

warnings
    resetting configurations 1–22
web server, enabling 1–18, 3–28
WWN binding 3–10
WWN binding option 2–18