hp StorageWorks

edge switch 2/24 installation guide

Part Number: AA-RTDWA-TE/958-000283-000

First Edition (January 2003)

This installation guide provides procedures for setting up,
configuring, and managing the Edge Switch 2/24.

hp invent

edge switch 2/24 installation guide
First Edition (January 2003)
Part Number: AA-RTDWA-TE/958-000283-000

Contents

About This Guide

2 Installing and Configuring the Edge Switch 2/24

Tables

About This Guide

This reference guide provides information to help you set up, configure and manage the Edge Switch 2/24.

Intended Audience

This guide 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 data.

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

Any enclosed 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. Contact with this surface could result in injury.

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 presence of multiple sources of power.

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

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 manually handling material.

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.**
- **In single rack installations, the stabilizing feet are attached to the rack.**
- **In multiple rack installations, the racks are coupled.**
- **Only one rack component is extended at any time. A rack may become unstable if more than one rack component is extended for any reason.**

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

Introduction

The HP StorageWorks Edge Switch 2/24 provides dynamic switched connections between Fibre Channel servers and devices in a storage area network (SAN) environment. SANs introduce the concept of server-to-device networking and multi-switch fabrics, eliminate requirements for dedicated connections, and enable the enterprise to become data centric.

A SAN provides speed, high capacity, and flexibility for the enterprise, and is primarily based upon Fibre Channel architecture. The switch implements Fibre Channel technology that provides a bandwidth of 2.125 Gbps, redundant switched data paths, a scalable number of active ports, and long transmission distances.

This chapter describes the switch and attached HP StorageWorks HA-Fabric Manager (HAFM) server. The chapter specifically discusses:

- Switch description including field replaceable units (FRUs) and front and rear panel features.

- Switch management options.

- Operational features.

- Optional kits.

Edge Switch 2/24 Description

The Edge Switch 2/24 provides Fibre Channel connectivity through 24 generic mixed ports (GX_Ports). Switch ports can be configured as:

- Fabric ports (F_Ports) to provide direct connectivity for up to 24 switched fabric devices.

- Fabric loop ports (FL_Ports) to provide arbitrated loop connectivity and fabric attachment for FC-AL devices. Each FL_Port can theoretically support the connection of 126 FC-AL devices.

- Expansion ports (E_Ports) to proved interswitch link (ISL) connectivity to fabric directors and switches.

The switch, shown in Figure 1–1, provides dynamic switched connections for servers and devices, supports mainframe and open-systems interconnection (OSI) computing environments, and provides data transmission and flow control between device node ports (N_Ports) as dictated by the Fibre Channel Physical and Signaling Interface (FC-PH 4.3). Through interswitch links (ISLs), the switch can connect additional switches to form a Fibre Channel multi-switch fabric.

The switch provides connectivity for devices manufactured by multiple original equipment manufacturers (OEMs). To determine if an OEM product can communicate through connections provided by the switch, or if communication restrictions apply, refer to the supporting publications for the product or contact your HP marketing representative.
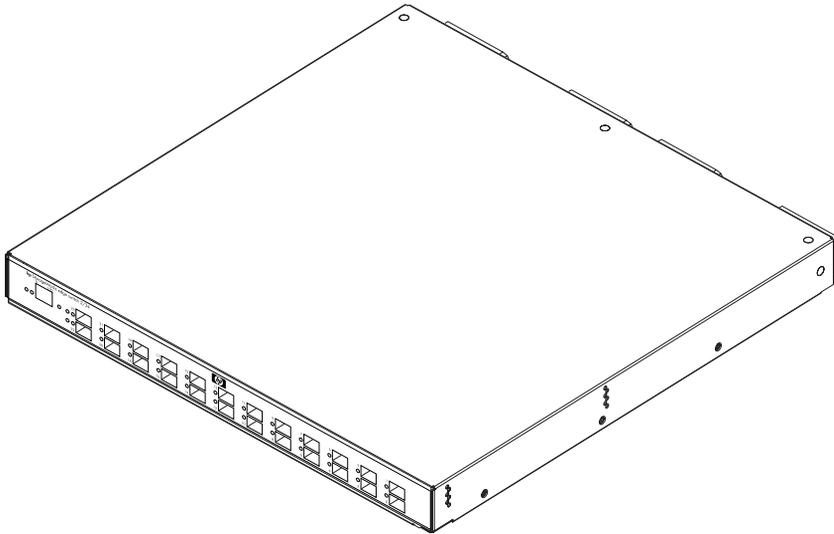
Figure 1–1: Edge Switch 2/24 (front view)

Field Replaceable Units (FRUs)

The switch provides a modular design that enables quick removal and replacement of FRUs, including small form factor pluggable (SFP) optical transceivers and power supply assemblies with internal cooling fans. Edge Switch 2/24 FRUs are detailed in the front and rear panel feature descriptions.

Front Panel Features

Connectors and indicators include the:

- Combined initial machine load and reset (IML/RESET) button.

- Ethernet LAN connector.

- Green power (PWR) and amber system error (ERR) LEDs.

- Green, blue and amber status LEDs associated with FRUs.

Figure 1–2 shows the front panel controls, connectors and indicators.
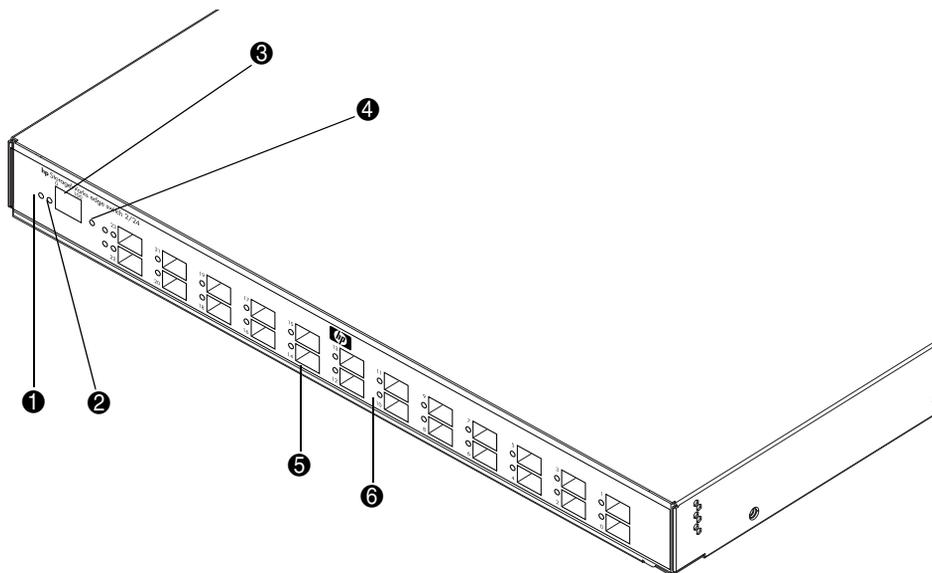
❶ Power LED (green)   ❹ Initial machine load (IML) button
❷ Error LED (amber   ❺ SFP fiber optic connectors
❸ Ethernet LAN connector   ❻ Port LEDs

Figure 1–2: Edge Switch 2/24 front panel features

Power and System Error LEDs

The PWR LED, as shown in Figure 1–2, illuminates when the switch is connected to facility AC power and powered on. If the LED extinguishes, a facility power source, power cord, or power distribution failure is indicated.

The ERR LED, as shown in Figure 1–2, illuminates when the switch detects an event requiring immediate operator attention, such as a FRU failure. The LED remains illuminated as long as an event is active. The LED extinguishes when the Clear System Error Light function is selected from the product manager application.

The LED blinks if unit beaconing is enabled. An illuminated LED (indicating a failure) takes precedence over unit beaconing. The LED also blinks (at twice the beaconing rate) when the IML/RESET button is pressed and held for more than three seconds.

Ethernet LAN Connector

The front panel provides a 10/100 megabit per second (Mbps) RJ-45 twisted-pair connector attaches to an Ethernet LAN to provide communication with the HAFM server or an SNMP management workstation. Two green LEDs are associated with the LAN connector. When illuminated, the left LED indicates LAN operation at 10 Mbps, and the right LED indicates LAN operation at 100 Mbps.

Initial Machine Load Button

The IML/RESET button is shown in Figure 1–2. When the IML/RESET button is pressed, held for three seconds, and released, the switch performs an initial machine load that reloads the firmware from FLASH memory. This operation is not disruptive to Fibre Channel traffic. If the button is held for more than three seconds, the ERR LED blinks at twice the unit beaconing rate.

When the IML/RESET button is pressed and held for ten seconds, the switch performs a reset. After three seconds, the ERR LED blinks at twice the unit beaconing rate. A reset is disruptive and resets the:

- Microprocessor and functional logic for the CTP card and reloads the firmware from FLASH memory.

- Ethernet LAN interface, causing the connection to the HAFM server to drop momentarily until the connection automatically recovers.

- Ports, causing all Fibre Channel connections to drop momentarily until the connections automatically recover. This causes attached devices to log out and log back in, therefore data frames lost during switch reset must be retransmitted.

A reset should only be performed if a CTP card failure is indicated. As a precaution, the IML/RESET button is flush mounted to protect against inadvertent activation.

SFP Transceivers (Fibre Channel Ports)

The Edge Switch 2/24 provides 24 Fibre Channel ports. A single-mode or multi-mode fiber-optic cable attaches to a port through a small form factor pluggable (SFP) transceiver. The SFP provides a duplex LC interface, and can be detached from the switch port for easy replacement. The following fiber-optic transceiver types are available:

- **Shortwave laser** - Shortwave laser SFPs provide short-distance connections (2 to 500 meters) through 50-micron or 62.5-micron multi-mode fiber.

- **Longwave laser** - Longwave laser SFPs provide long-distance connections (up to 10 kilometers) through 9-micron single-mode fiber.

- **Extended longwave laser** - Two types of extended longwave laser transceivers provide connections for transferring 2.125 Gbps data up to 20 kilometers or 35 kilometers through 9-micron singlemode fiber.

Port LEDs

Amber and green/blue LEDs to the left of each Fibre Channel port illuminate, extinguish, or blink to indicate port status and port speed.

- Amber LED - illuminates if the port fails.

- Green/blue LED - illuminates green to indicate 1.0625 Gbps port operation.

- Green/blue LED - illuminates blue to indicate 2.125 Gbps port operation.

Rear Panel Features

The switch provides a modular design that enables quick removal and replacement of field-replaceable power supply assemblies with internal cooling fans. Figure 1–3 illustrates the rear of the switch.

❶   Power supplies with internal   ❷   Maintenance port
      cooling fans (2)
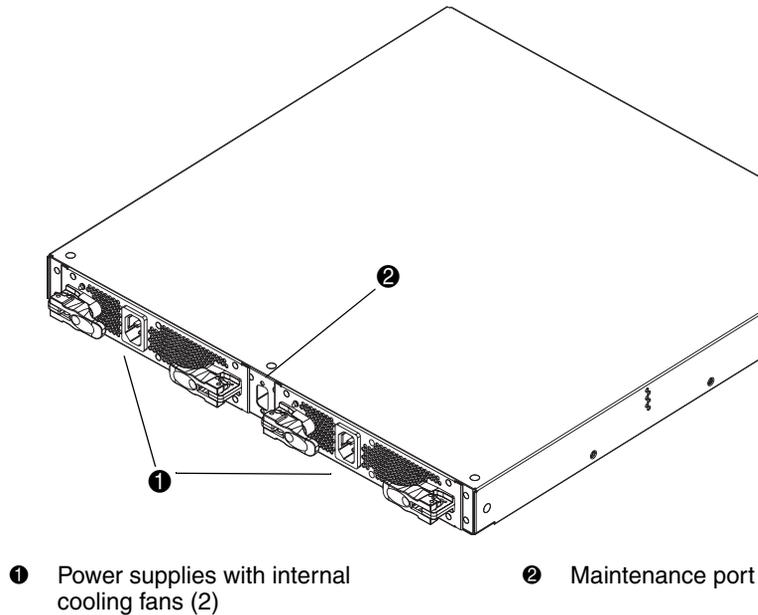
Figure 1–3: Edge Switch 2/24 (Rear View)

Power Supplies

The switch contains two power supply assemblies with internal cooling fans. The redundant, load-sharing power supply assemblies step down and rectify facility input power to provide 3.3 volts direct current (VDC), 5 VDC, and 12 VDC to the control processor (CTP) card. The power supplies also provide input filtering, overvoltage protection, and overcurrent protection. An amber LED on each assembly illuminates if the FRU fails.

Either power supply can be replaced while the switch is operational. Each power supply has a separate connection to the CTP card to allow for independent AC power sources. The power supplies are input rated at 90 to 264 volts alternating current (VAC).

Three cooling fans integrated in each power supply assembly (six fans total) provide cooling for the power supplies and CTP card, as well as redundancy for continued operation if a single fan fails. Fans are removed and replaced as part of the integrated power supply.

Power supply requirements are listed in Appendix B.

Maintenance Port

The rear panel provides a 9-pin DSUB maintenance port, as shown in Figure 1–3, that provides a connection for a local terminal or dial-in connection for a remote terminal. Although the port is typically used by authorized maintenance personnel, operations personnel can use the port to configure switch network addresses.

Switch Management

The switch is managed and controlled through a:

- Customer-supplied PC platform with an Internet connection to the Embedded Web Server (EWS) interface on the switch. Using this graphical user interface (GUI), operators can quickly view switch status. The interface also allows service personnel to perform configuration tasks, view system alerts and related log information, and monitor switch status, port status, and performance. FRU status and system alert information are highly visible.

- Optional High Availability Fabric Manager (HAFM) server with the Java™-based HAFM and Edge Switch 2/24 Product Manager applications installed. The HAFM server is a notebook PC that provides a central point of control for up to 48 switches or managed HP products.

- Customer-supplied remote workstation communicating with the HAFM server through a corporate intranet.

Embedded Web Server (EWS)

Administrators or operators with a browser-capable PC and an Internet connection monitor and manage the switch through the Embedded Web Server (EWS) interface. The EWS interface manages only a single switch, and provides a graphical user interface (GUI) that supports product configuration, statistics monitoring, and basic operation. The EWS interface is opened from a standard web browser running Netscape Navigator 4.6 or higher or Microsoft® Internet Explorer 4.0 or higher.

At the browser, enter the Internet Protocol (IP) address of the switch as the Internet uniform resource locator (URL). When prompted at a login screen, enter a user name and password.

Refer to the *hp StorageWorks embedded web server user guide* for more information.

High Availability-Fabric Manager and Product Manager Applications

As an option, the switch can be managed through an High Availability-Fabric Manager (HAFM) server running the Edge Switch 2/24 Product Manager application. Multiple switches and the HAFM server communicate on a local area network (LAN) through one or more 10/100 Base-T Ethernet hubs. One or more 24-port Ethernet hubs are optional and can be ordered with the switch. Up to three hubs are daisy-chained as required to provide additional Ethernet connections as more switches (or other HP managed products) are installed on a customer network.

Figure 1–4 illustrates the switch, HAFM server, and Ethernet hub.
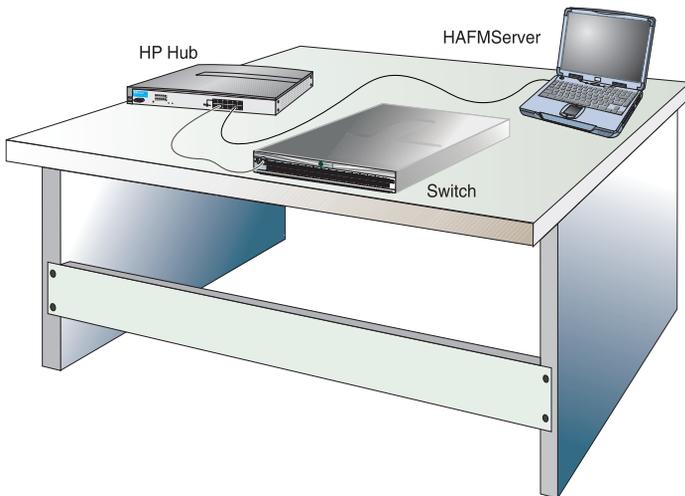
Figure 1–4: Switch, HAFM server, and Ethernet hub

The HAFM server, as shown in Figure 1–5 is a notebook personal computer (PC) that provides a central point of control for up to 48 LAN-connected Directors or Edge Switches.

Figure 1–5: HAFM server

The server is mounted in a slide-out drawer in the HP-supplied equipment rack. The HAFM server or Ethernet access to the embedded web server (EWS) interface is required to install, configure, and manage the Edge Switch 2/24.

Although a configured switch operates normally without HAFM server intervention, an attached server should operate at all times to monitor switch operation, log events and configuration changes, and report failures.

The HAFM server provides an auto-detecting 10/100 Mbps LAN connection, provided by an internal Ethernet adapter card. This LAN port attaches to the customer's public intranet to allow access from remote user workstations. An optional Ethernet adapter card (not supplied by HP) can be installed in the personal computer memory card international association (PCMCIA) slot to provide a connection to a private LAN segment for dedicated director communication.

Remote Workstations

Using a standard web browser, the HAFM and Edge Switch 2/24 Product Manager applications can be downloaded and installed on remote user workstations that are LAN-attached to the HAFM server. Operators at these workstations can manage and monitor switches controlled by the HAFM server. A maximum of nine concurrent users (eight remote users and one local user) can log in to the HAFM application. Each remote workstation must have access to the LAN segment on which the HAFM server is installed. Switch administrative functions are accessed through the LAN and HAFM serve.

LAN Interface Options

The LAN interface can be:

*   Part of the dedicated 10/100 Mbps segment that provides access to managed switches. This switch-to-HAFM server connection is part of the required equipment installation. Connection of remote workstations can be through an Ehternet hub supplied by HP or through the customer intranet.

    If only one HAFM server connection is used and this connection is provided through the customer intranet, functions provided by the HAFM server are available to all users.

    Dual LAN connections provide a dedicated LAN segment that isolates the HAFM server and managed switches from unauthorized users.

    Part of a second HAFM server interface that connects to a customer intranet and allows operation of the Edge Switch 2/24 Product Manager application from remote user PCs or workstations. Connection to this LAN segment is optional and depends on customer requirements.

Minimum Remote Workstation Requirements

Client HAFM and Product Manager applications download and install to remote workstations (from the HAFM server) using a standard web browser. The applications operate on platforms that meet the following minimum system requirements:

- Desktop or notebook PC with color monitor, keyboard, and mouse, using an Intel Pentium® processor with a 400 MHz or greater clock speed, and using the Microsoft Windows® 95, Windows 98, Windows 2000, Windows XP, Windows NT 4.0, or Linux 2.2 operating system.

- Unix workstation with color monitor, keyboard, and mouse, using a:

  — Hewlett-Packard HA PA-RISC® processor with a 400 MHz or greater clock speed, using the HP-UX® 11 or higher operating system.

  — Sun® Microsystems UltraSPARC™ II processor with a 400 MHz or greater clock speed, using the SunOS™ Version 5.5.1 or higher operating system, or Solaris™ Version 2.5.1 or higher operating system.

  — IBM PowerPC® microprocessor with a 400 MHz or greater clock speed, or POWER3™ microprocessor with a 400 MHz or greater clock speed, using the AIX Version 4.3.3 or higher operating system.

- At least 15 MB available on the internal hard drive.

- 128 MB or greater RAM.

- Video card supporting 256 colors at 800 x 600 pixel resolution.

- Ethernet network adapter.

- Java-enabled Internet browser, such as Microsoft Internet Explorer (Version 4.0 or later) or Netscape Navigator® (Version 4.6 or later).

Refer to the *hp StorageWorks HAFM server installation guide* and the *hp StorageWorks high availability-fabric manager user guide* for more information.

Command Line Interface

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 *hp StorageWorks CLI reference guide for directors and edge switches* for more information.

Operational Features

The Edge Switch 2/24 supports several operational features including:

- Advanced error detection, reporting and serviceability.

- Ability to create logical zones and zone sets.

- Support for multi-switch fabrics.

- Software diagnostics to aid in fault isolation and repair.

Error-Detection, Reporting, and Serviceability Features

The switch provides the following error detection, reporting, and serviceability features:

- Light-emitting diodes (LEDs) on switch FRUs and adjacent to Fibre Channel ports that provide visual indicators of hardware status or malfunctions.

- Redundant FRUs (SFP transceivers and integrated cooling fan and power supply assemblies) that are removed or replaced without disrupting switch or Fibre Channel link operation.

- A modular design that enables quick removal and replacement of FRUs without the use of tools or equipment.

- System alerts and logs that display switch, Ethernet link, and Fibre Channel link status at the EWS interface, HAFM server or remote workstation.

- Diagnostic software that performs power-on self-tests (POSTs) and port diagnostics (loopback tests).

- An RS-232 maintenance port at the rear of the switch (port access is password-protected) that enables installation or service personnel to change the switch's IP address, subnet mask, and gateway address.

  These parameters can also be changed through a Telnet session, access for which is provided through a local or remote PC with an Internet connection to the switch.

- Data collection through the EWS interface or Product Manager application to help isolate system problems. The data includes a memory dump file and audit, hardware, and engineering logs.

- Beaconing to assist service personnel in locating a specific port or switch. When port beaconing is enabled, the amber LED associated with the port flashes. When unit beaconing is enabled, the system error indicator on the front panel flashes. Beaconing does not affect port or switch operation.

- An external modem for use by support personnel to dial-in to the HAFM server (optional) for event notification and to perform remote diagnostics.

- Automatic notification of significant system events (to support personnel or administrators) through e-mail messages or the call-home feature.

- SNMP management using the Fibre Channel Fabric Element MIB (Version 2.2), Transmission Control Protocol/Internet Protocol (TCP/IP) MIB-II definition (RFC 1213), or a product-specific MIB that runs on the switch. Up to six authorized management workstations can be configured through the EWS interface and Product Manager application to receive unsolicited SNMP trap messages. The trap messages indicate product operational state changes and failure conditions.

- Optional SNMP management using the Fibre Alliance MIB that runs on the HAFM server. Up to 12 authorized management workstations can be configured through the HAFM application to receive unsolicited SNMP trap messages. The trap messages indicate operational state changes and failure conditions.

NOTE: For more information about SNMP support provided by Hewlett-Packard products, refer to the *hp StorageWorks SNMP reference guide for directors and edge switches*.

Zoning

The switch supports a name server zoning feature that partitions attached devices into restricted-access groups called zones. Devices in the same zone can recognize and communicate with each other through switched port-to-port connections. Devices in separate zones cannot communicate with each other.

Zoning is configured by authorizing or restricting access to name server information associated with device N_Ports that attach to switch fabric ports (F_Ports). A zone member is specified by the port number to which a device is attached, or by the eight-byte (16-digit) World Wide Name (WWN) assigned to the host bus adapter (HBA) or Fibre Channel interface installed in a device. A device can belong to multiple zones.

> ⚠ **CAUTION:** If zoning is implemented by port number, a change to the switch fiber-optic cable configuration disrupts zone operation and may incorrectly include or exclude a device from a zone.
>
> If zoning is implemented by WWN, removal and replacement of a device HBA or Fibre Channel interface (thereby changing the device WWN) disrupts zone operation and may incorrectly include or exclude a device from a zone.
>
> In Open Fabric mode, only zoning by WWN is supported. Zoning by port numbers is not.

Zones are grouped into zone sets. A zone set is a group of zones that is enabled (activated) or disabled across all switches in a multi-switch fabric. Only one zone set can be enabled at one time.

Multi-Switch Fabrics

A Fibre Channel topology that consists of one or more interconnected switches or switch elements is called a fabric. Operational software provides the ability to interconnect switches (through expansion port (E_Port) connections) to form a multi-switch fabric. The data transmission path through the fabric is typically determined by fabric elements and is user-transparent. Subject to zoning restrictions, devices attached to any interconnected switch can communicate with each other through the fabric.

Software Diagnostics

The switch provides the following diagnostic software features that aid in fault isolation and repair of problems:

- FRUs provide on-board diagnostic and monitoring circuits that continuously report FRU status to the Embedded Web Server (EWS), HAFM and product manager applications. These applications provide system alerts and logs that display failure and diagnostic information at the HAFM server or a remote workstation communicating with the HAFM server.

- The HAFM Services application that runs as a Windows 2000 service and provides an additional user interface to display operational status.

- The embedded web server interface that provides Internet access to isolate problems for a single switch.

- Unsolicited SNMP trap messages that indicate operational state changes or failures can be transmitted to up to 12 authorized management workstations.

- E-mail messages or call-home reports provide automatic notification of significant system events to designated support personnel or administrators.

Optional Kits

Contact your Hewlett-Packard authorized service provider to purchase the following optional Edge Switch 2/24 kits. See Table 1–1.

Table 1–1: Edge Switch 2/24 Optional Kits

Supporting Kit	Description
8-flexport upgrade for Edge Switch 2/24, Part Number: DS-DMGGE-BE / 316096-B21	Used to upgrade the Edge Switch 2/24 from: • 8 to 16 ports • 16 to 24 ports.
Edge Switch 2/24 product manager license, Part Number: QM-70GAA-AA / 317067-B21	Used when switch is managed through HAFM.

2

Installing and Configuring the Edge Switch 2/24

This chapter describes tasks to install, configure, and verify operation of the Edge Switch 2/24. The switch can be installed on a table or desk top, or mounted in any standard equipment rack.

For a list of the factory-set defaults for the switch and the Reset Configuration option, refer to Appendix B.

Summary of Installation Tasks

Table 2–1 summarizes installation tasks for the switch, HAFM server, and Ethernet hub. The table numbers and describes each task, states if the task is required or optional, and lists the page reference for the task. If a task is optional, decision-related information is included.

Table 2–1: Installation Task Summary

Task Number and Description	Required or Optional	Page
Task 1: Verify Installation Requirements	Required	2–3
Task 2: Unpack, Inspect, and Install the Ethernet Hub (Optional)	Optional—install only if ordered and Ethernet segment does not exist to connect switches and the HAFM server.	2–4
Task 3: Unpack, Inspect, and Install the Switch	Required	2–4
Task 4: Configure the Switch from the Embedded Web Server (Optional)	Optional—if not done, then the switch should be configured using the HAFM server.	2–6

Table 2–1: Installation Task Summary (Continued)

Task Number and Description	Required or Optional	Page
Task 5: Configure Network Information	Optional—configure if connecting multiple switches or if connecting a switch and HAFM server to a public LAN.	2–29
Task 6: LAN-Connect the Switch	Required	2–35
Task 7: HAFM server (Optional)	Optional—if not done, then the switch should be configured using the embedded web server (EWS) interface.	2–35
Task 8: Configure the Switch to the HAFM Application	Required if Task 7: HAFM server (Optional) task was done.	2–36
Task 9: Record or Verify HAFM Server Restore Information	Required if Task 7: HAFM server (Optional) task was done.	2–36
Task 10: Verify Switch-to-HAFM Server Communication	Required if Task 7: HAFM server (Optional) task was done.	2–37
Task 11: Configure Feature Key (Optional)	Optional—configure if a feature key is ordered by the customer.	2–39
Task 12: Configure Open Systems Management Server (Optional)	Optional—configure if the HAFM server is installed.	2–41
Task 13: Set Switch Date and Time	Required	2–41
Task 14: Configure the Edge Switch 2/24 Product Manager Application	Required	2–43
Task 15: Test Remote Notification (Optional)	Optional	2–65
Task 16: Back Up HAFM Configuration Data	Required	2–66
Task 17: Cable Fibre Channel Ports	Required	2–66
Task 18: Connect Switch to a Fabric (Optional)	Optional—perform this task to connect the switch to a fabric.	2–67

Installation Options

The switch is installed in one of two configurations. The options are:

- **Table or desk top—**one or more switches, an optional HAFM server, and an optional Ethernet hub are delivered and installed at the customer facility on a desk or table top. Ethernet cabling distance, and local area network (LAN) addressing issues must be considered.

- **Customer-supplied equipment rack—**one or more switches, an optional HAFM server, and an optional Ethernet hub are delivered to the customer facility for installation in a customer-supplied equipment rack. Rack-mount hardware is provided in the shipping container. Ethernet cabling, distance, and LAN addressing issues must be considered.

Task 1: Verify Installation Requirements

Verify the following requirements are met prior to switch and HAFM server installation. Ensure:

- A site plan is prepared, configuration planning tasks are complete, planning considerations are evaluated, and related planning checklists are complete. Fabric and device connectivity are evaluated, and the related planning worksheet is complete. Refer to the *hp StorageWorks SAN high availability planning guide*.

- Support is available for one of the following switch management methods:

  - A browser-capable PC and Internet connectivity to support switch management through the Embedded Web Server (EWS) interface, or

  - The HAFM server and LAN segment connectivity to support switch management through the HAFM and Product Manager applications.

- Support equipment and personnel are available for the installation.

- The required number and type of fiber-optic jumper cables are delivered and available. Ensure the cables are the correct length with the required connectors.

- A customer-supplied equipment rack and associated hardware are available (optional).

- Remote workstations or simple network management protocol (SNMP) workstations are available (optional). Workstations are customer-supplied and connected through a corporate or dedicated LAN.

Task 2: Unpack, Inspect, and Install the Ethernet Hub (Optional)

The HAFM server and one or more switches connect through an Ethernet hub installed on a 10/100 Mbps LAN segment. One hub port is required to connect the HAFM server, and one hub port is required to connect each switch. A combination of up to 48 HP products can be configured and managed by a single HAFM server, therefore multiple hubs may be required to provide sufficient port connections. These hubs must be connected in accordance with the hub manufacturer's specifications. HP recommends using a star or hub-and-spoke topology when connecting multiple hubs. The HAFM server must be connected to the center hub, and there should never be more than two hubs between the HAFM server and any switch. Refer to the hub manufacturer's documentation for more detailed information.

For instructions to unpack and inspect one or more Ethernet hubs, and install the hubs in a desktop or rack-mount configuration, refer to the appropriate Ethernet hub documentation.

Task 3: Unpack, Inspect, and Install the Switch

This section describes how to unpack and inspect the Edge Switch 2/24, and install it in a desktop or rack-mount configuration.

Unpack and Inspect the Switch

Unpack and inspect the switch:

$\triangle$ **CAUTION:** When you remove the switch from the carton, do not rest it on its rear window while examining it. To do so may break the FRU handles.

1. Inspect the shipping containers for damage caused during transit. If a container is damaged, ensure a representative from the freight carrier is present when the container is opened.

2. Unpack the shipping containers and inspect each item for damage. Save all shipping and packing materials. Ensure that all items on the enclosed shipping list are in each container.

3. If any items are damaged or missing, customers should contact a Hewlett-Packard authorized service provider or reseller.

Desktop Installation

To install and configure the switch on a desktop:

1. Remove the backing from the three adhesive rubber pads and apply the pads to the underside of the switch. Ensure the pads are aligned with the scribed circles in the front and rear of the switch.

2. Position the switch on a table or desktop as directed by the customer. Ensure:

   • Grounded AC electrical outlets are available.

   • Adequate ventilation is present.

   • Areas with excessive heat, dust, or moisture are avoided.

   • All planning considerations are met. Refer to the *hp StorageWorks SAN high availability planning guide*.

3. Verify all field-replaceable units (FRUs), including small form factor pluggable (SFP) optical transceivers and combined cooling fan and power supply assemblies are installed as ordered.

4. Connect the U.S. or country-specific (optional) AC power cords to the right (**PS0**) and left (**PS1**) receptacles at the rear of the chassis.

> ⚠ **WARNING: An HP-supplied power cord is provided for each switch power supply. To prevent electric shock when connecting the switch to primary facility power, use only the supplied power cords, and ensure the facility power receptacle is the correct type, supplies the required voltage, and is properly grounded.**

5. Connect the remaining ends of the AC power cords to separate facility power sources that provide single-phase, 120 to 240 volt alternating current (VAC) current. This provides power redundancy.

6. When the first power cord is connected, the switch powers on and performs power-on self-tests (POSTs). During POSTs:

   a. The green power (**PWR**) LED on the front panel illuminates.

   b. The amber system error (**ERR**) LED on the front panel blinks momentarily while the switch is tested.

    c.   The green LEDs associated with the Ethernet port blink momentarily while the port is tested.

    d.   The green/blue and amber LEDs associated with Fibre Channel ports blink momentarily while the ports are tested.

7.   After successful POST completion, the green power (**PWR**) LED remains illuminated and all other front panel LEDs extinguish.

8.   If a POST error or other malfunction occurs, refer to the *hp StorageWorks edge switch 2/24 service manual* to isolate the problem.

Rack-Mount Installation

To install the switch in a customer-supplied equipment rack, refer to the *hp StorageWorks edge switch 2/24 rack mount kit installation instructions* included with the switch hardware.

Task 4: Configure the Switch from the Embedded Web Server (Optional)

If an HAFM server is not available, use the embedded web server (EWS) interface to configure the Edge Switch 2/24. Selectively perform the following configuration tasks according to your installation requirements:

- Configure the switch ports.
- Configure the switch identification, date and time, operating parameters, and network addresses.
- Configure SNMP trap message recipients, enable the command line interface (CLI), and configure the open systems management server (OSMS) feature.
- Configure user passwords.

NOTE: This section covers the initial set up of the Edge Switch 2/24. For additional information regarding setting up zoning, zone sets, and SAN management in general, see the online EWS help or the *hp StorageWorks embedded web server user guide*.

A PC platform with LAN access and standard web browser running Netscape Navigator 4.6 or higher or Microsoft Internet Explorer 4.0 or higher is required. To open the embedded web server interface:

1.   Ensure the browser-capable PC and the Ethernet LAN segment (with the switch attached) are connected.

2. At the PC, launch the browser application (Netscape Navigator or Internet Explorer).

3. At the browser, enter the IP address of the switch as the internet uniform resource locator (URL). Use the default IP address of 10.1.1.10, the factory preset of 10.1.1.10, or the IP address configured while performing "Task 5: Configure Network Information" on page 2–29. The **Username and Password Required** dialog box displays, as shown in Figure 2–1.

Figure 2–1: Username and Password Required dialog box

4. Type the default user name and password.

   NOTE: The default user name is *Administrator* and the default password is *password*. The user name and password are case-sensitive.

5. Click **OK**. The embedded web server interface opens with the **View** window displayed, as shown in Figure 2–2.
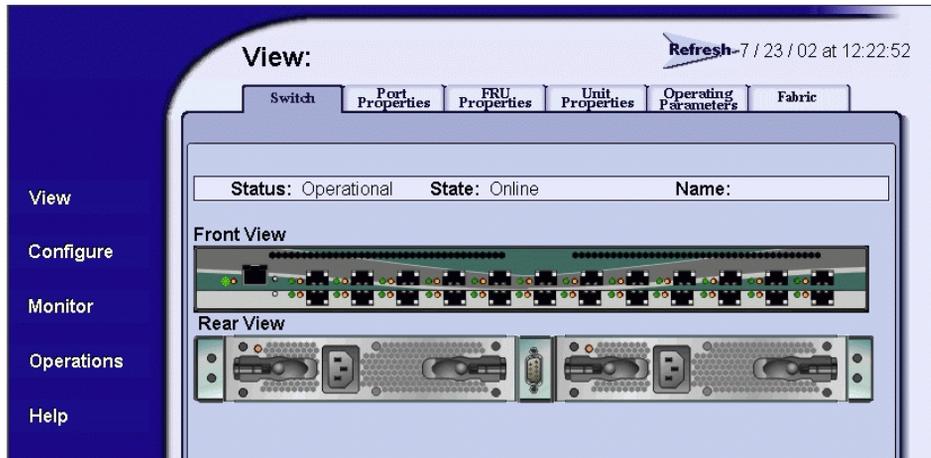
Figure 2–2: Embedded web server interface—View window

Configure Switch Ports

Perform the procedure in this section to configure names and operating characteristics for the switch ports.

To configure one or more ports:

1. At the **View** window, click **Configure** at the left side of the window. The **Configure** window opens with the **Ports** tab displayed.

    a. For each port to be configured, type a port name of 24 alphanumeric characters or less in the associated **Name** field. The port name should identify the device to which the port is attached.

    b. Choose the check box in the **Blocked** column to block or unblock a port (default is unblocked). A check mark in the box indicates the port is blocked. Blocking a port prevents the attached device from communicating with the switch. A blocked port continuously transmits the offline sequence (OLS), as shown in Figure 2–3.
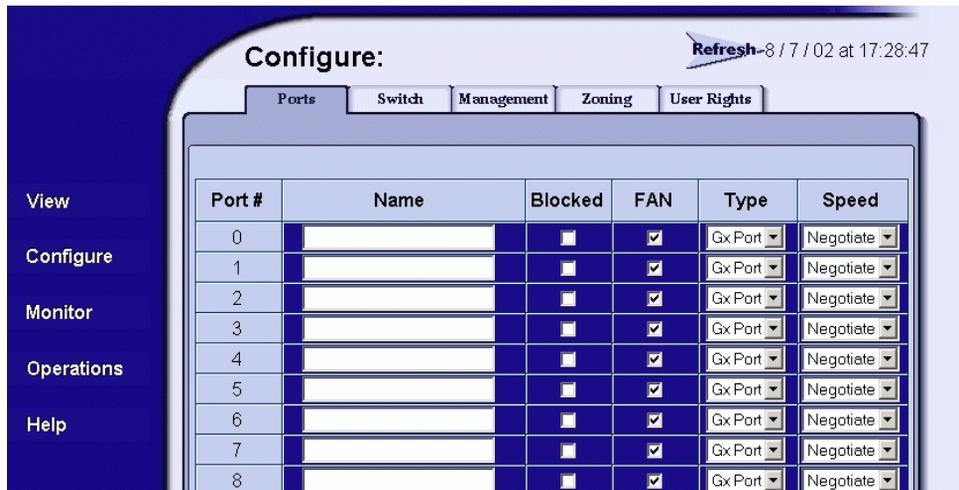
Figure 2–3: Block or unblock a port from the Configure window

    c. Choose the check box in the **10-100 km** column to enable extended distance buffering for a port (default is disabled). A check mark in the box indicates extended distance operation up to 100 kilometers (through repeaters) is enabled.

d. Select a **Type** field and choose generic port (**G_Port**), fabric port (**F_Port**), or expansion port (**E_Port**) from the list box. If **F_Port** or **E_Port** is selected, the port will only operate as the port type selected. If **G_Port** is selected, the port type is automatically detected and will operate as an E_Port or F_Port.

e. Click the **Speed** field for a port. A **Speed** drop-down list displays. Choose 1 Gb/sec, 2 Gb/sec, or Navigate as the desired setting depending on the speed capability of the device to be plugged into the port.

2. Click **Activate** to save the information. The message "`Your changes to the port configuration have been successfully activated`" displays.

Configure Switch Identification

Perform this procedure to configure the switch name, description, location, and contact person. The `Name`, `Location`, and `Contact` variables configured here correspond respectively to the SNMP variables `sysName`, `sysLocation`, and `sysContact`. These variables are used by SNMP management workstations when obtaining data from managed switches.

To configure the switch identification:

1. At the **Configure** window, click the **Switch** tab. The **Switch** page displays with **Identification** tab selected, as shown in Figure 2–4.
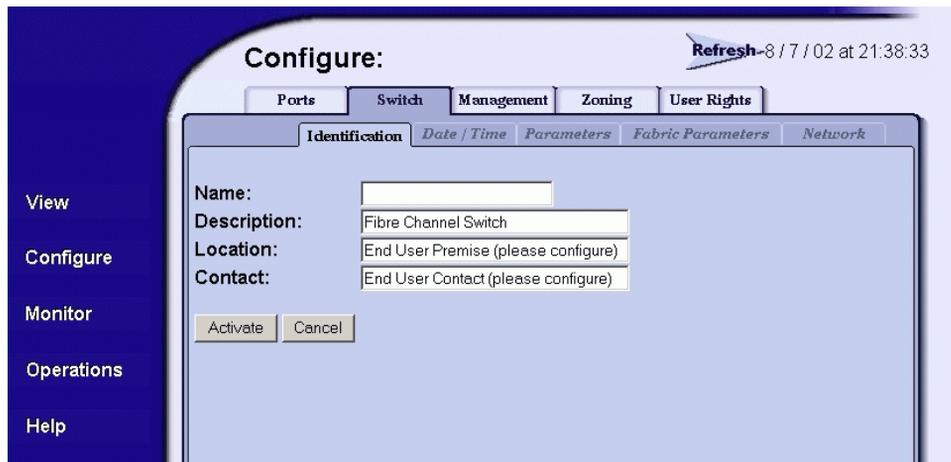
Figure 2–4: Switch page—Identification tab

a. Type a switch name of 24 alphanumeric characters or less in the **Name** field. Each switch should be configured with a unique name.

    If the switch is installed on a public LAN, the name should reflect the switch's Ethernet network DNS host name. For example, if the DNS host name is hpes224.hp.com, then enter `hpes224.`

b. Type a switch description of 255 alphanumeric characters or less in the **Description** field.

c. Type the switch physical location (255 alphanumeric characters or less) in the **Location** field.

d. Type the name of a contact person (255 alphanumeric characters or less) in the **Contact** field.

2. Click **Activate** to save the information. The message "`Your changes to the identification configuration have been successfully activated`" displays.

Configure Date and Time

Perform this procedure to configure the effective date and time for the switch. To set the date and time:

1. At the **Configure** window, click the **Switch** tab, then select **Date/Time** tab. The Switch page displays with **Date/Time** tab selected (highlighted red), as shown in Figure 2–5.
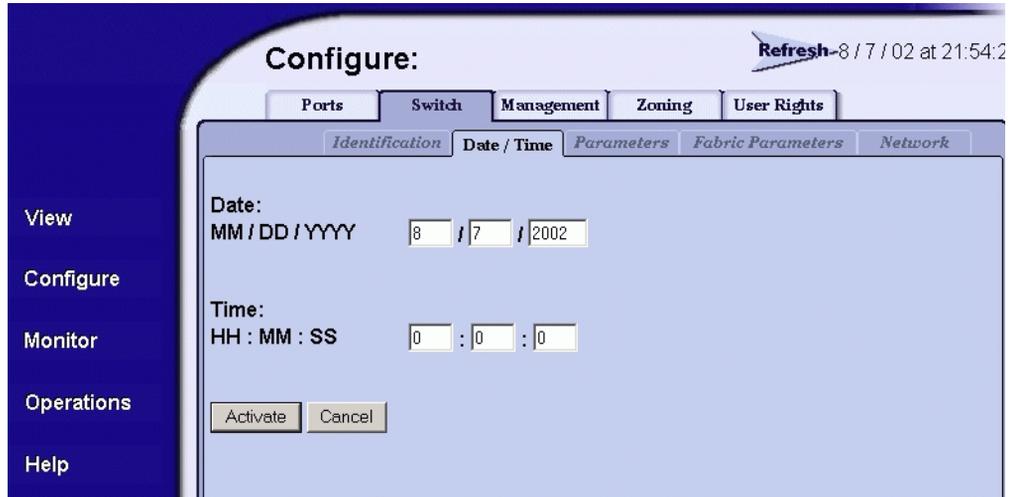
Figure 2–5: Switch page—Date/Time tab

    a. Click the **Date** fields that require change, and type numbers in the following ranges:

    Month (MM): 1 through 12
    Day (DD): 1 through 31
    Year (YY): greater than 1980

    b. Click the **Time** fields that require change, and type numbers in the following ranges:

    Hour (HH): 0 through 23
    Minute (MM): 0 through 59
    Second (SS): 0 through 59

2. Click **Activate** to save the information. The message "Your changes to the date/time configuration have been successfully activated" displays.

Configure Operating Parameters

The switch must be set offline to configure operating parameters. To configure the parameters:

1. Set the switch offline as follows:

    a. Choose **Operations** at the left side of the window. The **Operations** window opens with the **Switch** tab displayed.

    b. At the **Switch** tab, click the **Online State** tab, then click **Set Offline**. The message "Your operations changes have been successfully activated" displays.

2. Choose **Configure** at the left side of the window. The **Configure** window opens with the **Ports** tab displayed.

3. At the **Configure** window, click the **Switch** tab, then click the **Parameters** tab. The **Switch** page displays with **Parameters** tab selected, as shown in Figure 2–6.

Figure 2–6: Switch page—Parameters tab

a. At the **Preferred Domain ID** field, type a value between 1 through 31. The domain ID uniquely identifies each switch in a fabric.

If the switch is attached to a fabric element, the switch and element must have unique domain IDs. If the values are not unique, the E_Port connection to the element segments and the switch cannot communicate with the fabric.

b. At the **Insistent Domain ID** field, select **Enabled** or **Disabled**. When this parameter is enabled, the domain ID configured in the **Preferred Domain ID** field becomes the active domain identification when the fabric initializes. This parameter is enabled only if the optional SANtegrity feature is installed.

c. At the **Rerouting Delay** field, select **Enabled** or **Disabled**. When this parameter is enabled, traffic is delayed through the fabric by the specified error detect time out value (E_D_TOV). This delay ensures Fibre Channel frames are delivered to their destination in order, even if a change to the fabric topology creates a new (shorter) transmission path.

d. At the **Domain RSCNs** field, select **Enabled** or **Disabled**. When this parameter is enabled, attached devices can register to receive notification when another attached device changes state.

4. Click **Activate** to save and activate the changes. The message "Your changes to the operating parameters configuration have been successfully activated" appears.

5. If fabric parameters require configuration, go on to Configure Fabric Parameters. If the configuration is complete, set the switch online as follows:

a. At the **Configure** panel, select the **Operations** option at the left side of the panel. The **Operations** panel opens and the **Switch** page displays with the **Beacon** tab selected

b. Click the **Online State** tab, then click **Set Online**. The message "Your operations changes have been successfully activated" displays.

Configure Fabric Parameters

Perform this procedure to configure the fabric operating parameters, including resource allocation time out value (R_A_TOV), E_D_TOV, switch priority, and interop mode. The switch must be set offline. To configure parameters:

1. If required, set the switch offline as follows:

   a. At the **Configure** panel, select the **Operations** option at the left side of the panel. The **Operations** panel opens and the **Switch** page displays with the **Beacon** tab selected

   b. Click the **Online State** tab, then click **Set Offline**. The message "`Your operations changes have been successfully activated`" appears.

2. At the **Operations** panel, select the **Configure** option at the left side of the panel. The **Configure** panel opens with the **Ports** page displayed.

3. At the **Configure** panel, click the **Switch** tab, then click the **Fabric Parameters** tab. The **Switch** page displays with the **Fabric Parameters** tab selected, as shown in Figure 2–7.
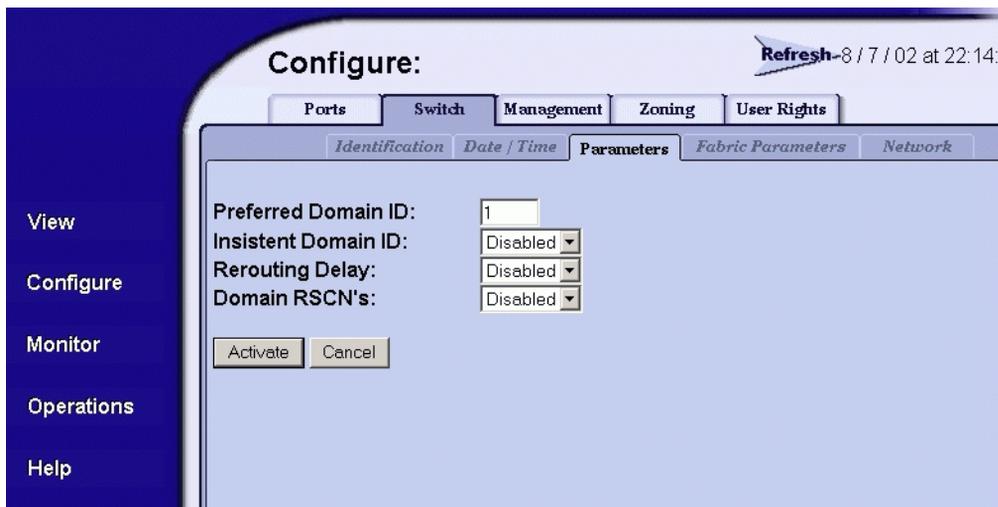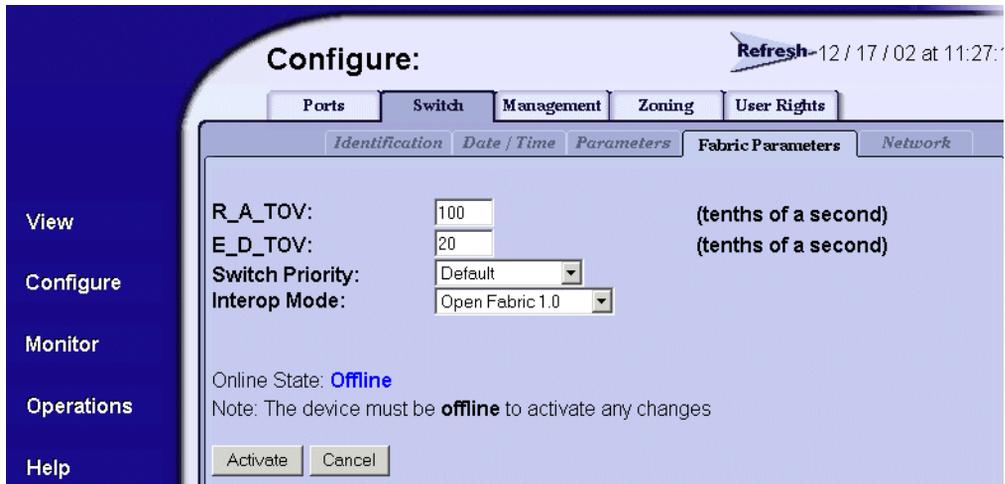

Figure 2–7: Switch page—Fabric Parameters tab

a. At the **R_A_TOV** field, type a value between 10 through 1200 tenths of a second (one through 120 s). The default is 100 tenths of a second (10 s).

> **NOTE:** All fabric-attached switches must be set to the same R_A_TOV. If the value is not compatible, the E_Port connection to the switch segments and the switch cannot communicate with the fabric. In addition, the R_A_TOV must be greater than the E_D_TOV.

b. At the **E_D_TOV** field, type a value between 2 through 600 tenths of a second (0.2 through 60 s). The default is 20 tenths of a second (2 s).

> **NOTE:** All fabric-attached switches must be set to the same E_D_TOV. If the value is not compatible, the E_Port connection to the switch segments and the switch cannot communicate with the fabric. In addition, the E_D_TOV must be less than the R_A_TOV.

c. Select from the **Switch Priority** drop-down list to set the switch priority. Available selections are **Default**, **Principal**, and **Never Principal**. The default setting is **Default**.

This value designates the fabric's principal switch. The principal switch is assigned a priority of 1 and controls the allocation and distribution of domain IDs for all fabric elements (including itself).

Principal is the highest priority setting, **Default** is the next highest, and **Never Principal** is the lowest priority setting. The setting **Never Principal** means the switch is incapable of becoming a principal switch. If all switches are set to **Principal** or **Default**, the switch with the highest priority and the lowest world wide name (WWN) becomes the principal switch.

At least one switch in a fabric must be set as **Principal** or **Default**. If all switches are set to **Never Principal**, all interswitch links (ISLs) segment.

d. Select from the **Interop Mode** drop-down list to set the switch operating mode. This setting only affects the mode used to manage the switch; it does not affect port operation. Available selections are:

— **Homogeneous Fabric -** Select this option (default) if the switch is fabric-attached only to other HP StorageWorks directors or switches operating in Homogeneous fabric mode.

— **Open Fabric 1.0 -** Select this option for managing heterogeneous fabrics and if the switch is fabric-attached to HP directors or switches and open-fabric compliant switches produced by other original equipment manufacturers (OEMs).

4. Click **Activate** to save the information. The message, `Your changes to the operating parameters configuration have been successfully activated`, displays.

5. Set the switch online as follows:

   a. Choose **Operations** at the left side of the window. The **Operations** window opens with the **Switch** tab displayed.

   b. At the **Switch** tab, click the **Online State** tab, then click **Set Online**. The message, `Your changes to the operating parameters configuration have been successfully activated`, displays.

Configure Network Information

Verify the type of LAN installation with the customer's network administrator. If one switch is installed on a dedicated LAN, network information (IP address, subnet mask, and gateway address) does not require change. Go to "Configure Switch Ports" on page 2–53.

If multiple switches are installed, or a public LAN segment is used, network information must be changed to conform to the customer's LAN addressing scheme. Perform one of the following:

- If network information was changed while performing "Task 5: Configure Network Information" on page 2–29, this procedure is not required. Go to "Configure SNMP Trap Message Recipients" on page 2–55.

- If network information was not changed, perform this procedure.

Perform the following steps to change a switch IP address, subnet mask, or gateway address.

1. Choose **Configure** at the left side of the window. The **Configure** window opens with the **Ports** page displayed.

2. At the **Configure** window, click the **Switch** tab, then click the **Network** tab. The **Switch** page displays with the **Network** tab selected, as shown in Figure 2–8.
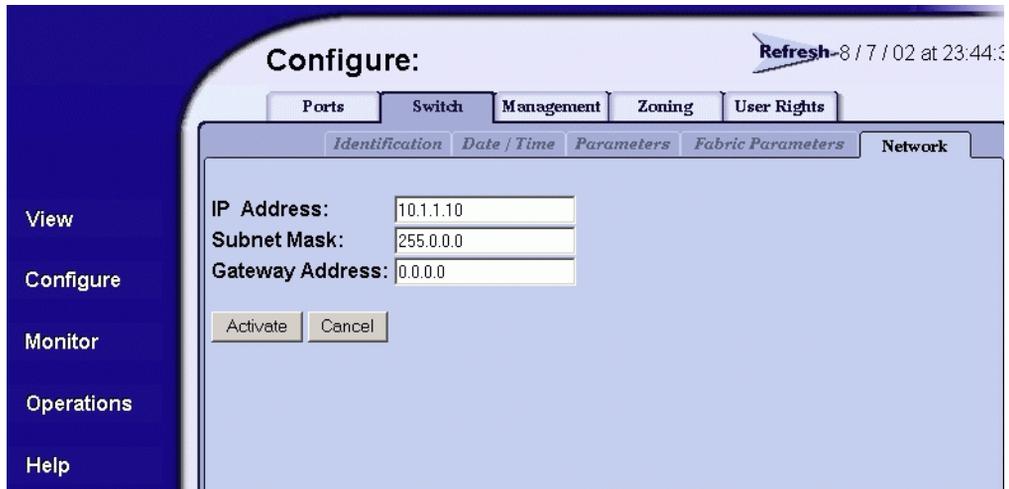
Figure 2–8: Switch page—Network tab

> a. At the **IP Address** field, type the new value as specified by the customer's network administrator (default is *10.1.1.10*, factory preset is *10.1.1.10*).
>
> b. At the **Subnet Mask** field, type the new value as specified by the customer's network administrator (default is *255.0.0.0*).
>
> c. At the **Gateway Address** field, type the new value as specified by the customer's network administrator (default is *0.0.0.0*).

3. Click **Activate** to save the information. The following message box displays, as shown in Figure 2–9.
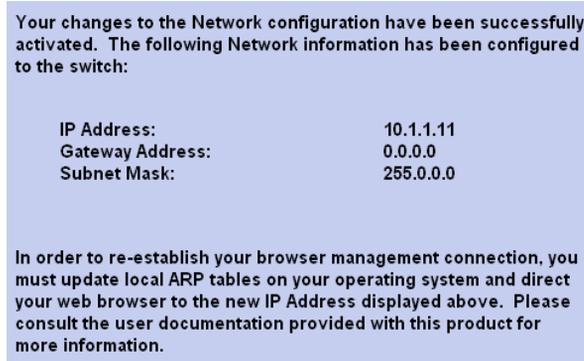
Figure 2–9: Network configuration changes activated

4. Update the address resolution protocol (ARP) table for the browser PC.

   a. Choose **File >Exit** to close the embedded web server and browser applications. The Windows desktop displays.

   b. Choose **Start > Programs** > **Command Prompt**. A disk operating system (DOS) window displays.

   c. Delete the switch's *old* IP address from the ARP table. At the command (C:\) prompt, type arp -d xxx.xxx.xxx.xxx, where xxx.xxx.xxx.xxx is the old IP address for the switch.

   d. Click close (**X**) at the upper right corner of the DOS window to close the window or enter exit at the prompt to return to the Windows desktop.

5. At the PC, launch the browser application (Netscape Navigator or Internet Explorer).

6. At the browser, enter the switch's *new* IP address as the Internet URL. The **Username and Password Required** dialog box displays.

7. Type the default user name and password.

   NOTE: The default user name is *Administrator* and the default password is *password*. The user name and password are case-sensitive.

8. Click **OK**. The embedded web server interface opens with the **View** window displayed.

Configure SNMP Trap Message Recipients

Perform this procedure to configure community names, write authorizations, and network addresses and for up to 6 SNMP trap message recipients. A trap recipient is a management workstation that receives notification (through SNMP) if a switch event occurs.

To configure SNMP trap recipients:

1. Choose **Configure** at the left side of the window. The **Configure** window opens with the **Ports** tab displayed.

2. At the **Configure** window, click the **Management** tab. The **Management** page displays with **SNMP** tab selected, as shown in Figure 2–10.

Figure 2–10: Management page—SNMP tab

> a. For each trap recipient to be configured, type a community name of 32 alphanumeric characters or less in the associated **Community Name** field. The community name is incorporated in SNMP trap messages to ensure against unauthorized viewing or use.
>
> b. Click the check box in the **Write Authorization** column to enable or disable write authorization for the trap recipient (default is disabled). A check mark in the box indicates write authorization is enabled. When the feature is enabled, a management workstation user can change `sysContact, sysName`, and `sysLocation` SNMP variables.
>
> c. Type the IP address or DNS host name of the trap recipient (SNMP management workstation) in the associated **Trap Recipient** field. Use 64 alphanumeric characters or less. It is recommended the IP address be used.
>
> d. The default user datagram protocol (UDP) port number for trap recipients is *162*. Type a decimal port number in the associated **UDP Port Number** field to override the default.

3. Click **Activate** to save the information. The message "`Your changes to the SNMP configuration have been successfully activated`" displays.

Enable or Disable the CLI

Perform this procedure to toggle (enable or disable) the state of the switch's command line interface. To change the CLI state:

1. At the **Configure** window, click the **CLI** tab. The **Management** page displays with the **CLI** tab selected, as shown in Figure 2–11.

Figure 2–11: Management page—CLI tab

2. Perform one of the following steps as required:

   a. Click **Enable** to activate the CLI. The message "Your changes to the CLI enable state have been successfully activated" displays.

   b. Click **Disable** to deactivate the CLI. The message "Your changes to the CLI enable state have been successfully activated" displays.

Enable or Disable Host Control

Perform this procedure to toggle (enable or disable) host control of the switch through the OSMS. The OSMS feature must be installed to access this control. Refer to "Task 12: Configure Open Systems Management Server (Optional)" on page 2–41 for instructions. If the feature is not installed, the message "Feature not installed" displays. To enable or disable host control:

1. At the **Configure** window, click the **OSMS** tab. The **Management** page displays with the **OSMS** tab selected, as shown in Figure 2–12.
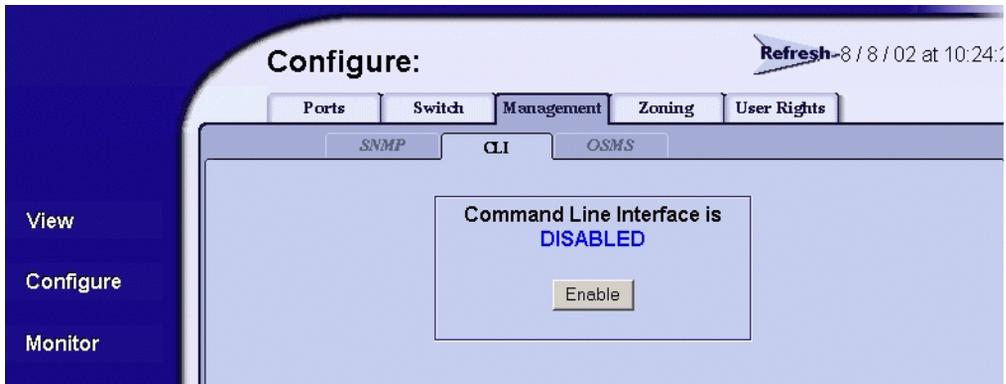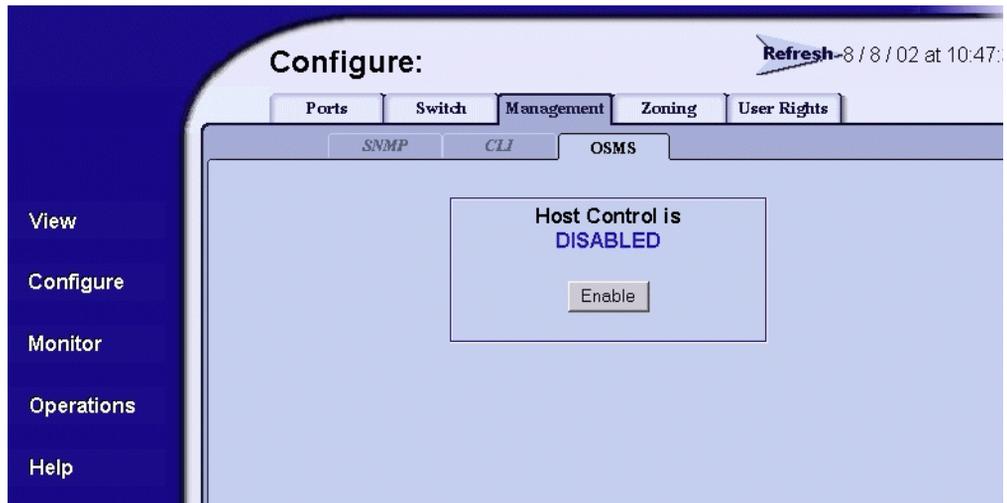

Figure 2–12: Management page—OSMS tab

2. Perform one of the following steps as required:

   a. Click **Enable** to activate the OSMS. The message "Your changes to the host control enable state have been successfully activated" displays.

   b. Click **Disable** to deactivate the OSMS. The message "Your changes to the host control enable state have been successfully activated" displays.

Configure Zones

Perform this procedure to configure, change, add, or delete zones. A zone is a group of devices that can access each other through port- to-port connections. Devices in the same zone can recognize and communicate with each other; devices in different zones cannot. To configure zones:

1. At the **Configure** panel, click the **Zoning** tab. The **Zoning** page displays with the **Zone Set** tab selected. Click the **Zones** tab. The **Zoning** page displays with the **Zones** tab selected, as shown in .
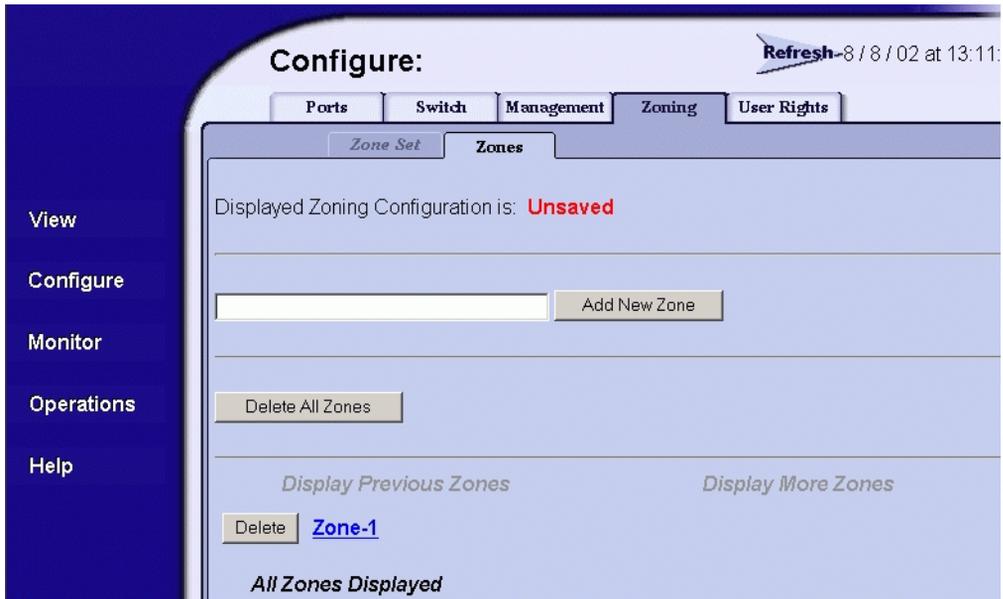
Figure 2–13: Zoning page—Zones tab

2. To configure a zone, first add the zone name to the zoning library. The following naming conventions apply to zones and zone sets:

   — All names must be unique and may not differ by case only. For example, **zone-1** and **Zone-1** are both valid individually, but are not considered unique.

   — The first character of a zone set name must be a letter (**A** through **Z** or **a** through **z**).

   — A zone set name cannot contain spaces.

— Valid characters are alphanumerics and the caret (**^**), hyphen (**-**), underscore (**_**), or dollar (**$**) symbols.

— A zone set name can have a maximum of 64 characters.

3. Type the zone name and click **Add New Zone**. After the name is validated, the new zone name (**Zone-1**) and an associated **Delete** button appear at the bottom of the page. Note the following:

— Save and activate the zone - Changes to a zone or zoning configuration are not saved and activated on the switch until saved as part of a zone set. Go to "Configure Zone Sets" on page 2–25 to perform this function.

— Delete all zones - To delete all configured zones and zone members, click **Delete All Zones**. A confirmation dialog box displays. Click OK to delete all zones.

— Delete a single zone - To delete a single zone and its zone members, click the **Delete** button adjacent to the zone name. A confirmation dialog box displays. Click **OK** to delete the zone.

— Display more zones - If a zone set contains more than 64 zones, the **Display More Zones** link activates to display subsequent pages. In addition, the **Display Previous Zones** link activates on subsequent displayed pages.

4. To add devices (members) to the zone, click the zone name (**Zone-1**). The **Zoning** page displays with the **Modify Zone** tab selected, as shown in Figure 2–14.
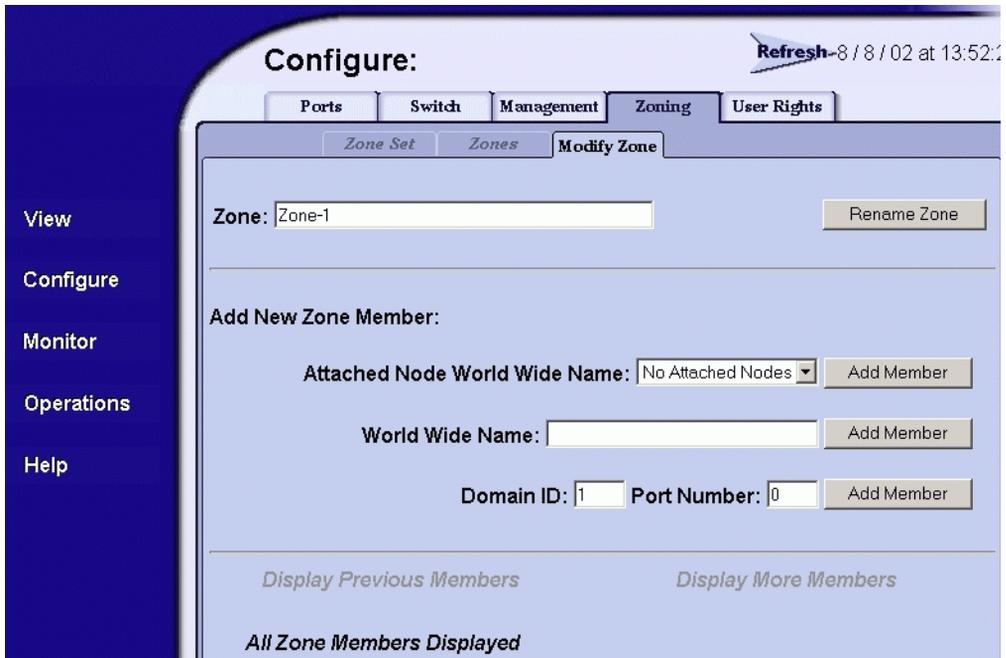
Figure 2–14: Zoning page—Modify Zone tab

5. To rename a configured zone, type the new name in the **Zone** field and click **Rename Zone**. After the name is validated, the zone name is changed.

6. Add or delete zone members as follows:

    — Add member by attached node WWN - Select the WWN of an attached device (node) from the **Attached Node World Wide Name** drop-down list and click the adjacent **Add Member** button. The device is added to the zone.

    — Add member by WWN - Type the WWN of an attached device in the **World Wide Name** field and click the adjacent **Add Member** button. The device is added to the zone.

    — Add member by domain ID and port number - Type the domain ID (1 through 31) of the switch in the **Domain ID** field, type the switch port number (0 through 23) to which a device is attached, and click the adjacent **Add Member** button. The device attached to that port is added to the zone.

— Delete a member - To delete a zone member, click the **Delete** button adjacent to the configured zone member (WWN or domain ID and port number) at the bottom of the page. A confirmation dialog box displays. Click **OK** to delete the zone member.

Changes to a zone, zoning configuration, or zone member are not saved and activated on the switch until saved as part of a zone set. Go to "Configure Zone Sets" on page 2–25 to perform this function.

Configure Zone Sets

Perform this procedure to configure, change, enable, or disable zone sets. A zone set is a group of zones that is activated or deactivated as a single entity across all managed products in either a single switch or a multi-switch fabric. Only one zone set can be active at one time. To configure zone sets:

1. At the **Configure** panel and **Zoning** page, click the **Zone Set** tab. The **Zoning** page displays with the **Zone Set** tab selected, as shown in Figure 2–15.
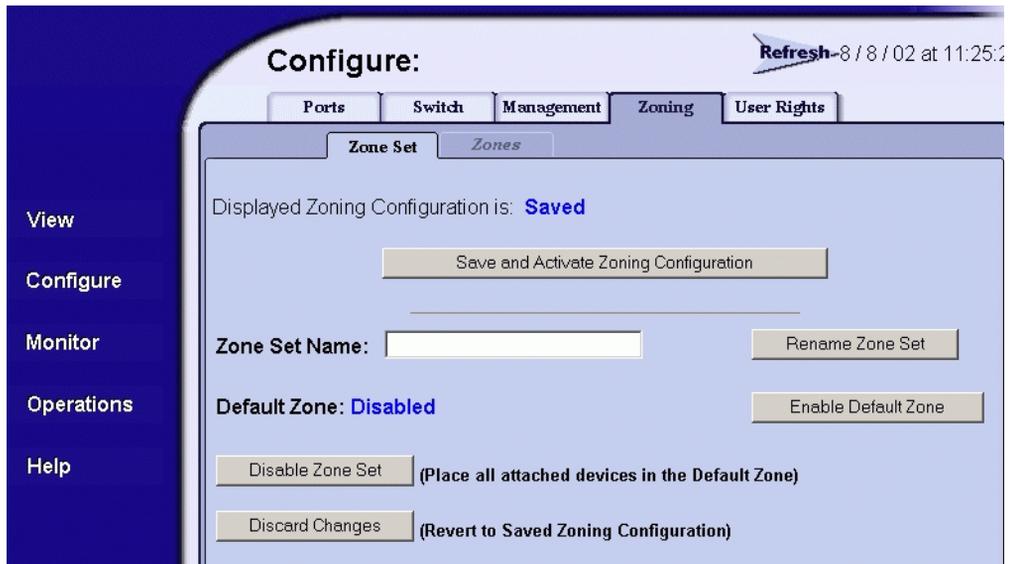

Figure 2–15: Zoning page—Zone Set tab

2. To create a zone set that incorporates zones and zone members (configured under "Configure Zones" on page 2–22), type a new zone set name in the **Zone Set Name** field.

3. Click **Save and Activate Zoning Configuration**. After the zone set name is validated, a confirmation dialog box displays.

4. Click **OK** to save and activate the new zone set. The message "`Your changes to the Zoning configuration have been successfully activated`" displays. Note the following:

    — Rename zone set - To rename a zone set, type the new name in the **Zone Set Name** field. Click **Rename Zone Set**. The new zone set name is validated and changed.

    — Enable or disable default zone - To toggle (enable or disable) the default zone state, click **Enable Default Zone** or **Disable Default Zone**. Depending on the toggle state, the **Default Zone** field changes to **Enabled** or **Disabled**.

    — Disable zone set - To disable the active zone set and place all attached devices in the default zone, click **Disable Zone Set**. A confirmation dialog box displays. Click **OK** to disable the active zone set.

    — Discard changes - To discard unsaved changes made to a zone set configuration and revert to a saved zoning configuration, click **Discard Changes**. A confirmation dialog box displays. Click **OK** to discard the changes.

Configure User Rights

Perform this procedure to configure the administrator-level and operator-level passwords used to access the embedded web server interface through the **Username and Password Required** dialog box.

To configure passwords:

1. At the **Configure** window, click the **User Rights** tab. The **User Rights** page displays.

2. For the **Administrator** set of data fields:

    a. Type the administrator user name (as specified by the customer's network administrator) in the **New User Name** field. Use 16 alphanumeric characters or less.

    b. Type the administrator password (as specified by the customer's network administrator) in the **New Password** field. Use 16 alphanumeric characters or less.

c.   Type the administrator password again in the **Confirm New Password** field, as shown in Figure 2–16.
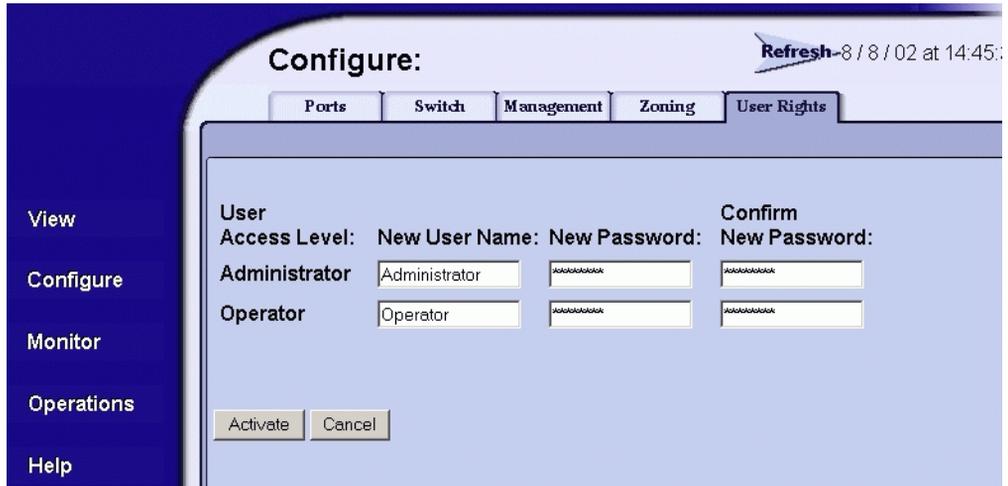
Figure 2–16: User Rights page

3.   For the **Operator** set of data fields:

a.   Type the operator user name (as specified by the customer's network administrator) in the **New User Name** field. Use 16 alphanumeric characters or less.

b.   Type the operator password (as specified by the customer's network administrator) in the **New Password** field. Use 16 alphanumeric characters or less.

c.   Type the operator password again in the **Confirm New Password** field.

4.   Click **Activate** to save the information. The message "`Your changes to the user rights configuration have been successfully activated`" displays.

5.   Close the browser application by choosing **File > Close**.

Install Feature Keys (Optional)

Perform this procedure to install one or more of the following optional features:

- OSMS **-** These feature allows open systems host control of the switch.

- Flexport - A Flexport switch is delivered at a discount with only eight ports enabled. When additional port capacity is required, the remaining ports are enabled (in eight-port increments) through purchase of this feature.

- SANtegrity - This feature enhances security in SANs that contain a large and mixed group of fabrics and attached devices.

After purchasing a feature, obtain the required feature key by following the enclosed instructions. A feature key is an alphanumeric string consisting of both uppercase and lowercase characters. The total number of characters may vary. The feature key is case sensitive and must be entered exactly, including dashes.

The following is an example of a feature key format:

```
XxXx-XXxX-xxXX-xX
```

After obtaining the feature key, install the feature as follows:

1. At the **Configure** window, select the **Operations** option at the left side of the panel. The **Operations** window opens with the **Switch** page displayed.

2. Click the **Feature Installation** tab. The Operations window displays with the Feature Installation tab selected, as shown in Figure 2–17.

Figure 2–17: Features Installation tab

3. Type the feature key and click **Activate**. The interface displays a confirmation page with a warning, stating this action overrides the current set of switch features.

4. Click **Activate** to activate the new feature key. The switch performs an IPL when the feature key is activated.

NOTE: When **Activate** is selected, all current features are replaced with new features.

Task 5: Configure Network Information

The Edge Switch 2/24 is delivered with the following default network addresses:

- MAC address—the media access control (MAC) address is programmed into FLASH memory on the CTP card at the time of manufacture. The MAC address is unique for each switch, and should not be changed. The address is in xx.xx.xx.xx.xx.xx format, where xx is a hexadecimal pair.

  NOTE: References to the CTP in this manual are to the control processor logic contained on the switch motherboard. If an event occurs that indicates the CTP as faulty, replacement of the switch assembly is required.

- IP address—the factory preset default internet protocol (IP) address is 10.1.1.10. The default IP address is also 10.1.1.10.

  If **Reset Configuration** is selected from the product manager application, the switch resets to the default address of 10.1.1.10.

  If multiple switches are installed on the same LAN, each switch (and the HAFM server) must have a unique IP address. One switch can use the factory-set address, but the addresses of the remaining switches must be changed.

NOTE: If you have enabled additional port function with the HP Flexport Feature since the switch shipped from the factory, resetting the configuration will return this feature to the factory default of only 8 ports enabled. You must re-enable the additional ports using the Configure Feature Key dialog box (see "Task 11: Configure Feature Key (Optional)" on page 2–39).

⚠️ **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 parameters.**

- **Subnet mask—**the default subnet mask is **255.0.0.0**. If the switch is installed on a complex public LAN with one or more routers, the address may require change.

- **Gateway address—**the default gateway address is **0.0.0.0**. If the switch is installed on a dedicated LAN with no connection through a router, the address does not require change. If the switch is installed on a public LAN (corporate intranet), the gateway address must be changed to the address of the corporate intranet's local router.

Verify the type of LAN installation with your network administrator. If one switch is installed on a dedicated LAN, network addresses do not require change.

If multiple switches are installed or a public LAN segment is used, network addresses must be changed to conform to the customer's LAN addressing scheme. The following tools are required:

- A maintenance terminal (desktop or notebook PC) with:

  — The Microsoft Windows 98, Windows 2000, Windows XP, or Windows Millennium Edition operating system installed.

  — RS-232 serial communication software (such as ProComm Plus or HyperTerminal) installed. HyperTerminal is provided with Windows operating systems.

  Note that the HAFM server may be used for this function and that HyperTerminal is included in Windows 2000 provided in the HAFM server as a windows 2000 application.

- An asynchronous RS-232 null modem cable (provided with the switch).

Perform the following steps to change a switch's IP address, subnet mask, or gateway address:

1. Remove the protective metal plate from the 9-pin maintenance port at the rear of the switch (a phillips-tip screwdriver is required). Connect the 9-pin end of the RS-232 null modem cable to the port.

2. Connect the other cable end to a 9-pin communication port (**COM1** or **COM2**) at the rear of the maintenance terminal PC.

3. Power on the maintenance terminal. After the PC powers on, the Windows desktop displays. Refer to operating instructions shipped with the PC.

   NOTE: Steps 4-13 describe changing network addresses using the HyperTerminal serial communication software.

4. Choose **Start** > **Programs** > **Accessories** > **Communications** >**HyperTerminal**. The **Connection Description** dialog box displays, as shown in Figure 2–18.
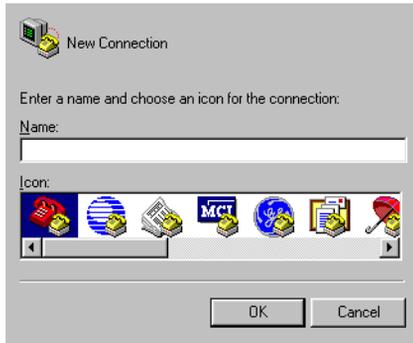
Figure 2–18: Connection Description dialog box

5. Type edge switch 2-24 in the **Name** field and click **OK**. The **Connect To** dialog box displays, as shown in Figure 2–19.

Figure 2–19: Connect To dialog box

6. Ensure the **Connect using** field displays **COM1** or **COM2** (depending on the serial communication port connection to the switch), and click **OK**. The **Port Settings** dialog box displays, as shown in Figure 2–20.
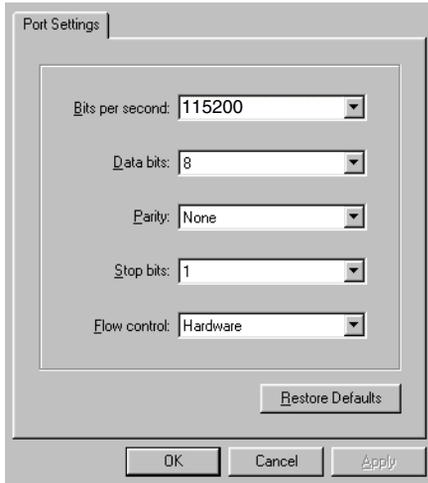
Figure 2–20: Port Settings dialog box

7. Configure the **Port Settings** parameters as follows:

   — **Bits per second**—115200

   — **Data bits**—8

   — **Parity**—None

   — **Stop bits**—1

   — **Flow control**—Hardware

   When the parameters are set, click **OK**. The **HyperTerminal** window displays.

8. At the **>** prompt, type the user-level password (the default is password) and press **Enter**. The password is case sensitive. The **HyperTerminal** window displays with a C**>** prompt at the top of the window, as shown in Figure 2–21.

Figure 2–21: HyperTerminal window

9. At the `C>` prompt, type `ipconfig` and press **Enter**. The **HyperTerminal** window displays with configuration information listed as follows:

   — **MAC Address**

   — **IP Address** (default is `10.1.1.10`**,** factory preset is `10.1.1.10`)

   — **Subnet Mask** (default is `255.0.0.0`).

   — **Gateway Address** (default is `0.0.0.0`)

   — **Auto Negotiate**.

   — **Speed**.

   — **Duplex**.

   Only the **IP Address**, **Subnet Mask**, and **Gateway Address** fields are configurable.

10. Change the IP address, subnet mask, and gateway address as directed by the customer's network administrator. To change switch network addresses, type the following at the `C>` prompt and press **Enter**.

    `ipconfig xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy zzz.zzz.zzz.zzz`

The IP address is always xxx.xxx.xxx.xxx, the subnet mask is always yyy.yyy.yyy.yyy, and the gateway address is always zzz.zzz.zzz.zzz, where the octets *xxx*, *yyy*, and *zzz* are decimals from zero through 255. If a network address is to remain unchanged, type the current address in the respective field.

When the new network addresses are configured at the switch, the message Request completed OK displays at the bottom of the **Edge Switch 2/24 - HyperTerminal** window.

11. Choose **Exit** from the **File** menu to close the HyperTerminal application. A message box displays, as shown in Figure 2–22.
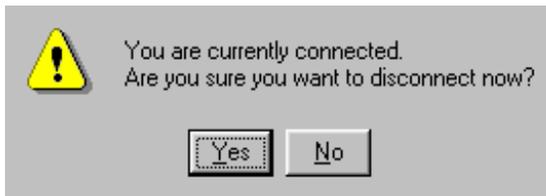
Figure 2–22: Disconnect Now dialog box

12. Click **Yes**. A message box displays, as shown in Figure 2–23.
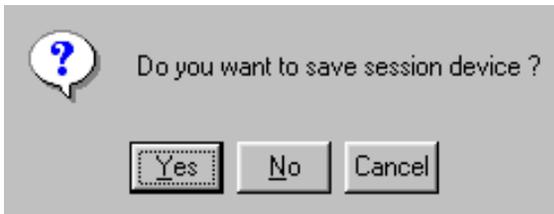
Figure 2–23: Save Session dialog box

13. Click **No** to exit and close the HyperTerminal application.

14. Power off the maintenance terminal:

    a. Choose **Start** > **Shut Down**. The **Shut Down Windows** dialog box displays.

    b. At the **Shut Down Windows** dialog box, choose **Shut down the Computer** and click **Yes** to power off the PC.

15. Disconnect the RS-232 null modem cable from the switch and the maintenance terminal. Replace the protective plate over the maintenance port.

Task 6: LAN-Connect the Switch

Connect the switch to the customer-supplied Ethernet LAN segment or the HP-supplied Ethernet hub.

To connect the desktop or rack-mounted switch to the Ethernet LAN segment:

1. Connect one end of the Ethernet patch cable (supplied with the switch) to the RJ-45 connector (labeled **10/100**) on the left front of the chassis.

2. Connect the remaining end of the Ethernet cable to the LAN as follows:

   a. If the switch is installed on a customer-supplied LAN segment, connect the cable to the LAN as directed by the customer's network administrator.

   b. If the switch is installed on the HP-supplied Ethernet hub, connect the cable to any available port on the hub.

3. Perform one of the following steps:

   - If an HAFM server is delivered and available, the Ethernet LAN segment does not require connection to the internet. Go to "Task 7: HAFM server (Optional)" on page 2–35.

   - If an HAFM server is not available and the switch is managed through the EWS interface, attach the Ethernet LAN segment to an internet connection and go to "Task 4: Configure the Switch from the Embedded Web Server (Optional)" on page 2–6.

Task 7: HAFM server (Optional)

To run HAFM software, you must set up and configure the HP OmniBook 6000/62000 notebook PC to function as an HAFM server.

Refer to the *hp StorageWorks HAFM server installation guide* for instructions on:

- Setting up the HAFM server
- Connecting the HAFM server to the LAN
- Configuring the network addressing for the HAFM server
- Setting HAFM server date and time
- Creating HAFM user names and passwords

Task 8: Configure the Switch to the HAFM Application

To manage a new switch, it must be identified to the HAFM application. To identify the new switch:

1. Right-click in a blank area of the **Product View** and select **New** or click **Product** on the menu bar and choose **New**. The **New Product** dialog box displays, as shown in Figure 2–24.
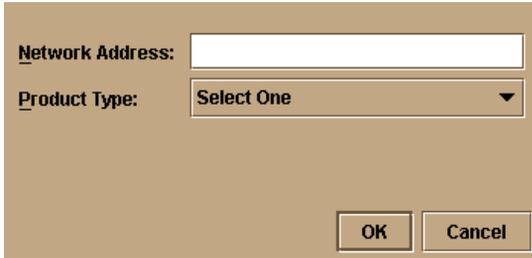
Figure 2–24: New Product dialog box

2. Type the IP address or DNS host name of the switch (determined by the customer's network administrator).

3. Select **edge-24** from the **Product Type** field and click **OK**. A new switch icon displays at the **Product View**.

4. Repeat step 1 through step 3 for each new switch.

Task 9: Record or Verify HAFM Server Restore Information

Configuration information must be recorded to restore the HAFM server in case of hard drive failure. The Windows 2000 operating system and the HAFM with Edge Switch 2/24 product manager application must also be restored. Refer to the *hp StorageWorks edge switch 2/24 service manual* for instructions.

To record or verify HAFM server configuration information refer to the *hp StorageWorks HAFM server installation guide* for instructions.

Task 10: Verify Switch-to-HAFM Server Communication

Communication must be verified between the switch and the HAFM server (High Availability Fabric Manager and product manager applications). To verify switch-to-server communication:

1. At the Windows 2000 desktop, click HAFM at the task bar (bottom of the desktop) to maximize the **Product View**.

2. At the **Product View**, inspect the shape and color of the symbol behind the Edge Switch 2/24 icon. Table 2–2 explains operational states and associated symbols.

Table 2–2: Switch Operational States and Symbols

Operational State	Symbol
Operational—switch-to server communication is established, the switch is operational, and no failures are indicated. Go to "Task 13: Set Switch Date and Time" on page 2–41.	
Degraded—switch-to server communication is established, but the switch is operating in degraded mode and requires service. This condition is typical if a port or redundant FRU fails. Go to step 3.	
Failed—switch-to server communication is established, but the switch failed and requires immediate service. Go to step 3.	
Status Unknown—the switch status is unknown because of a network communication failure between the switch and HAFM server. Go to step 3.	

3. Double-click the switch icon. The **Hardware View** for the selected switch displays, as shown in Figure 2–25. In the example, FRU failures are indicated by *Flashing* red and yellow diamonds, and switch degradation is indicated by the yellow triangle at the alert panel.
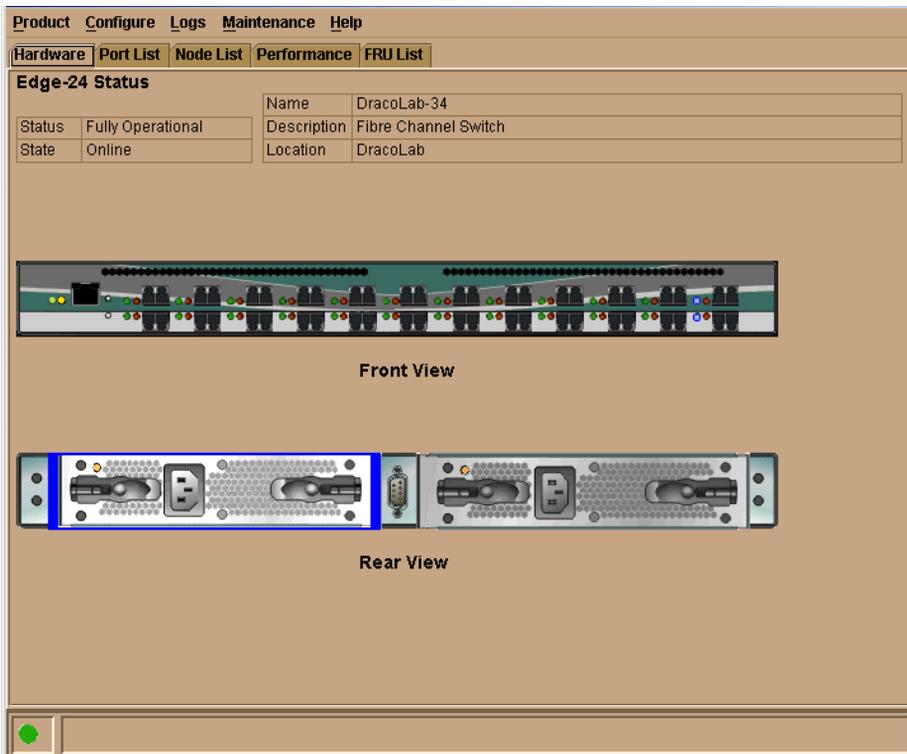
Figure 2–25: Switch Hardware View

4. Inspect switch status at the **Hardware View** and perform one of the following steps:

   a. If the switch displays operational (no FRU alert symbols and a green circle at the alert panel), go to "Task 13: Set Switch Date and Time" on page 2–41.

   b. If switch operation displays degraded or a switch failure is indicated (FRU alert symbols and a yellow triangle or red diamond at the alert panel), refer to the *hp StorageWorks edge switch 2/24 service manual* to isolate the problem.

Task 11: Configure Feature Key (Optional)

Perform this task to display or install operating features that are available as customer-specified options. Available features include:

- OSMS - Open systems management server. This feature allows open systems host control of the switch.

- SANtegrity - This feature enhances security in SANs that contain a large and mixed group of fabrics and attached devices.

- Flexport - A Flexport switch is delivered at a discount with a subset of available ports enabled. When additional port capacity is required, the remaining ports are enabled (in eight-port increments) through purchase of this feature.

NOTE: This Flexport key enables additional port function. The factory default settings enable 8 of the 24 ports, and this feature key enables additional ports. Until this feature is enabled the additional ports will display as Not Installed in the Port Operational State window of the Hardware View and Port List Views. See *hp StorageWorks edge switch 2/24 flexport upgrade instruction* for information on configuring this feature key and on upgrading the number of ports.

Features are enabled through a feature key that is encoded to work with the serial number of a unique switch. A feature key is a case-sensitive alphanumeric string with dashes every four characters.

To configure a feature key:

1. Ensure the switch is set offline.

2. At the Hardware View for the selected switch, choose **Configure** > **Features**.

   The **Configure Feature Key** dialog box displays, as shown in Figure 2–26.
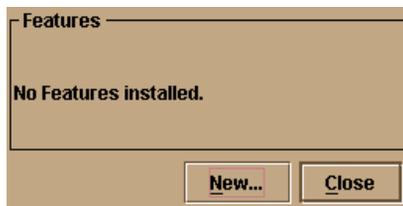
Figure 2–26: Configure Feature Key dialog box

3. Click **New**. The **New Feature Key** dialog box displays, as shown in Figure 2–27.

Figure 2–27: New Feature Key dialog box

4. Type the feature key (case-sensitive xxxx-xxxx-xxxx-xx format) and click **OK**. The **Enable Feature Key** dialog box displays, as shown in Figure 2–28.
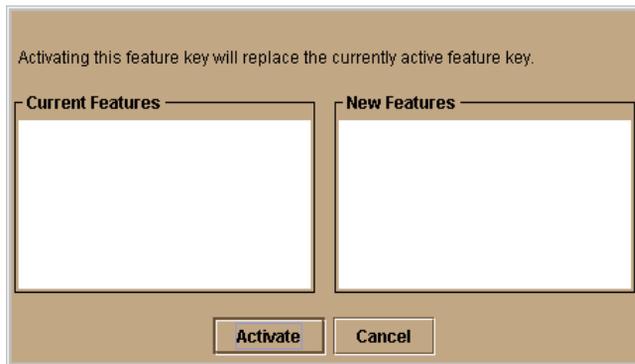
Figure 2–28: Enable Feature Key dialog box

5. Click **Activate** to enable the feature key. When the feature key is enabled, the switch performs an IPL, but *is not* automatically set to open systems operating mode.

Task 12: Configure Open Systems Management Server (Optional)

Perform this task to configure the open systems management server (OSMS) and enable OSI host control of the switch. Implementing host control requires installation of a SAN management application on the OSI server. Management applications include Veritas SANPoint Control (Version 1.0 or later), or Tivoli NetView (Version 6.0 or later).

To configure the open systems management server:

1. At the **Hardware View** for the selected switch, choose **Configure > Management Server**. The **Configure Open Systems Management Server** dialog box displays, as shown in Figure 2–29.

Figure 2–29: Configure Open Systems Management server dialog box

2. Allow or prohibit host (OSI server) control by selecting **Host Control Prohibited**. If a check mark displays, host control is prohibited, preventing a host management program from changing configuration and connectivity parameters on the switch. The host program has read-only access to configuration and connectivity parameters. An unchecked box allows a host management program to change configuration and connectivity parameters.

3. Click **Activate** to enable a change and allow or prohibit open systems host control.

Task 13: Set Switch Date and Time

The Edge Switch 2/24 product manager log entries are stamped with the date and time received from the switch. To set the effective date and time for the switch:

1. At the **Hardware View** for the selected switch, choose **Configure > Date/Time**. The **Configure Date and Time** dialog box displays, as shown in Figure 2–30.

The switch date and time can be set manually, or set to be periodically updated by the HAFM application (the switch and HAFM application synchronize at least once daily).
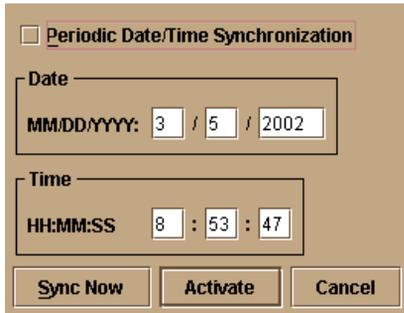
Figure 2–30: Configure Date and Time dialog box

Set Date and Time Manually

To set the switch date and time manually:

1. At the **Configure Date and Time** dialog box, click **Periodic Date/Time Synchronization** to deselect the option (no check mark in the box). The greyed out **Date and Time** fields activate.

2. Click the **Date** fields that require change, and type numbers in the following ranges:

   Month (MM): 1 through 12
   Day (DD): 1 through 31
   Year (YY): greater than 1980

3. Click the **Time** fields that require change, and type numbers in the following ranges:

   Hour (HH): 0 through 23
   Minute (MM): 0 through 59
   Second (SS): 0 through 59

4. Click **Activate** to set the switch date and time and close the **Configure Date and Time** dialog box.

Periodically Synchronize Date and Time

To set the switch to periodically synchronize date and time with the HAFM application:

1. Click **Periodic Date/Time Synchronization** to select the option (check mark in the box). The **Date and Time** fields are greyed out and not selectable. Perform one of the following options:

   - Click **Activate** to enable synchronization and close the **Configure Date and Time** dialog box. The switch date and time synchronize with the HAFM application date and time at the next update period (at least once daily).

   - Click **Sync Now** to synchronize the switch and HAFM application immediately. The **Date and Time Synced** dialog box displays, as shown in .
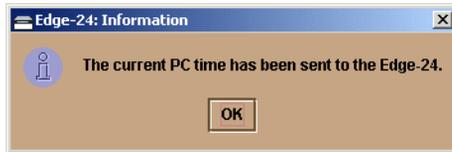
Figure 2–31: Date and Time Synced dialog box

2. Click **OK** to synchronize the date and time and close the **Date and Time Synced** dialog box, then click **Activate** to enable synchronization and close the **Configure Date and Time** dialog box.

Task 14: Configure the Edge Switch 2/24 Product Manager Application

Selectively perform the following configuration tasks for the Edge Switch 2/24 product manager application according to the customer's installation requirements. For additional information, refer to the *hp StorageWorks edge switch 2/24 product manager user guide*.

- Identify the switch to the HAFM application.

- Configure switch parameters.

- Configure fabric parameters.

- Configure switch binding.

- Configure switch ports.

- Configure SNMP trap message recipients.

- Configure threshold alerts.

- Enable Embedded Web Server and Telnet access.

- Configure and enable e-mail notification.

- Enable call-home notification.

Configure Switch Identification

Perform this procedure to configure the switch name, description, location, and contact person for the HAFM application. The information displays in multiple dialog boxes throughout the application. In addition, the Name, Location, and Contact variables configured at the **Configure Identification** dialog box correspond respectively to the SNMP variables sysName, sysLocation, and sysContact. These variables are used by SNMP management workstations when obtaining data from managed switches.
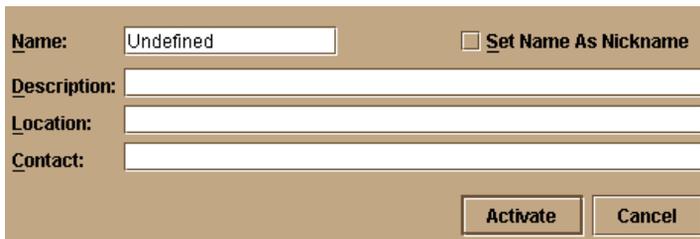
To configure the switch identification:

1. At the **Hardware View** for the selected switch, choose **Configure > Identification**. The **Configure Identification** dialog box displays, as shown in Figure 2–32.

Figure 2–32: Configure Identification dialog box

   a. Type a switch name of 24 alphanumeric characters or less in the **Name** field. Each switch should be configured with a unique name.

   If the switch is installed on a public LAN, the name should reflect the switch's Ethernet network DNS host name. For example, if the DNS host name is hpes224.hp.com, enter hpes224.

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

c. Type a switch description of 255 alphanumeric characters or less in the **Description** field.

d. Type the switch's physical location (255 alphanumeric characters or less) in the **Location** field.

e. Type the name of a contact person (255 alphanumeric characters or less) in the **Contact** field.

2. Click **Activate** to configure the switch identification and close the dialog box.

Configure Switch Parameters

Perform this procedure to configure the switch's preferred domain ID, insistent domain ID, rerouting delay, and domain RSCNs. The switch must be set offline to configure the preferred domain ID. To configure switch parameters:

1. Ensure the switch is set offline.

2. At the **Hardware View**, select **Configure > Operating Parameters > Switch Parameters**. The **Configure Switch Parameters** dialog box displays, as shown in Figure 2–33.

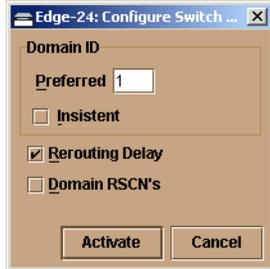**Figure 2–33: Configure Switch Parameters dialog box**

a. At the **Preferred Domain ID** field, type a value between 1 through 31. The domain ID uniquely identifies each switch in a fabric.

If the switch is attached to a fabric element, the switch and element must have unique domain IDs. If the values are not unique, the E_Port connection to the element segments and the switch cannot communicate with the fabric.

b.   Click the **Insistent Domain ID** check box to enable or disable this parameter. A check mark in the box indicates the parameter is enabled. When the parameter is enabled, the domain ID configured in the **Preferred Domain ID** field becomes the active domain identification when the fabric initializes. This parameter is enabled only if the optional SANtegrity feature is installed.

c.   Click the **Rerouting Delay** check box to enable or disable this parameter. A check mark in the box indicates the parameter is enabled. When the parameter is enabled, traffic is delayed through the fabric by the specified E_D_TOV. This delay ensures Fibre Channel frames are delivered to their destination in order, even if a change to the fabric topology creates a new (shorter) transmission path.

d.   Click the **Domain RSCNs** check box to enable or disable this parameter. A check mark in the box indicates the parameter is enabled. When the parameter is enabled, attached devices can register to receive notification when another attached device changes state.

3.   Click *Activate* to save the information and close the dialog box.

4.   Set the switch online.

Configure Fabric Parameters

Perform this procedure to configure the fabric operating parameters, including R_A_TOV, E_D_TOV, switch priority, and interop mode. The switch must be set offline. To configure fabric parameters:

1.   Ensure the switch is set offline.

2.   At the **Hardware View**, select **Configure** > **Operating Parameters** > **Fabric Parameters**. The **Configure Fabric Parameters** dialog box displays, as shown in Figure 2–34.
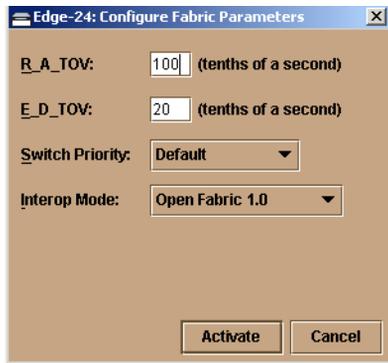
Figure 2–34: Configure Fabric Parameters dialog box

    a.   At the **R_A_TOV** field, type a value between 10 through 1200 tenths of a second (one through 120 seconds).

        If the switch is attached to a fabric element, the switch and element must be set to the same R_A_TOV value. If the values are not identical, the E_Port connection to the element segments and the switch cannot communicate with the fabric. In addition, the R_A_TOV value must be greater than the E_D_TOV value.

    b.   At the **E_D_TOV** field, type a value between 2 through 600 tenths of a second (0.2 through 60 seconds).

        If the switch is attached to a fabric element, the switch and element must be set to the same E_D_TOV value. If the values are not identical, the E_Port connection to the element segments and the switch cannot communicate with the fabric. In addition, the E_D_TOV value must be less than the R_A_TOV value.

    c.   Select from the **Switch Priority** drop-down list to set the switch priority. Available selections are **Default**, **Principal**, and **Never Principal**. The default setting is **Default**.

        This value designates the fabric's principal switch. The principal switch is assigned a priority of 1 and controls the allocation and distribution of domain IDs for all fabric elements (including itself).

        Principal is the highest priority setting, **Default** is the next highest, and

Never Principal is the lowest priority setting. The setting **Never Principal** means the switch is incapable of becoming a principal switch. If all switches are set to **Principal** or **Default**, the switch with the highest priority and the lowest WWN becomes the principal switch.

At least one switch in a fabric must be set as **Principal** or **Default**. If all switches are set to **Never Principal**, all ISLs segment.

d. Select from the **Interop Mode** drop-down list to set the switch operating mode. This setting only affects the mode used to manage the switch; it does not affect port operation. Available selections are:

— **Homogeneous Fabric -** Select this option (default) if the switch is fabric-attached only to other HP directors or switches operating in Homogeneous fabric mode.

— **Open Fabric 1.0 -** Select this option for managing heterogeneous fabrics and if the switch is fabric-attached to HP directors or switches and open-fabric compliant switches produced by other OEMs.

3. Click **Activate** to save the information and close the dialog box.

4. Set the switch online.

Configure Switch Binding

The switch binding (SANtegrity) feature specifies devices that can connect to Edge Switch 2/24 ports. This provides security in SAN environments by ensuring that only an intended set of devices can communicate with the switch.

Overview

To configure switch binding, enable the feature and select the type of port for which connection is to be restricted (connection policy). Port selections include E_Ports, F_Ports, or all port types. For instructions, refer to "Enable or Disable Switch Binding" on page 2–50.

If the switch is online, binding populates a membership list at the **Switch Binding - Membership List** dialog box displays (as shown in Figure 2–36) with WWNs of devices connected to the switch. The list is modified by the connection policy set in the **Switch Binding - Change State** dialog box displays, as shown in Figure 2–35.

When the switch binding feature is first installed but not enabled, the associated membership list is empty. The list is populated with device WWNs as follows:

- When switch binding is enabled with the switch online, the membership list is automatically populated with the WWNs of all devices and fabric elements connected to the switch.

- When switch binding is enabled with the switch offline, the membership list is not automatically populated.

- After enabling switch binding, prohibit devices from connecting with switch ports by removing the devices from the membership list. Allow devices to connect to switch ports by adding the devices to the membership list.

Online State and Switch Binding

Specific operating parameters and optional features must be enabled for switch binding to function. In addition, there are requirements for disabling these parameters and features when the switch is online or offline. Be aware that:

- Switch binding can be enabled or disabled when the switch is offline or online.

- If Enterprise Fabric Mode is enabled from the HAFM **Fabrics** tab:

    — Switch binding is automatically enabled.

    — Switch binding cannot be disabled if the switch is online.

    — Switch binding can be disabled if the switch is offline. However, if switch binding is disabled, Enterprise Fabric Mode is also disabled.

- WWNs can be added to the membership list when switch binding is either enabled or disabled.

- WWNs can be removed from the membership list *only* if one or more of the following are true:

    — The switch is offline.

    — Switch binding is disabled.

    — The associated device is not connected to the switch.

    — The associated device is connected to a blocked port.

    — Switch binding is not enabled for the same port type as enabled at the **Switch Binding - Change State** dialog box (Connection Policy). For example, a WWN for a fabric switch connected to an E_Port can be removed if switch binding is enabled to restrict only F_Ports.

- If the switch is online and switch binding is not enabled, all WWNs of devices attached to the switch are automatically added to the membership list.

Zoning and Switch Binding

SANtegrity switch binding parameters have no effect on zoning configurations. However, if a device WWN is in a specific zone, but the WWN is not in the membership list, the device cannot log in to a switch port and cannot connect to other devices in the zone with switch binding enabled.

Enable or Disable Switch Binding

Perform this procedure to configure (enable or disable) switch binding:

1. Ensure the SANtegrity feature key is installed and configured. For instructions, refer to "Task 11: Configure Feature Key (Optional)" on page 2–39.

2. At the *Hardware View*, select **Configure** > **Switch Binding** > **Change State**. The **Switch Binding - Change State** dialog box displays, as shown in Figure 2–35.

Figure 2–35: Switch Binding - Change State dialog box

3. Perform one of the following:

    •   To enable switch binding, click the **Enable Switch Binding** check box to add a check mark. Go to step 4 to set the connection policy.

    •   To disable switch binding, click the **Enable Switch Binding** check box to remove the check mark, then click **Activate** to enable the change and close the dialog box.

4. Select a **Connection Policy** radio button as follows:

    •   **Restrict E_Ports -** Select this button to restrict connections from specific fabric elements to switch E_Ports. WWNs can be added to the membership list to allow element connection and removed from the list to prohibit element connection. Devices are allowed to connect to any F_Port or FL_Port without restriction.

- **Restrict F_Ports -** Select this button to restrict connections from specific devices to switch F_Ports or FL_Ports. WWNs can be added to the membership list to allow device connection and removed from the list to prohibit device connection. Fabric switches are allowed to connect to any E_Port without restriction.

- **Restrict All -** Select this button to restrict connections from specific devices to switch F_Ports or FL_Ports and fabric elements to switch E_Ports. WWNs can be added to the membership list to allow connection and removed from the list to prohibit connection.

5. Click **Activate** to enable the changes and close the **Switch Binding - Change State** dialog box.

Edit Membership List

Perform this procedure to edit the switch binding membership list:

Ensure the SANtegrity feature key is installed and configured. For instructions, refer to "Task 11: Configure Feature Key (Optional)." on page 2–39.

1. At the **Hardware View**, select **Configure** > **Switch Binding** > **Edit Membership List**. The **Switch Binding - Membership List** dialog box displays. WWNs of devices that are allowed to connect to switch ports appear in the **Switch Membership List** window.
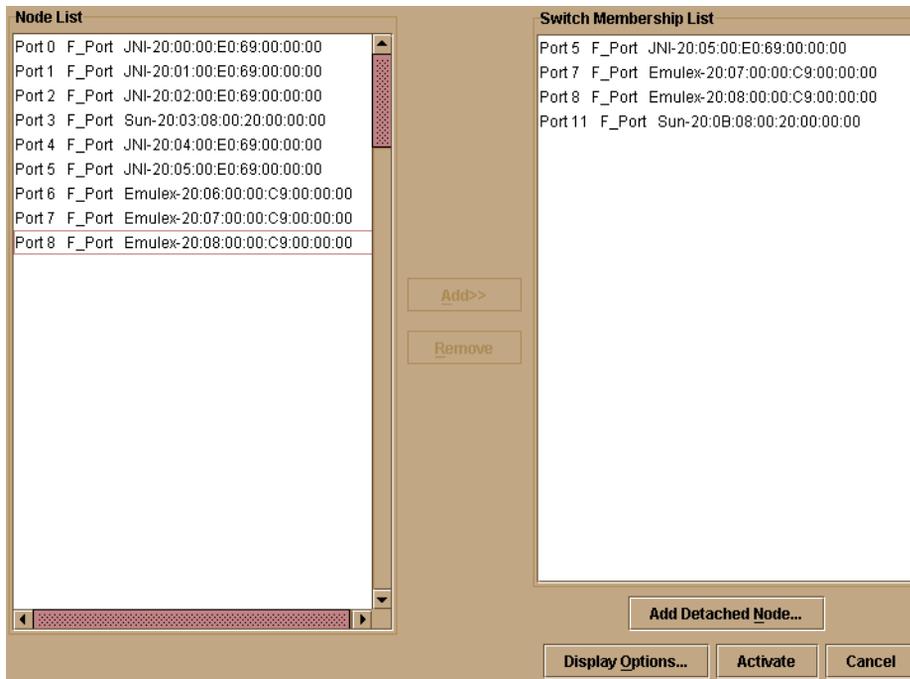
Figure 2–36: Switch Binding - Membership List dialog box

2. If nicknames are configured (through the HAFM application) and are to be displayed instead of WWNs, click **Display Options**. The **Display Options** dialog box displays . If nicknames are not configured, go to step 4.

3. Click the **Nickname** radio button, then click **OK**. The dialog box closes and nicknames appear in the **Switch Binding - Membership List** dialog box.

4. Perform one of the following:

   • To allow a switch port connection to a device listed in the **Node List** panel, select the WWN or nickname and click **Add>>**. The device WWN or nickname moves to the **Switch Membership List** panel.

   • To prohibit a switch port connection to a device listed in the **Switch Membership List** panel, select the WWN or nickname and click **<<Remove**. The device WWN or nickname moves to the **Node List** panel.

NOTE: Device connectivity and membership list edits are subject to the rules defined under "Online State and Switch Binding" on page 2–49.

5. To add a WWN or nickname for a device not connected to the switch, click **Detached Node**. The **Add Detached Node** dialog box displays.

6. Type the device WWN or nickname and click **OK**. The WWN or nickname appears in the **Switch Membership List**.

7. Click **Activate** to enable the changes and close the **Switch Binding - Membership List** dialog box.

Configure Switch Ports

To configure switch Fibre Channel ports:

1. At the **Hardware View** for the selected switch, choose **Configure > Ports**. The **Configure Ports** dialog box (open systems mode) displays.

Port #	Name	Blocked	LIN Alerts	FAN	Type	Speed	Port Binding	Bound WWN
0		☐	☑	☐	G_PORT	1 Gb/sec	☑	20:00:00:00:C9:00:00:00
1		☐	☑	☐	G_PORT	1 Gb/sec	☐	20:01:00:E0:69:00:00:00
2		☐	☑	☐	G_PORT	1 Gb/sec	☐	20:02:00:00:C9:00:00:00
3		☐	☑	☐	G_PORT	1 Gb/sec	☑	20:03:00:00:C9:00:00:00
4		☐	☑	☐	G_PORT	1 Gb/sec	☐	20:04:00:E0:69:00:00:00
5		☐	☑	☐	G_PORT	1 Gb/sec	☐	20:05:08:00:20:00:00:00
6		☐	☑	☐	G_PORT	1 Gb/sec	☑	20:06:00:60:48:00:00:00
7		☐	☑	☐	G_PORT	1 Gb/sec	☐	20:07:08:00:20:00:00:00
8		☐	☑	☐	G_PORT	1 Gb/sec	☐	20:08:08:00:20:00:00:00
9		☐	☑	☐	G_PORT	1 Gb/sec	☑	20:09:00:00:C9:00:00:00
10		☐	☑	☐	G_PORT	1 Gb/sec	☐	20:0A:08:00:20:00:00:00
11		☐	☑	☐	G_PORT	1 Gb/sec	☐	20:0B:00:E0:69:00:00:00
12		☐	☑	☐	G_PORT	1 Gb/sec	☑	20:0C:08:00:20:00:00:00
13		☐	☑	☐	G_PORT	1 Gb/sec	☐	20:0D:00:60:48:00:00:00
14		☐	☑	☐	G_PORT	1 Gb/sec	☐	20:0E:00:60:48:00:00:00
15		☐	☑	☐	G_PORT	1 Gb/sec	☑	20:0F:00:60:48:00:00:00
16		☐	☑	☐	G_PORT	1 Gb/sec	☐	20:10:00:60:48:00:00:00
17		☐	☑	☐	G_PORT	1 Gb/sec	☐	20:11:08:00:20:00:00:00
18		☐	☑	☐	G_PORT	1 Gb/sec	☑	20:12:08:00:20:00:00:00
19		☐	☑	☐	G_PORT	1 Gb/sec	☐	20:13:00:00:C9:00:00:00
20		☐	☑	☐	G_PORT	1 Gb/sec	☐	20:14:08:00:20:00:00:00
21		☐	☑	☐	G_PORT	1 Gb/sec	☑	20:15:00:60:48:00:00:00
22		☐	☑	☐	G_PORT	1 Gb/sec	☐	20:16:00:00:C9:00:00:00
23		☐	☑	☐	G_PORT	1 Gb/sec	☐	20:17:00:60:48:00:00:00

Activate   Cancel

Figure 2–37: Configure Ports dialog box

a. Select a blank **Name** field and type a descriptive port name of 24 or fewer alphanumeric characters. Use a name that reflects the device connected to the port.

b. Click **Blocked** check box to block or unblock a port. A check mark in the box indicates the port is blocked. Blocking the port prevents the attached device from communicating with the switch. A blocked port continuously transmits the offline sequence (OLS), as shown in Figure 2–37.

c. Click **LIN Alerts** to enable or disable LIN alerts for a port. A check mark in the box indicates alerts are enabled. When the feature is enabled and an incident occurs on the link, an alert indicator (yellow triangle) displays at the **Hardware View**, **Port List View**, and **Port Card View**s, and a message is sent to configured e-mail recipients. LIN alerts are enabled by default.

d. Click the check box in the **FAN** column to enable or disable the fabric address notification (FAN) feature (default is enabled). A check mark in the box indicates FAN is enabled. When the feature is enabled, the port transmits a FAN frame after loop initialization to verify that FC-AL devices are still logged in. It is recommended this option be enabled for ports configured for loop operation.

e. Select from the drop-down list in the **Type** column to configure the port type. Available selections are:

— Generic port (**G_Port**).

— Fabric port (**F_Port**).

— Expansion port (**E_Port**).

— Fabric mixed port (**FX_Port**). Use this selection to configure a port as an F_Port or FL_Port.

— Generic mixed port (**GX_Port**). Use this selection to configure a port as a G_Port or GL_Port. This is the default selection.

f. Click the **Speed** field for a port. A **Speed** drop-down list displays. Choose **1 Gb/sec**, **2 Gb/sec**, or **Negotiate** as the desired setting depending on the speed capability of the device to be plugged into the port.

A right-click in the **Speed** column allows you to choose from a menu to set all ports to **1 Gb/sec**, **2 Gb/sec**, or **Negotiate**.

g. Click the check box in the **Port Binding** column to enable or disable port binding (default is disabled). A check mark in the box indicates port binding is enabled and the port can connect only to a device with a WWN listed in the **Bound WWN** column.

h. If port binding is enabled, type the WWN or nickname of the device attached to the port in the **Bound WWN** column.

— If the check box in the **Port Binding** column is checked and a WWN or nickname appears in the **Bound WWN** field, only the specified device can attach to the port.

— If the check box in the **Port Binding** column is checked but no WWN or nickname appears in the **Bound WWN** field, no device can connect to the port.

— If the check box in the **Port Binding** column is not checked, any device can connect to the port.Use the vertical scroll bar as necessary to display additional port information rows (up to 24 ports).

2. Click **Activate** to save the configuration information and close the dialog box.

Configure SNMP Trap Message Recipients

Perform this procedure to configure community names, write authorizations, and network addresses and for up to 6 SNMP trap message recipients. A trap recipient is a management workstation that receives notification (through SNMP) if a switch event occurs.

To configure SNMP trap recipients:

1. At the **Hardware View** for the selected switch, choose **Configure > SNMP Agent**. The **Configure SNMP Agent** dialog box displays, as shown in Figure 2–38.

Figure 2–38: Configure SNMP Agent dialog box

    a. For each trap recipient to be configured, type a community name of 32 alphanumeric characters or less in the associated **Community Name** field. The community name is incorporated in SNMP trap messages to ensure against unauthorized viewing or use.

    b. Click the check box in the **Write Authorization** column to enable or disable write authorization for the trap recipient (default is disabled). A check mark in the box indicates write authorization is enabled. When the feature is enabled, a management workstation user can change the HAFM server's `sysContact`, `sysName`, and `sysLocation` SNMP variables.

    c. Type the IP address or DNS host name of the trap recipient (SNMP management workstation) in the associated **Trap Recipient** field. Use 32 alphanumeric characters or less. It is recommended the IP address be used.

    d. The default user datagram protocol (UDP) port number for trap recipients is `162`. Type a decimal port number in the associated **UDP Port Number** field to override the default.

2. To enable transmission of trap messages to configured SNMP management workstations, click **Enable Authorization Traps**. A check mark displays in the box when transmission is enabled.

3. Click **Activate** to save the information and close the dialog box.

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 or F_Ports).

You are notified of a threshold alert in four ways:

- 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 is recorded in the **Threshold Alert** log.

Choose **Configure** > **Threshold Alerts** 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 is 50% of capacity.

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

  — The time that the percentage of throughput capacity (% utilization) must exist during the set time interval before an alert generates.

- 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.

Create New Alert

1. At the **Hardware View** for the selected switch, choose **Configure > Threshold Alerts**. The **Configure Threshold Alerts** dialog box displays, as shown in Figure 2–39.

   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).
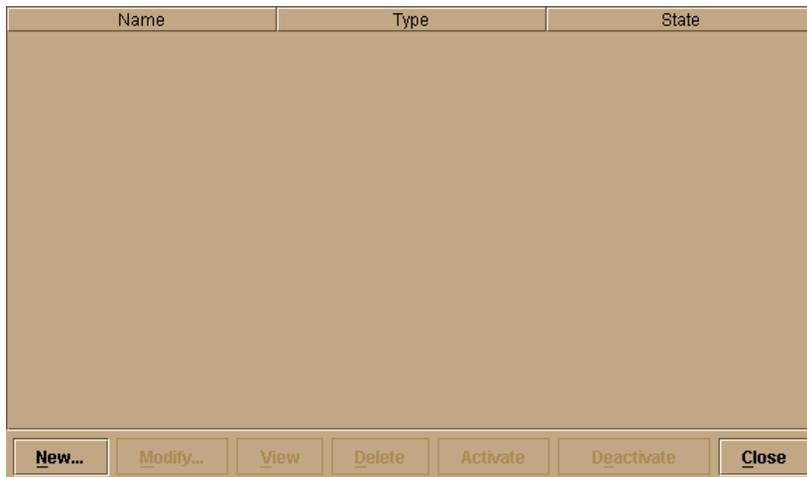

Figure 2–39: Configure Threshold Alerts dialog box

2. Click **New.** The **New Threshold Alert** dialog box displays, as shown in Figure 2–40.

Figure 2–40: 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 options 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 displays with additional parameters. The name configured for the alert displays at the top of the screen. Click **Previous** to return to the previous screen, as shown in Figure 2–41.

Figure 2–41: 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 displays for selecting ports for the alerts, as shown in Figure 2–42.
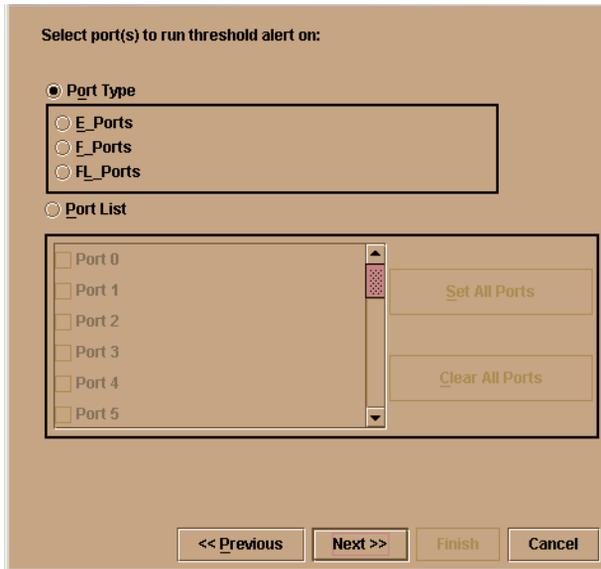
Figure 2–42: New Threshold Alerts dialog box—third screen

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 displays to provide a summary of your alert configuration. To make any changes, backwards and forwards through the configuration screens by selecting **Previous** and **Next**, as shown in Figure 2–43.
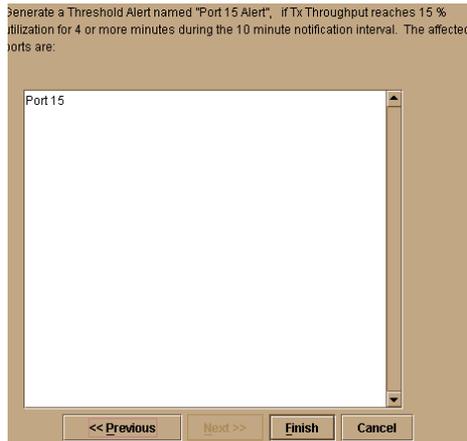
Figure 2–43: New Threshold Alerts dialog box—summary screen

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

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**, as shown in Figure 2–44.
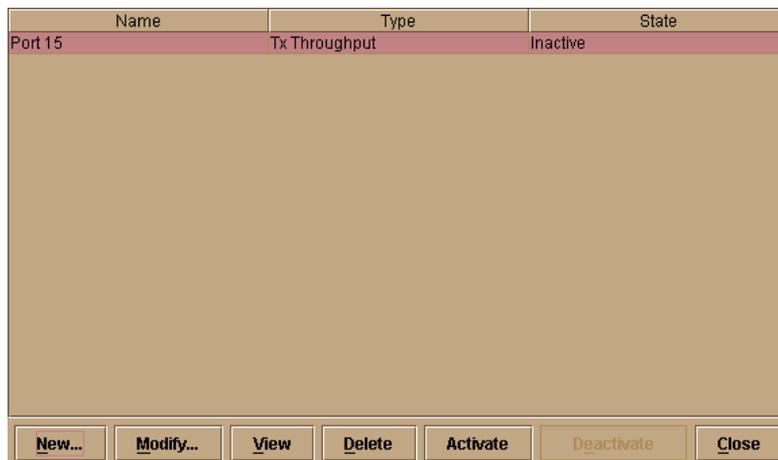
Figure 2–44: Configure Threshold Alerts dialog box—alerts activated

Modify an Alert

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

1. Choose **Configure > Threshold Alerts**. 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, click **Deactivate**, then select the alert information in the table again.

4. Click **Modify**.

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

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

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

6. Click **Next** when you are done. A Modify Threshold screen displays 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. Make appropriate changes, then continue through the Modify Threshold screens, making changes as necessary, until the summary screen displays showing 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. Choose **Configure > Threshold Alerts**. 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 information in the table.

    •   If the alert is active, click **Deactivate** to change to the deactive state.

    •   If the alert is deactive, click **Activate** to change to the active state.

Delete Alerts

Use the following steps to delete existing threshold alerts.

1. Choose **Configure > Threshold Alerts**. 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. Click **Delete**. A message displays asking you to confirm the deletion.

4. Click **Yes**. The alert is removed from the dialog box.

Enable the EWS Interface and Telnet Access

Perform this procedure to enable Embedded Web Server (EWS) and Telnet access through the maintenance port at the rear of the switch. To enable these functions:

1. To enable the EWS interface at the **Hardware View**, select **Enable Web Server** from the **Configure** menu. A check mark appears in the box when the interface is enabled, and the menu closes.

2. To enable Telnet access at the **Hardware View**, select **Enable Telnet** from the **Configure** menu. A check mark appears in the box when access is enabled, and the menu closes.

Configure and Enable E-mail Notification

Perform this procedure to configure and enable e-mail addresses and simple mail transfer protocol (SMTP) server addresses to receive e-mail notification of switch (and other managed product) events. The addresses must be configured at the HAFM application, then enabled. See "Task 15: Test Remote Notification (Optional)" on page 2–65 for instructions on testing this notification feature.

To configure and enable e-mail and SMTP server addresses:

1. At the **Product View**, choose **Maintenance > Configure E-Mail**. The **Configure E-Mail** dialog box displays, as shown in Figure 2–45.
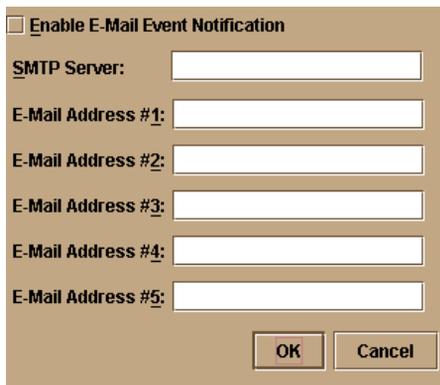
Figure 2–45: Configure E-Mail dialog box

   a. Type the IP address or DNS host name of the SMTP server in the **SMTP server** field. Use 64 alphanumeric characters or less. It is recommended the IP address be used.

   b. For the **E-Mail Addresses** fields, type the e-mail addresses of up to five recipients who should be informed of system events. Use 64 alphanumeric characters or less for each entry.

2. To enable e-mail transmission to configured addresses, click **Enable E-Mail Event Notification**. A check mark displays in the box when transmission is enabled.

   NOTE: The enable function must also be activated for each switch through the Edge Switch 2/24 product manager application. E-mail notification can be active for some switches and inactive for others.

3. Double-click the switch icon. The **Hardware View** for the selected switch displays.

4. At the **Hardware View** for the selected switch, choose **Maintenance > Enable E-Mail Notification**. A check mark displays in the check box to indicate e-mail notification for the switch is enabled, and the menu closes.

Configure and Enable Call-Home Features

There are two call-home features available, and only one is installed when the HAFM application is installed on the HAFM server. To learn more about configuring Call-Home features, refer to the *hp StorageWorks HAFM server installation guide*.

Task 15: Test Remote Notification (Optional)

If the call-home and e-mail notification features are enabled, set up the HAFM application to test these remote notification features. Because the features are configured at the HAFM application, call-home and e-mail notification are enabled for multiple switches or HP managed products. To test remote notification:

1. Close the **Hardware View** for the switch and return to the **Product View** by closing the window.

2. At the **Product View**, choose **Maintenance > Test Remote Notification**. The **Test Remote Notification** dialog box displays, as shown in Figure 2–46.

Figure 2–46: Test Remote Notification dialog box

3. Choose **Call Home** and **E-Mail** to perform applicable tests.

   The call home test provides a test notification message to a remote support center. Depending on the option chosen during HAFM installation, the test notification message is transmitted over telephone lines or LAN.

4. Click **Send Test**. Call-home and e-mail test messages are transmitted and an **Information** dialog box displays, as shown in Figure 2–47. Click **OK** to close the dialog box.

5.   Verify with recipients that call-home and e-mail notifications were received.

Figure 2–47: Information dialog box

Task 16: Back Up HAFM Configuration Data

It is important to back up the HAFM configuration data. This data is used to restore the HAFM server operating environment in case of hard drive failure.

Refer to the *hp StorageWorks HAFM server installation guide* for instructions on backing up the HAFM configuration data.

Once the HAFM configuration data is backed up, go to "Task 17: Cable Fibre Channel Ports" on page 2–66.

Task 17: Cable Fibre Channel Ports

Perform this task to connect devices to the switch. To cable Fibre Channel ports:

1.   Route fiber-optic jumper cables from customer-specified Fibre Channel devices, FC-AL devices, or fabric switches to ports at the front of the switch.

2.   Connect device cables to SFP optical port transceivers. Start with port 0 (far right) and continue sequentially to the left through port 23.

3.   Perform one of the following:

   a.   If the switch is installed on a table or desk top, bundle and secure the Fibre Channel cables as directed by the customer.

   b.   If the switch is installed in a customer-supplied equipment rack, bundle Fibre Channel cables from the switch and other equipment (groups of 16 maximum), and secure them as directed by the customer.

4.   Set the switch online.

Task 18: Connect Switch to a Fabric (Optional)

To provide Fibre Channel connectivity between public devices and fabric-attached devices, connect the switch to an expansion port (E_Port) of an HP Director or Edge Switch. The switch port to switch port connection is called an interswitch link (ISL). To fabric-attach the switch and create an ISL:

1. Ensure the switch is accessible through the EWS interface or defined to the HAFM application. If the fabric element must be defined, refer to the appropriate switch or director installation manual for instructions.

2. Ensure the preferred domain ID for the switch is unique and does not conflict with the ID of another switch participating in the fabric.

    • To change the domain ID using the EWS interface, see "Task 4: Configure the Switch from the Embedded Web Server (Optional)" on page 2–6.

    • To change the domain ID from the HAFM server, see "Task 14: Configure the Edge Switch 2/24 Product Manager Application" on page 2–43.

3. Ensure the R_A_TOV and E_D_TOV values for the switch are identical to the values for all switches participating in the fabric.

    • To change the values using the EWS interface, see "Task 4: Configure the Switch from the Embedded Web Server (Optional)" on page 2–6.

    • To change the values from the HAFM server, see "Task 14: Configure the Edge Switch 2/24 Product Manager Application" on page 2–43.

4. Route a multimode or singlemode fiber-optic cable (depending on the type of SFP transceiver installed) from a customer-specified E_Port of the switch to the switch.

5. Connect the switch-attached fiber-optic cable to the port SFP transceiver.

6. If the switch is managed by an attached HAFM server, go to step 7. If the switch is managed by the EWS interface:

    a. Choose **View** at the left side of the window. The **View** window opens with the **Switch** tab selected and displayed.

    b. At the **View** window, click the **Port Properties** tab. The **Port Properties** page displays with 0 selected, and port information listed for port 0.

    c.   Choose the port number of the port used to make this ISL connection.

    d.   Ensure the **Operational State** field displays **Online** and the **Reason** field displays **N/A** or is blank. If an ISL segmentation or other problem is indicated, refer to the *hp StorageWorks edge switch 2/32 service manual* to isolate the problem. If no problems are indicated, installation tasks are complete.

7.   At the HAFM server's **Product View**, double-click the switch icon. The **Hardware View** for the selected switch displays.

8.   Double-click the port connector used to make this ISL connection to open the **Port Properties** dialog box, as shown in Figure 2–48.
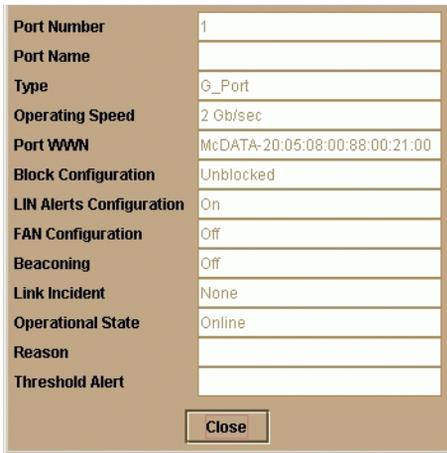
Port Number	1
Port Name	
Type	G_Port
Operating Speed	2 Gb/sec
Port WWN	McDATA-20:05:08:00:88:00:21:00
Block Configuration	Unblocked
LIN Alerts Configuration	On
FAN Configuration	Off
Beaconing	Off
Link Incident	None
Operational State	Online
Reason	
Threshold Alert	

Close

Figure 2–48: Port Properties dialog box

9.   Ensure the **Link Incident** field displays **None** and the **Reason** field is blank. If an ISL segmentation or other problem is indicated, refer to the *hp StorageWorks edge switch 2/24 service manual* to isolate the problem. If no problems are indicated, installation tasks are complete.

A

Regulatory Compliance Notices

This appendix covers the following topics:

Regulatory Compliance ID Numbers

For the purpose of regulatory compliance certifications and identification, your HP StorageWorks Edge Switch 2/24 is assigned a Hewlett-Packard Regulatory Model Number. The Hewlett-Packard Regulatory Model Number for this product is:

RSVLB-0216

The HP StorageWorks Edge Switch 2/24 Regulatory Model Number can be found on the product label, along with the required approval markings and information. When requesting certification information for this product, always refer to this Regulatory Model Number. This Regulatory Model Number should not be confused with the marketing name or product number for your HP StorageWorks Edge Switch 2/24.

Federal Communications Commission Notice

Part 15 of the Federal Communications Commission (FCC) Rules and Regulations has established Radio Frequency (RF) emission limits to provide an interference-free radio frequency spectrum. Many electronic devices, including computers, generate RF energy incidental to their intended function and are, therefore, covered by these rules. These rules place computers and related peripheral devices into two classes, A and B, depending upon their intended installation. Class A devices are those that may reasonably be expected to be installed in a business or commercial environment. Class B devices are those that may reasonably be expected to be installed in a residential environment (for example, personal computers). The FCC requires devices in both classes to bear a label indicating the interference potential of the device as well as additional operating instructions for the user.

The rating label on the device shows the classification (A or B) of the equipment. Class B devices have an FCC logo or FCC ID on the label. Class A devices do not have an FCC logo or ID on the label. After the class of the device is determined, refer to the corresponding statement in the sections below.

Class A Equipment

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at personal expense.

Class B Equipment

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.

- Increase the separation between the equipment and receiver.

- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

- Consult the dealer or an experienced radio or television technician for help.

Declaration of Conformity for Products Marked with FCC Logo—U.S. Only

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

For questions regarding your product, refer to http://thenew.hp.com.

For questions regarding this FCC declaration, contact:

Hewlett-Packard Company
Product Regulations Manager
3000 Hanover St.
Palo Alto, CA 94304

Or call 1-650-857-1501

To identify this product, refer to the part, Regulatory Model Number, or product number found on the product.

Modifications

The FCC requires the user to be notified that any changes or modifications made to this device that are not expressly approved by Hewlett-Packard Company may void the user's authority to operate the equipment.

Network and Serial Cables

Connections to this device must be made with shielded cables with metallic RFI/EMI connector hoods in order to maintain compliance with FCC Rules and Regulations.

IEC EMC Statement (Worldwide)

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

Spécification ATI Classe A (France)

DECLARATION D'INSTALLATION ET DE MISE EN EXPLOITATION d'un matériel de traitement de l'information (ATI), classé A en fonction des niveaux de perturbations radioélectriques émis, définis dans la norme européenne EN 55022 concernant la Compatibilité Electromagnétique.

Canadian Notice (Avis Canadien)

Class A Equipment

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

Class B Equipment

This Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

European Union Notice

Products with the CE Marking comply with both the EMC Directive (89/336/EEC) and the Low Voltage Directive (73/23/EEC) issued by the Commission of the European Community.

Compliance with these directives implies conformity to the following European Norms (the equivalent international standards are in parenthesis):

•   EN55022 1998 (CISPR 22)-Electromagnetic Interference

- EN55024 1998 (IEC61000-4-2, IEC61000-4-3, IEC61000-4-4, IEC61000-4-5, IEC61000-4-6, IEC61000-4-8, IEC61000-4-11)-Electromagnetic Immunity

- EN60950 (IEC60950)-Product Safety

- Power Quality: (IEC610000-3-2)-Harmonics and (IEC61000-3-3)-Voltage Fluctuations and Flicker

- Also approved under UL 1950, 3rd Edition/CSA C22.2 No. 950-95, Safety of Information Technology Equipment

Japanese Notice

ご使用になっている装置にVCCIマークが付いていましたら、次の説明文を
お読み下さい。

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準
に基づくクラスB情報技術装置です。この装置は、家庭環境で使用すること
を目的としていますが、この装置がラジオやテレビジョン受信機に近接して
使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。

VCCIマークが付いていない場合には、次の点にご注意下さい。

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に
基づくクラスA情報技術装置です　この装置を家庭環境で使用すると電波
妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ず
るよう要求されることがあります。

Taiwanese Notice

警告使用者：這是甲類的資訊產品，在居住的
環境中使用時，可能會造成射頻干擾，在這種
情況下，使用者會被要求採取某些適當的對策。

Harmonics Conformance (Japan)

高調波ガイドライン適合品

German Noise Declaration

Schalldruckpegel Lp =64.4 dB(A)
Am Arbeitsplatz (operator position)
Normaler Betrieb (normal operation)
Nach ISO 7779:1988 / EN 27779:1991 (Typprüfung)

Laser Safety

> ⚠ **WARNING: To reduce the risk of exposure to hazardous radiation:**
> - Do not try to open the laser device enclosure. There are no user-serviceable components inside.
> - Do not operate controls, make adjustments, or perform procedures to the laser device other than those specified herein.
> - Allow only Hewlett-Packard authorized service technicians to repair the laser device.

Certification and Classification Information

This product contains a laser internal to the Optical Link Module (OLM) for connection to the Fibre communications port.

In the USA, the OLM is certified as a Class 1 laser product conforming to the requirements contained in the Department of Health and Human Services (DHHS) regulation 21 CFR, Subchapter J. The certification is indicated by a label on the plastic OLM housing.

Outside the USA, the OLM is certified as a Class 1 laser product conforming to the requirements contained in IEC 825-1:1993 and EN 60825-1:1994, including Amendment 11:1996.

The OLM includes the following certifications:

- UL Recognized Component (USA)

- CSA Certified Component (Canada)

- TUV Certified Component (European Union)

- CB Certificate (Worldwide)

The following figure shows the Class 1 information label that appears on the metal cover of the OLM housing.

CLASS 1
LASER PRODUCT

LASER KLASSE 1

Laser Safety (Finland)

LASERTURVALLISUUS

LUOKAN 1 LASERLAITE

KLASS 1 LASER APPARAT

hp StorageWorks edge switch 2/24 -kytkinlaitteessa on 24 optista liitäntäporttia, joissa on laserdiodin sisältävä lähetinosa. Fibre Channel -kytkinlaite on käyttäjälle turvallinen luokan 1 laserlaite, eikä käyttäjä voi altistua turvallisuusluokan 1 ylittävälle lasersäteilylle toimiessaan käyttöohjeen mukaisesti.

Laitteen turvallisuusluokka on määritetty standardin EN 60825-1 (1994) mukaisesti.

VAROITUS ! Laitteen käyttäminen muulla kuin käyttöohjeessa mainitulla tavalla saattaa altistaa käyttäjän turvallisuusluokan 1 ylittävälle näkymättömälle lasersäteilylle.

VARNING ! Om apparaten används på annat sätt än i bruksanvisning specificerats, kan användaren utsättas för osynlig laserstrålning, som överskrider gränsen för laserklass 1.

hp StorageWorks edge switch 2/24 -kytkinlaitteessa ei ole käyttäjän tehtäväksi tarkoitettuja huolto- tai säätötoimenpiteitä. Laitteen saa avata ja huoltaa ainoastaan sen huoltamiseen koulutettu henkilö.

Tiedot laitteessa käytettävän laserdiodin säteilyominaisuuksista:

Aallonpituus 850 nm

Declaration of Conformity

The Declaration of Conformity is shown on the next page.

DECLARATION OF CONFORMITY
According to ISO/IEC Guide 22 and EN 45014

Manufacturer's Name: Hewlett-Packard Company

Manufacturer's Address: 11311 Chinden Blvd.
Boise, ID 83714
USA

Declares, that the product

Product Name: hp StorageWorks edge switch 2/24
Product Number: 316095-B21, DS-DMGGE-BD, and ES-4500
Regulatory Model Number: RSVLB-0216
Product Options: All

Conforms to the following Product Specifications:

Safety: IEC 60950:1991+A1+A2+A3+A4 / EN 60950:1992+A1+A2+A3+A4+A11
GB 4943:1995
IEC 60825-1:1993 / EN 60825-1:1994 +A11, Class 1 (Laser/LED)

EMC: CISPR 22:1997+A1 / EN 55022:1998 +A1 Class A [1]
GB 9254:1988
CISPR 24:1997 / EN 55024:1998
IEC 61000-3-2:1995 / EN 61000-3-2:1995 + A14
IEC 61000-3-3:1994 / EN 61000-3-3:1995

Supplementary Information:

The product herewith complies with the requirements of the Low Voltage Directive
73/23/EEC and the EMC Directive 89/336/EEC and carries the CE-marking accordingly.

1) The Product was tested in a worst-case configuration which maximizes RFI
emissions.

Boise, ID USA
November 18, 2002

George E. Barrett, Regulatory Mgr.

European contact for regulatory topics only: Hewlett-Packard GmbH, HQ-TRE, Herrenberger Strasse 140, D-71034
Böblingen (FAX: + 49-7031-14-3143)

B

Technical Specifications

This appendix contains the following information:

Factory Defaults

Table B–1 lists the defaults for the passwords, and IP, subnet, and gateway addresses.

Table B–1: Factory-Set Defaults

Item	Default
Customer password	password
Maintenance password	level-2
IP address	10.1.1.10
Subnet mask	255.0.0.0
Gateway address	0.0.0.0

Table B–2 provides the Edge Switch factory-default values for Reset Configuration option.

Table B–2: Switch Factory-Default Values for Reset Configuration Option

Configuration	Description	Default
Identification	Switch Name	NULL string
	Switch Description	"Fibre Channel Switch"
	Switch Contact	"End User Contact (please configure)"
	Switch Location	"End User Contact (please configure)"
Ports	Port Names	NULL strings
	Port Blocked States	Unblocked
	FAN	Enabled
	LIN Alerts	Enabled
	Ports enabled	8
Switch Addressing	IP Address	10.1.1.10
	Subnet Mask	255.0.0.0
	Gateway Address	0.0.0.0
	MAC Address	PROM value
Operating Mode	Must select one of two modes: Homogeneous mode or Open Fabric 1.0. The recommended mode is Open Fabric 1.0.	Open Fabric 1.0 mode
Operating Parameters	Preferred Domain ID	1
	R_A_TOV	10 seconds (100 tenths)
	E_D_TOV	2 seconds (20 tenths)
	Switch Priority	Default
	Switch Speed	2 Gb/sec
	Rerouting Delay	Enabled

Table B–2: Switch Factory-Default Values for Reset Configuration Option

Configuration	Description	Default
SNMP	SNMP Communities	"public" — 5 NULL strings
	SNMP Write Authorizations	Read only per community
	Trap Recipient IP Addressees	0 for each
	UDP Port	162
	SNMP Authorization Trap State	disabled
Management Server	Active Equal Saved State	Disabled
	Remote Offline Control State	Disabled
Zoning	Number of Zone Members	0
	Number of Zones	0
	Number of Zone Sets	0
	Zone Names	None
	Zone Sets Names	None
	Zone Members	None
	Default Zone State	Disabled
	Active Zone Set State	Disabled
	Active Zone Set Name	NULL string

Physical Dimensions

Table B–3 lists Edge Switch 2/24 dimensions.

Table B–3: Dimensions

Dimension	Size
Height	4.3 cm (1.7 in)
Width	43.4 cm (17.1 in)
Depth	48.3 cm (19.0 in)
Weight	7.7 kg (17 lb)
Shipping Weight	18.1 kg (40 lb)

Environmental Specifications

Figure B–4 lists environmental ranges for shipping, storing, and operating the HP StorageWorks Edge Switch 2/24.

Table B–4: Environmental Specifications

Specification	Shipping	Storage	Operating
Weight	18.1 kg (40 lb)	7.7 kg (17 lb)	7.7 kg (17 lb)
Temperature	-40° F to 140° F (-40° C to 60° C)	34° F to 140° F (1° C to 60° C)	40°F to 104°F (4°C to 40 °C)
Humidity	5% to 100%	5% to 80%	8% to 80%
Maximum wet-bulb temperature	84° F (29° C)	84°F (29°C)	81°F (27°C)
Altitude	40,000 ft (12,192 m)	40,000 ft (12,192 m)	10,000 ft (3,048 m)

Power Requirements

Table B–5 lists Edge Switch 2/24 power requirements.

Table B–5: Power Requirements

Specification	Value
Input voltage	90 to 264 VAC
Input frequency	47 to 63 Hz

Operating Tolerances

Table B–6 lists heating and cooling specifications, shock tolerances, vibration, acoustical noise and inclination.

Table B–6: Operating Tolerances

Specification	Value
Heat dissipation	49 watts (167 BTU/hr)
Cooling airflow clearances	Right and left sides: 1.3 cm (0.5 inches)
	Front and rear: 7.6 cm (3.0 in)
	Top and bottom: No clearance required
Shock and vibration tolerance	60 Gs for 10 milliseconds without nonrecoverable errors
Acoustical noise	70 dB "A" scale
Inclination	10° maximum

Laser Information

Three configurations of cards with fixed optics will be provided for each of the connector types: four extended long-wave ports, four long-wave ports, and four short-wave ports.

Table B–7: Laser Specifications - 2 Gb

Part Number	Transceivers on UPM Card	Wave Length	Media/ Distance	Standard
300836-B21 Long wave - 35 Km	4 Extended Long wave	1310 nm	*9/125* μm Single-mode: 1 m–35 Km	100-SM-LL-L
300835-B21 Long wave - 10 Km	4 Long wave	1310 nm	*9/125* μm Single-mode: 1 m–10 Km	100-SM-LL-L
300834-B21 Short wave	4 Short wave	850 nm	*50/125* μm Multimode: 2 m–500 m *62.5/125* μm Multimode: 1 m–200 m	100-M5-SN-I

C

Electrostatic Discharge

This appendix contains the following information.

- Precautions Against Electrostatic Discharge
- Ground Methods

Precautions Against Electrostatic Discharge

To prevent damaging the system, be aware of the precautions you need to follow when setting up the system or handling parts. A discharge of static electricity from a finger or other conductor may damage system boards or other static-sensitive devices. This type of damage may reduce the life expectancy of the device.

To prevent electrostatic damage, observe the following precautions:

- Avoid hand contact by transporting and storing products in static-safe containers.
- Keep electrostatic-sensitive parts in their containers until they arrive at static-free workstations.
- Place parts on a grounded surface before removing them from their containers.
- Avoid touching pins, leads, or circuitry.
- Always make sure you are properly grounded when touching a static-sensitive component or assembly.

Grounding Methods

There are several methods for grounding. Use one or more of the following methods when handling or installing electrostatic-sensitive parts:

- Use a wrist strap connected by a ground cord to a grounded workstation or computer chassis. Wrist straps are flexible straps with a minimum of 1 megohm ± 10 percent resistance in the ground cords. To provide proper ground, wear the strap snug against the skin.

- Use heel straps, toe straps, or boot straps at standing workstations. Wear the straps on both feet when standing on conductive floors or dissipating floor mats.

- Use conductive field service tools.

- Use a portable field service kit with a folding static-dissipating work mat.

If you do not have any of the suggested equipment for proper grounding, have a HP authorized reseller install the part.

NOTE: For more information on static electricity, or for assistance with product installation, contact your HP authorized reseller.

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