hp StorageWorks

edge switch 2/24 service manual

Part Number: AA-RTDXA-TE

First Edition (January 2003)

This manual describes the HP StorageWorks Edge Switch 2/24 and attached HP StorageWorks High Availability Fabric Manager (HAFM) application. For service representatives, it describes diagnostic procedures, repair procedures, and the removal and replacement procedures for field-replaceable units (FRUs).

invent

Hewlett-Packard Company makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Hewlett-Packard Company shall not be liable for technical or editorial errors or omissions contained herein. The information is provided “as is” without warranty of any kind and is subject to change without notice. The warranties for Hewlett-Packard Company products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty.

Printed in the U.S.A.

edge switch 2/24 service manual
First Edition (January 2003)
Part Number: AA-RTDXA-TE

Contents

Contents

About This Manual

General Information

Diagnostics

Repair Information

FRU Removal and Replacement

Messages

Event Codes

Glossary

Index

Figures

Tables

About This Manual

This manual describes the service procedures for the HP StorageWorks Edge Switch 2/24.

Intended Audience

This publication is intended for service personnel, and any individuals who monitor, configure, and repair the Edge Switch 2/24.

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 manual. They have the following meanings.

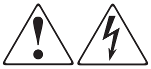
⚠ **WARNING: Text set off in this manner indicates that failure to follow directions in the warning could result in bodily harm or loss of life.**

△ **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.

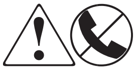
NOTE: Text set off in this manner presents commentary, sidelights, or interesting points of information.

Symbols on Equipment



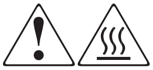
Any enclosed surface or area of the equipment marked with these symbols indicates the presence of electrical shock hazards. Enclosed area contains no operator serviceable parts.

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



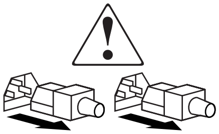
Any RJ-45 receptacle marked with these symbols indicates a network interface connection.

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



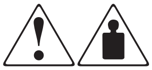
Any surface or area of the equipment marked with these symbols indicates the presence of a hot surface or hot component. Contact with this surface could result in injury.

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 manual, 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

General Information

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 gigabits per second, redundant switched data paths, a scalable number of active ports, and long transmission distances (up to 35 kilometers).

Switch Description

The Edge Switch 2/24 provides Fibre Channel connectivity through 24 generic mixed ports (GX_Ports). Switch ports operate at either 1.0625 or 2.125 gigabits per second (Gbps), and 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 can be installed on a table or desk top, or mounted in an equipment cabinet or in any standard equipment rack.

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.

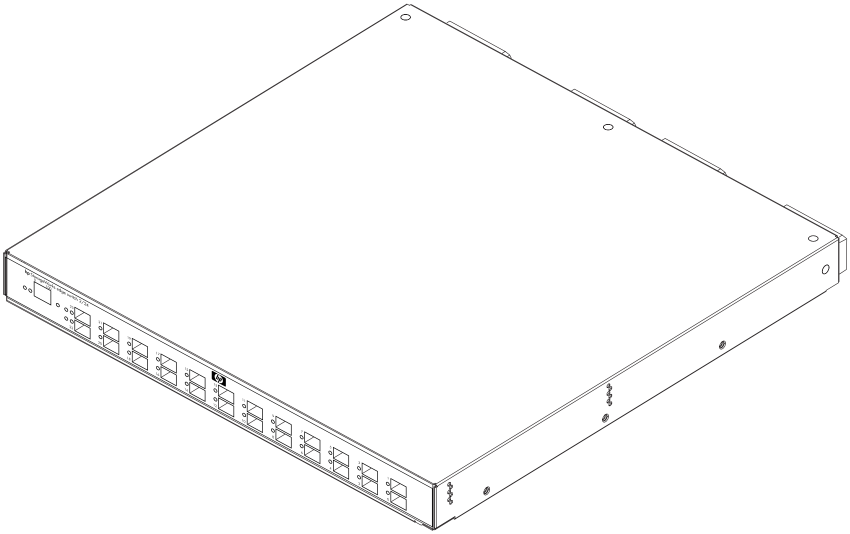


Figure 1–1: Edge Switch 2/24 (front view)

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.

Maintenance Approach

Whenever possible, the maintenance approach instructs service personnel to perform fault isolation and repair procedures without degrading or interrupting operation of the switch, attached devices, or associated applications. Switch fault isolation begins when one or more of the following occur:

- System event information displays at the attached HAFM server, a remote workstation communicating with the HAFM server, or the embedded web server interface.
- LEDs on the switch front panel or FRUs illuminate to indicate a hardware malfunction.
- An unsolicited SNMP trap message is received at a management workstation, indicating an operational state change or failure.
- Notification of a significant system event is received at a designated support center through an e-mail message or the call-home feature.

System events can be related to one of the following:

- Switch or HAFM server failure (hardware or software).
- Ethernet LAN communication failure between the switch and HAFM server
- Link failure between a port and attached device.
- ISL failure or segmentation of an E_Port.

Fault isolation and service procedures vary depending on the system event information provided. Fault isolation and related service information is provided through maintenance analysis procedures (MAPs) documented in Chapter 3. MAPs consist of step-by-step procedures that prompt service personnel for information or describe a specific action to be performed. MAPs provide information to interpret system event information, isolate a switch failure to a single FRU, remove and replace the failed FRU, and verify switch operation. The fault isolation process normally begins with "MAP 0000: Start MAP" on page 2-6.

Ensure the correct switch is selected for service (if the HAFM server manages multiple switches or other HA Fabric Directors and Edge Switches) by enabling unit beaconing at the failed switch. The amber system error LED on the switch front panel blinks when beaconing is enabled. Instructions to enable beaconing are incorporated into MAP steps.

Tools and Test Equipment

This section describes tools and test equipment that may be required to install, test, service, and verify operation of the switch and attached HAFM server.

Tools Supplied with the Switch

The following tools are supplied with the switch. Use of the tools may be required to perform one or more installation, test, service, or verification tasks. These tools are supplied with the switch or must be supplied by service personnel.

- Fiber-optic loopback plug - An SFP multi-mode (shortwave laser) or single-mode (longwave laser) loopback plug is required to perform port loopback diagnostic tests. One loopback plug is shipped with the switch, depending on the type of port transceivers installed. Both plugs are shipped if shortwave laser and longwave laser transceivers are installed. The plug is shown in Figure 1–2.

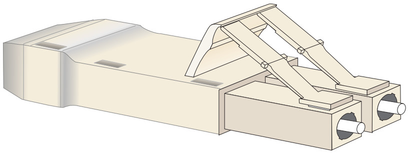


Figure 1–2: Multi-mode and Single-mode Loopback Plugs

- **Fiber-optic protective plug -** For safety and port transceiver protection, fiber-optic protective plugs must be inserted in all port SFPs without fiber-optic cables attached. The switch is shipped with protective plugs installed in all ports. A protective plug is shown in Figure 1–3.

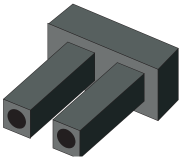


Figure 1–3: Fiber-Optic Protective Plug

- **Null modem cable -** An asynchronous RS-232 null modem cable is required to configure switch network addresses and acquire event log information through the maintenance port. The cable has nine conductors and DB-9 male and female connectors. A null modem cable is not a standard (straight-through) RS-232 cable. Refer to Figure 1–4.

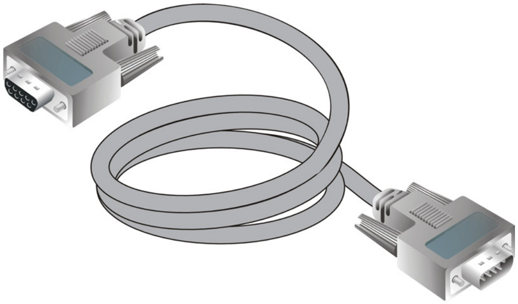


Figure 1–4: Null Modem Cable

Tools Supplied by Service Personnel

The following tools are expected to be supplied by service personnel performing switch installation and maintenance actions. Use of the tools may be required to perform one or more installation, test, service, or verification tasks.

- **Scissors or pocket knife -** A sharp cutting edge (scissors or knife blade) may be required to cut the protective strapping when unpacking the switch, HAFM server, Ethernet hub, or replacement FRUs.
- **Standard flat-tip and cross-tip (Phillips) screwdrivers -** Screwdrivers are required to remove, replace, adjust or tighten various connector or chassis components, and to remove and replace power supplies.
- **Maintenance terminal (desktop or notebook PC) -** the PC is required to configure switch network addresses and acquire event log information through the maintenance port. The PC must have:
  - — The Microsoft Windows 98, Windows 2000, 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.
- **Fiber-optic cleaning kit -** The kit contains tools and instructions to clean fiber-optic cable, connectors, loopback plugs, and protective plugs.

Additional Information

The following Edge Switch 2/24 documents provide additional information:

- For detailed information about Edge Switch 2/24 front and rear panel features, field replaceable units (FRUs), management options and operational features, installation, configuration and technical specifications, see the *hp StorageWorks edge switch 2/24 installation guide*.
- For information on managing the Edge Switch 2/24 using the High Availablity Fabric Manager (HAFM) and Product Manager applications, see the *hp StorageWorks edge switch 2/24 product manager user guide*.

2

Diagnostics

This chapter describes diagnostic procedures used by service representatives to isolate HP StorageWorks Edge Switch 2/24 problems or failures to the field-replaceable unit (FRU) level. The chapter specifically describes how to perform maintenance analysis procedures (MAPs).

Maintenance Analysis Procedures

Maintenance Analysis Procedures (MAPs) provide fault isolation and related service procedures. They are step-by-step procedures that prompt service personnel for information and describe a maintenance action. They provide information to interpret system events, isolate a switch failure to a single FRU, remove and replace the failed FRU, and verify switch operation.

Factory Defaults

Table 2–1 lists the defaults for the passwords, and IP, subnet, and gateway addresses.

Table 2–1: 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

Quick Start

Table 2–2 lists the MAPs in this chapter. Fault isolation normally begins at MAP 0000: Start MAP on page 2–6.

Table 2–2: MAP Summary

MAP	Page
MAP 0000: Start MAP	page 2–6
MAP 0100: Power Distribution Analysis	page 2–27
MAP 0200: POST Failure Analysis	page 2–35
MAP 0300: Console Application Problem Determination	page 2–38
MAP 0400: Loss of Console Communication	page 2–44
MAP 0500: FRU Failure Analysis	page 2–59
MAP 0600: Port Failure and Link Incident Analysis	page 2–64
MAP 0700: Fabric, ISL, and Segmented Port Problem Determination	page 2–79
MAP 0800: Console PC Problem Determination	page 2–91

Table 2–3 lists the event codes and the corresponding MAP references, providing a quick start reference if an event code is readily available.

Table 2–3: Event Codes versus Maintenance Action

Event Code	Explanation	Action
001	System power-down.	Power on switch.
011	Login server database invalid.	Go to MAP 0700.
021	Name server database invalid.	Go to MAP 0700.
031	SNMP request received from unauthorized community.	Add community name.
051	Management server database invalid.	Go to MAP 0700.
052	Management server internal error.	Go to MAP 0700.
061	Fabric controller database invalid.	Go to MAP 0700.
062	Maximum interswitch hop count exceeded.	Go to MAP 0700.
063	Received link state record too large.	Go to MAP 0700.

Table 2–3: Event Codes versus Maintenance Action (Continued)

Event Code	Explanation	Action
070	E_Port is segmented.	Go to MAP 0700.
071	Switch is isolated.	Go to MAP 0700.
072	E_Port connected to unsupported switch.	Go to MAP 0700.
073	Fabric initialization error.	Refer to Collecting Maintenance Data on page 3–22.
074	ILS frame delivery error threshold exceeded.	Refer to Collecting Maintenance Data on page 3–22.
080	Unauthorized worldwide name.	Go to MAP 0600.
081	Invalid attachment.	Go to MAP 0600
120	Error while processing system management command.	Go to MAP 0600
121	Zone set activation failed - zone set too large.	Reduce size of zone set and retry.
200	Power supply AC voltage failure.	Go to MAP 0100.
201	Power supply DC voltage failure.	Go to MAP 0100.
203	Power supply AC voltage recovery.	No action required.
204	Power supply DC voltage recovery.	No action required.
206	Power supply removed.	Replace FRU.
207	Power supply installed.	No action required.
300	Cooling fan propeller failed.	Go to MAP 0500.
301	Cooling fan propeller failed.	Go to MAP 0500.
302	Cooling fan propeller failed.	Go to MAP 0500.
303	Cooling fan propeller failed.	Go to MAP 0500.
304	Cooling fan propeller failed.	Go to MAP 0500.
305	Cooling fan propeller failed.	Go to MAP 0500.
310	Cooling fan propeller recovered.	No action required.
311	Cooling fan propeller recovered.	No action required.
312	Cooling fan propeller recovered.	No action required.

Table 2–3: Event Codes versus Maintenance Action (Continued)

Event Code	Explanation	Action
313	Cooling fan propeller recovered.	No action required.
314	Cooling fan propeller recovered.	No action required.
315	Cooling fan propeller recovered.	No action required.
400	Power-up diagnostic failure.	Go to MAP 0200.
410	CTP reset.	No action required.
411	Firmware fault.	Go to MAP 0200.
421	Firmware download complete.	No action required.
423	CTP firmware download initiated.	No action required.
430	Excessive Ethernet transmit errors.	Go to MAP 0400.
431	Excessive Ethernet receive errors.	Go to MAP 0400.
432	Ethernet adapter reset.	Go to MAP 0400.
433	Non-recoverable Ethernet fault.	Go to MAP 0500.
440	Embedded port hardware failed.	Go to MAP 0500.
442	Embedded port anomaly detected.	No action required.
445	ASIC detected a system anomaly.	No action required.
453	New feature key installed.	No action required.
506	Fibre Channel port failure.	Go to MAP 0600.
507	Loopback diagnostics port failure.	Go to MAP 0600.
508	Fibre Channel port anomaly detected.	No action required.
510	SFP optical transceiver hot-insertion initiated.	No action required.
512	SFP optical transceiver nonfatal error.	Go to MAP 0600.
513	SFP optical transceiver hot-removal completed.	No action required.
514	SFP optical transceiver failure.	Go to MAP 0600.
523	FL_Port open request failed.	No action required.
524	No AL_PA acquired.	No action required.
525	FL_Port arbitration timeout.	No action required.
581	Implicit incident.	Go to MAP 0600.

Table 2–3: Event Codes versus Maintenance Action (Continued)

Event Code	Explanation	Action
582	Bit error threshold exceeded.	Go to MAP 0600.
583	Loss of signal or loss of synchronization.	Go to MAP 0600.
584	Not operational primitive sequence received.	Go to MAP 0600.
585	Primitive sequence timeout.	Go to MAP 0600.
586	Invalid primitive sequence received for current link state.	Go to MAP 0600.
810	High temperature warning (CTP thermal sensor).	Go to MAP 0500.
811	Critically hot temperature warning (CTP thermal sensor).	Go to MAP 0500.

MAP 0000: Start MAP

This MAP describes initial fault isolation for the Edge Switch 2/24. Fault isolation begins at the High Availability Fabric Manager (HAFM) server, failed switch, Internet-connected personal computer (PC) running the Embedded Web Server (EWS) interface, or attached host.

1

Prior to fault isolation, acquire the following information from the customer:

- A system configuration drawing or planning worksheet that includes the HAFM server, switch, other HP products, and device connections.
- The location of the HAFM server and all switches.
- The internet protocol (IP) address, gateway address, and subnet mask for the switch reporting the problem.
- If performing fault isolation using the HAFM server:
    - The Windows NT user name and password. These are required when prompted during any MAP or repair procedure that directs the HAFM server to be rebooted.
    - The user name, maintenance password, and HAFM server name. All are case sensitive and required when prompted at the **HAFM Login** dialog box.
- If performing fault isolation using a customer-supplied server:
    - The operating system user name and password. These are required when prompted during any MAP or repair procedure that directs the server to be rebooted.
    - The user name, maintenance password, and server name. All are case sensitive and required when prompted at the **HAFM Login** dialog box.
- If performing fault isolation using the EWS interface, the administrator user name and password. Both are case sensitive and required when prompted at the **Username and Password Required** dialog box. (Note: operational status for the switch can be obtained from the EWS by viewing the Fabric page, Products tab.)

Continue.

2

Are you at the HAFM server (or customer-supplied server)?

YES **NO**

↓ **Go to** step 22

3

Did the HAFM server (or customer-supplied server) lock up or crash and:

- Display an application warning or error message, or
- Not display an application warning or error message, or
- Display a **Dr. Watson for Windows NT** dialog box?

NO **YES**

↓ An HAFM server (or customer-supplied server) application problem is indicated. Event codes are not recorded. Go to MAP 0300: Console Application Problem Determination on page 2-38. **Exit MAP.**

4

Did the HAFM server (or customer-supplied server) crash and display a blue screen with the system dump file in hexadecimal format (blue screen of death)?

NO **YES**

↓ An HAFM server (or customer-supplied server) application problem is indicated. Event codes are not recorded. Go to MAP 0300: Console Application Problem Determination on page 2–38. **Exit MAP.**

5

Is the HAFM application active?

NO **YES**

↓ **Go to** step 7**.**

6

Reboot the HAFM server (or customer-supplied server) PC. If the customer-supplied server does not use the Windows 2000 operating system, refer to the supporting documentation to reboot the server.

Reboot the HAFM server PC and perform system diagnostics.

a. Click the Windows **Start** button. The **Windows Workstation** menu displays.

b. At the **Windows Workstation** menu, select **Shut Down**. The **Shut Down Windows** dialog box appears.

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

d. Wait approximately 30 seconds and power on the PC. After POSTs complete, the **Begin Logon** dialog box displays.

e. At the **HAFM Login** dialog box, type a user name, password, and HAFM server name (obtained in step 1, and all are case sensitive), and click **Login**. The application opens and the **Products View** displays (Figure 2–1).

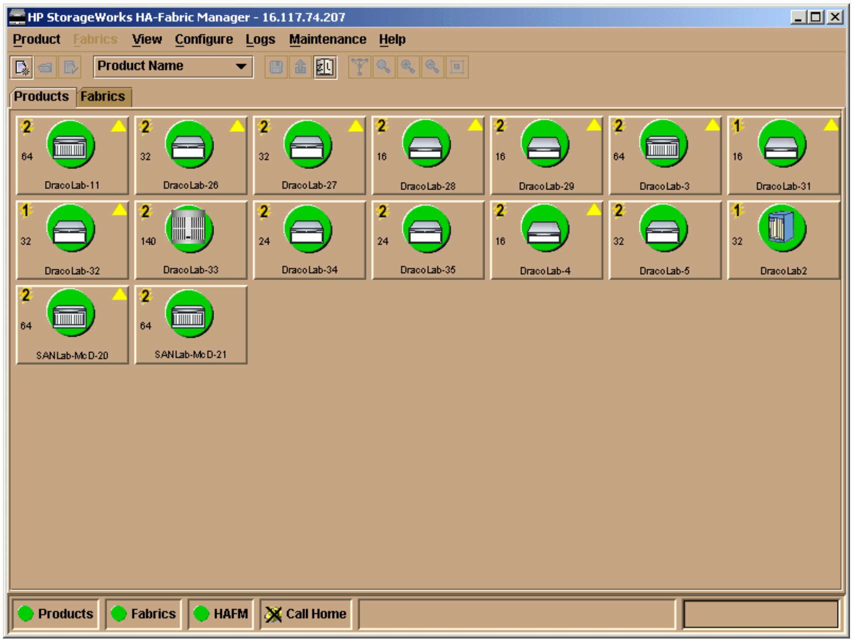


Figure 2–1: Products View

Did the **Products View** display and does the HAFM application appear operational?

YES **NO**

↓ An HAFM server (or customer-supplied server) hardware problem is indicated. Event codes are not recorded. Go to MAP 0800: Console PC Problem Determination on page 2–91. **Exit MAP.**

7

Inspect the alert indicators of each managed switch (or switch) at the top of the **Products View**. The indicator shows the status of managed switches or the status of the link between the HAFM server (or customer-supplied server) and managed switches as follows:

- A green circle indicates that the switch is operational.
- A yellow triangle indicates that the switch is operating in degraded mode.
- A red diamond with yellow background indicates that the switch is not operational.
- A grey square indicates that the status of the switch is unknown.

Does a grey square appear as the background to the icon representing the switch reporting the problem?

YES **NO**

↓ **Go to** step 11**.**

The grey square indicates the HAFM server (or customer-supplied server) cannot communicate with the switch because:

- The switch-to-server Ethernet link failed.
- AC power distribution in the switch failed, or AC power was disconnected.
- The switch control processor (CTP) failed.

Continue.

8

Ensure the switch reporting the problem is connected to facility AC power. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES **NO**

↓ A power distribution problem is indicated. **Go to** step 21 to obtain event codes. If no event codes are found, go to MAP 0100: Power Distribution Analysis on page 2–27. **Exit MAP.**

9

At the switch, inspect the amber LED on the switch.

Is the amber LED illuminated on the switch?

NO **YES**

↓ Failure of the CTP is indicated. Event codes are not recorded. Go to MAP 0500: FRU Failure Analysis on page 2-59. **Exit MAP.**

10

A switch-to-server Ethernet link failure is indicated.

Go to step 21 to obtain event codes. If no event codes are found, go to MAP 0400: Loss of Console Communication on page 2-44.
Exit MAP.

11

Does a red diamond with yellow background (failure indicator) appear as the background to the icon representing the switch reporting the problem?

YES **NO**

↓ **Go to** step 13**.**

12

Double-click the icon representing the switch reporting the problem. The **Hardware View** displays. At the **Hardware View**:

- Observe the **Edge Switch 2/24 Status** table is yellow and the switch status is NOT OPERATIONAL.
- Inspect FRUs for a blinking red and yellow diamond (failed FRU indicator) that overlays the FRU graphic.

Do blinking red and yellow diamonds overlay FRU graphics?

NO **YES**

↓ Failure of all installed FRUs is indicated. **Go to** step 21 to obtain event codes. If no event codes are found, go to MAP 0700: Fabric, ISL, and Segmented Port Problem Determination on page 2-79. **Exit MAP.**

13

Does a yellow triangle (attention indicator) appear as the background to the icon representing the switch reporting the problem?

YES **NO**

↓ **Go to** step 16**.**

14

Double-click the icon representing the switch reporting the problem. The **Hardware View** displays. At the **Hardware View**:

- Observe the **Edge-24 Status** table is yellow and the switch status is **Minor Failure** or **Redundant Failure**.
- Inspect FRUs for a blinking red and yellow diamond (failed FRU indicator) that overlays the FRU graphic.

Does a blinking red and yellow diamond overlay a power supply graphic?

NO **YES**

↓ A power supply failure is indicated. **Go to** step 21 to obtain event codes. If no event codes are found, go to MAP 0100: Power Distribution Analysis on page 2-27. **Exit MAP.**

15

Does a blinking red and yellow diamond overlay a FRU graphic?

NO **YES**

↓ A port failure is indicated. **Go to** step 21 to obtain event codes. If no event codes are found, go to MAP 0700: Fabric, ISL, and Segmented Port Problem Determination on page 2-79.
Exit MAP.

16

A green circle appears as the background to the icon representing the switch reporting the problem. Although the switch is operational, a minor problem may exist.

Double-click the icon representing the switch reporting the problem. The **Hardware View** displays. At the **Hardware View**:

- Inspect the switch for a yellow triangle that overlays the FRU graphic and indicates FRU beaconing is enabled.
- Inspect ports for a yellow triangle (attention indicator) that overlays the port graphic.

Does a yellow triangle overlay the switch or FRU graphic?

YES	NO
↓	**Go to** step 18**.**

17

Beaconing is enabled for the FRU.

a. Consult the customer and next level of support to determine the reason FRU beaconing is enabled.

b. Disable FRU beaconing.

   1. At the **Hardware View**, right-click the FRU graphic. A pop-up menu appears.
   2. Click the **Enable Beaconing** option. The check mark disappears from the box adjacent to the option, and FRU beaconing is disabled.

Was FRU beaconing enabled because a FRU failure or degradation was suspected?

YES	NO
↓	The switch appears operational. **Exit MAP.**

Go to step 2.

18

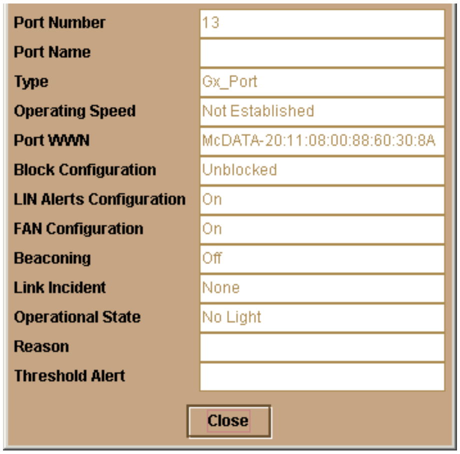
Does a yellow triangle (attention indicator) overlay a port graphic?

YES	NO
↓	**Go to** step 20**.**

19

Inspect the port state and LED status for all ports with an attention indicator.

a. Double-click a port to open the **Port Properties** dialog box (Figure 2–2).



Port Number	13
Port Name	
Type	Gx_Port
Operating Speed	Not Established
Port WWN	McDATA-20:11:08:00:88:60:30:8A
Block Configuration	Unblocked
LIN Alerts Configuration	On
FAN Configuration	On
Beaconing	Off
Link Incident	None
Operational State	No Light
Reason	
Threshold Alert	

Figure 2–2: Port Properties Dialog Box

b. Inspect the **Operational State** field.

Does the **Operational State** field display a `Segmented E_Port` message?

NO **YES**

↓ Expansion port (E_Port) segmentation is indicated. **Go to** step 21 to obtain event codes. If no event codes are found, go to MAP 0700: Fabric, ISL, and Segmented Port Problem Determination on page 2-79. **Exit MAP.**

A message displays indicating a link incident problem. **Go to** step 21 to obtain event codes. If no event codes are found, go to MAP 0700: Fabric, ISL, and Segmented Port Problem Determination on page 2-79.
Exit MAP.

20

A link incident may have occurred, but the LIN alerts option is not enabled for the port and the attention indicator does not appear.

At the **Hardware View**, click **Logs** and select **Link Incident Log**. The **Link Incident Log** displays (Figure 2–3).

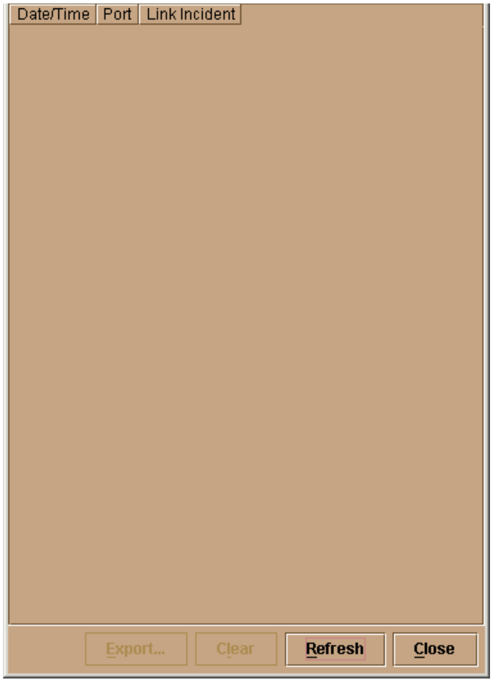


Figure 2–3: Link Incident Log

If a link incident occurred, the affected port number is listed with one of the following messages.

```
Link interface incident - implicit incident.

Link interface incident - bit-error threshold exceeded.

Link failure - loss of signal or loss of synchronization.

Link failure - not-operational primitive sequence (NOS)
received.
```

```
Link failure - primitive sequence timeout.

Link failure - invalid primitive sequence received for the
current link state.
```

Did one of the listed messages appear in the **Link Incident Log**?

YES **NO**

↓ The switch appears operational. **Exit MAP.**

A link incident problem is indicated. **Go to** step 21 to obtain event codes. If no event codes are found, go to MAP 0700: Fabric, ISL, and Segmented Port Problem Determination on page 2-79. **Exit MAP.**

21

Obtain event codes from the Edge Switch 2/24 **Event Log**.

> If multiple event codes are found, note all codes and associated severity levels. Record the date, time, and listed sequence, and determine if the codes are related to the reported problem. Begin fault isolation with the most recent event code with the highest severity level. Other codes may accompany this event code, or may indicate a normal indication after a problem is recovered.

a. At the **Hardware View**, click **Logs** and select **Event Log**. The **Event Log** displays (Figure 2–4).

b. Record the event code, date, time, and severity (**Informational**, **Minor**, **Major**, or **Severe**).

c. Record all event codes that may relate to the reported problem.

Figure 2–4: Event Log

Were one or more event codes found?

NO **YES**

↓ **Go to** Table 2–3 on page 2-2**.**

Return to the MAP step that sent you here.

22

Are you at the switch reporting the problem?

YES **NO**

↓ **Go to** step 34**.**

23

Is the power LED (green) at the switch front bezel illuminated?

NO **YES**

↓ **Go to** step 28**.**

24

Is the switch connected to facility AC power and powered on?

NO **YES**

↓ **Go to** step 27**.**

25

Connect the switch to facility AC power. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES **NO**

↓ A power distribution problem is indicated. **Go to** step 21 to obtain event codes. If no event codes are found, go to MAP 0100: Power Distribution Analysis on page 2-27. **Exit MAP.**

26

Is the power LED (green) at the switch front bezel illuminated?

NO **YES**

↓ **Go to** step 28**.**

A faulty power LED is indicated, but switch and Fibre Channel port operation is not disrupted. The LED is connected to the circuitry in a fan module, and the module must be removed and replaced (See RRP 2: Redundant Power Supply on page 4–5.) **Exit MAP.**

27

Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES **NO**

↓ A power distribution problem is indicated. **Go to** step 21 to obtain event codes. If no event codes are found, go to MAP 0100: Power Distribution Analysis on page 2-27. **Exit MAP.**

A faulty power LED is indicated, but switch and Fibre Channel port operation is not disrupted. The LED is connected to the circuitry in a fan module, and the power supply module must be removed and replaced (See RRP 2: Redundant Power Supply on page 4–5.) Exit MAP.

28

Is the system error LED (amber) at the switch front bezel blinking?

YES **NO**

↓ **Go to** step 30**.**

29

Unit beaconing is enabled for the switch.

a. Consult the customer and next level of support to determine the reason unit beaconing is enabled.

b. Disable unit beaconing.

   1. At the **Hardware View**, right-click the front bezel graphic (away from a FRU). A pop-up menu appears.
   2. Click the **Enable Unit Beaconing** option. The check mark disappears from the box adjacent to the option, and unit beaconing is disabled.

Was unit beaconing enabled because a switch failure or degradation was suspected?

YES **NO**

↓ The switch appears operational. **Exit MAP.**

Go to step 22.

30

Is the system error LED (amber) at the switch front bezel illuminated?

YES **NO**

↓ The switch appears operational. Verify operation at the HAFM server (or customer-supplied server). **Go to** step 3**.**

31

Check FRUs for failure symptoms.

Are any amber LEDs associated with Fibre Channel ports illuminated?

NO **YES**

↓ A Fibre Channel port failure is indicated. **Go to** step 21 to obtain event codes. If no event codes are found, go to MAP 0700: Fabric, ISL, and Segmented Port Problem Determination on page 2-79. **Exit MAP.**

32

Is the amber LED on the switch or FRU illuminated?

NO **YES**

↓ A FRU failure is indicated. **Go to** step 21 to obtain event codes. If no event codes are found, go to MAP 0500: FRU Failure Analysis on page 2-59. **Exit MAP.**

33

Is the amber **PWR** Error LED on a power supply illuminated?

NO **YES**

↓ A power supply failure is indicated. **Go to** step 21 to obtain event codes. If no event codes are found, go to MAP 0100: Power Distribution Analysis on page 2-27. **Exit MAP.**

The switch appears operational. **Exit MAP.**

34

Are you at a PC with a web browser (such as Netscape Navigator or Microsoft Internet Explorer) and an Internet connection to the switch reporting the problem.

YES **NO**

↓ **Go to** step 51**.**

35

Is the web browser PC powered on and communicating with the switch through the Internet connection?

NO **YES**

↓ **Go to** step 37**.**

36

Boot the web browser PC.

a. Power on the PC in accordance with the instructions delivered with the PC. The Windows desktop appears.

b. Launch the PC browser application by double-clicking the appropriate icon at the Windows desktop.

c. At the **Netsite** field (Netscape Navigator) or **Address** field (Internet Explorer), type `http://xxx.xxx.xxx.xxx`, where *`xxx.xxx.xxx.xxx`* is the IP address of the switch (obtained in step 1). The **Username and Password Required** dialog box appears.

d. Type the user name and password obtained in step 1, and click **OK**. The EWS interface opens with the **View** panel displayed.

Continue.

37

Does the EWS interface appear operational with the **View** panel displayed?

NO **YES**

↓ **Go to** step 42**.**

38

A `Page cannot be found, Unable to locate the server, HTTP 404 - file not found`, or other similar message appears. The message indicates the web browser PC cannot communicate with the switch because:

- The switch-to-PC Internet link could not be established.
- AC power distribution in the switch failed, or AC power was disconnected.
- The switch CTP failed.

Continue.

39

Ensure the switch reporting the problem is connected to facility AC power. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES **NO**

↓ A power distribution problem is indicated. Go to MAP 0100: Power Distribution Analysis on page 2-27. **Exit MAP.**

40

At the switch, inspect the amber LED at the switch.

Is the amber LED illuminated?

NO **YES**

↓ Failure of the CTP is indicated. Event codes are not recorded. Go to MAP 0500: FRU Failure Analysis on page 2-59. **Exit MAP.**

41

A switch-to-PC Internet link problem (Internet too busy or IP address typed incorrectly) is indicated.

a. Wait approximately five minutes, then attempt to login to the switch again.

b. At the **Netsite** field (Netscape Navigator) or **Address** field (Internet Explorer), type `http://xxx.xxx.xxx.xxx`, where *`xxx.xxx.xxx.xxx`* is the IP address of the switch (obtained in step 1). The **Username and Password Required** dialog box appears.

c. Type the user name and password obtained in step 1, and click **OK**. If the **View** panel does not display, wait another five minutes and perform this step again.

Does the EWS interface appear operational with the **View** panel displayed?

YES **NO**

↓ Perform switch fault isolation at the HAFM server (or customer-supplied server). **Go to** step 3**.**

42

At the **View** panel, inspect the **Status** field.

Does the switch status indicate **Operational**?

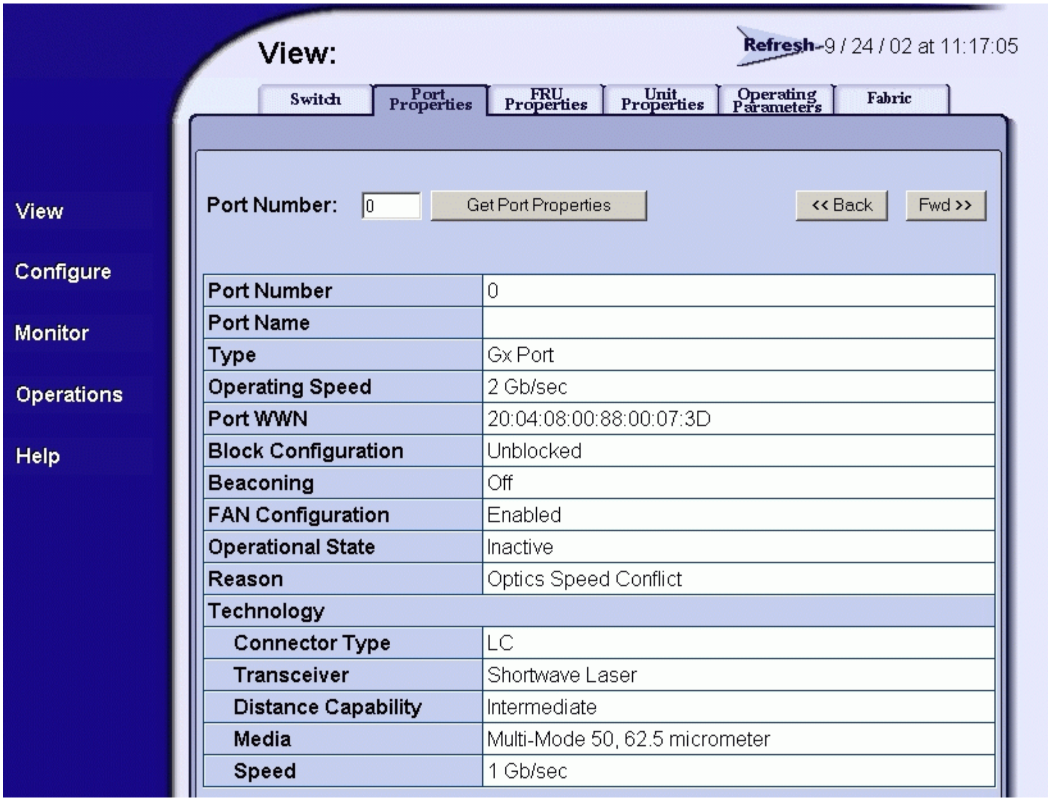
NO **YES**

↓ The switch appears operational. **Exit MAP.**

43

Inspect Fibre Channel port operational states.

a. At the **View** panel, click the **Port Properties** tab. The **View** panel (**Port Properties** tab) displays with port **0** highlighted.



Port Number	0
Port Name	
Type	Gx Port
Operating Speed	2 Gb/sec
Port WWN	20:04:08:00:88:00:07:3D
Block Configuration	Unblocked
Beaconing	Off
FAN Configuration	Enabled
Operational State	Inactive
Reason	Optics Speed Conflict
Technology	
Connector Type	LC
Transceiver	Shortwave Laser
Distance Capability	Intermediate
Media	Multi-Mode 50, 62.5 micrometer
Speed	1 Gb/sec

Figure 2–5: View Panel (Port Properties)

b. Inspect the **Beaconing** and **Operational State** fields.

Does the **Beaconing** field display an **On** message?

YES **NO**

↓ **Go to** step 45**.**

44

Port beaconing is enabled.

a. Consult the customer and next level of support to determine the reason port beaconing is enabled.

b. Disable port beaconing:

1. At the **View** panel, select **Operations** at the left side of the panel. The **Operations** panel opens with the **Port Beaconing** page displayed.
2. Click the **Beaconing State** check box for the port. The check mark disappears from the box and port beaconing is disabled.
3. Return to the **View** panel (**Port Properties** tab).

Continue.

45

At the **View** panel, does the **Operational State** field display a `Segmented` message?

NO **YES**

↓ Port segmentation is indicated. **Go to** step 50 to obtain event codes. If no event codes are found, go to MAP 0700: Fabric, ISL, and Segmented Port Problem Determination on page 2-79. **Exit MAP.**

46

At the **View** panel, does the **Operational State** field display a message indicating a port problem?

NO **YES**

↓ **Go to** step 50 to obtain event codes. If no event codes are found, go to MAP 0700: Fabric, ISL, and Segmented Port Problem Determination on page 2-79. **Exit MAP.**

47

Repeat step 43 through step 46 for each remaining Fibre Channel port for which a problem is suspected (ports **0** through **23**).

Is an problem indicated for any of the ports?

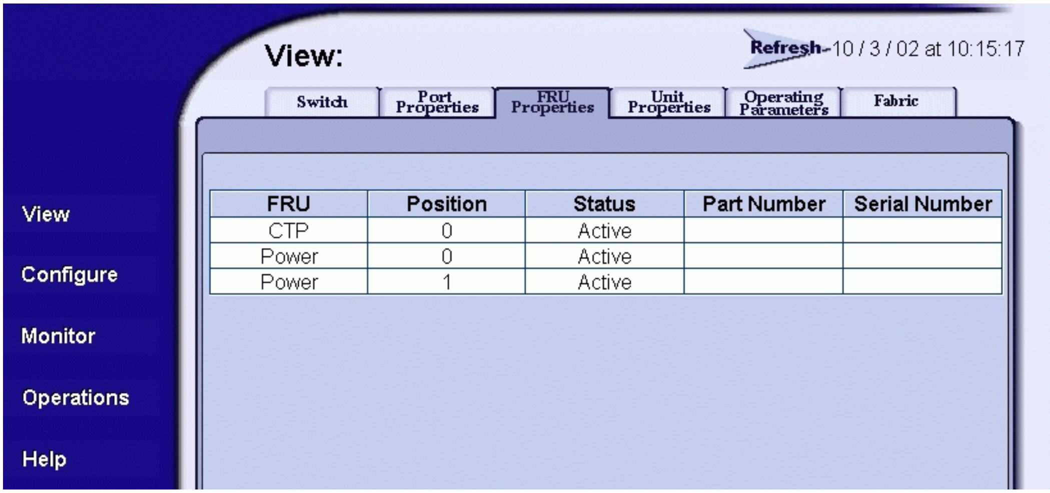
NO **YES**

↓ **Go to** step 50 to obtain event codes. If no event codes are found, go to MAP 0700: Fabric, ISL, and Segmented Port Problem Determination on page 2-79. **Exit MAP.**

48

Inspect power supply operational states.

a. At the **View** panel, click the **FRU Properties** tab. The **View** panel (**FRU Properties** tab) displays.



FRU	Position	Status	Part Number	Serial Number
CTP	0	Active		
Power	0	Active		
Power	1	Active		

Figure 2–6: View Panel (FRU Properties)

b. Inspect the **Status** fields for both power supplies.

Does the **Status** field display a `Failed` message for either power supply?

NO **YES**

↓ A power supply failure is indicated. **Go to** step 50 to obtain event codes. If no event codes are found, go to MAP 0100: Power Distribution Analysis on page 2-27. **Exit MAP.**

49

Inspect the **Status** fields for switch FRUs.

Does the **State** field display a `Failed` message for any of the FRUs?

YES **NO**

↓ The switch appears operational. **Exit MAP.**

A FRU failure is indicated. Continue to the next step to obtain event codes. If no event codes are found, go to MAP 0500: FRU Failure Analysis on page 2-59. **Exit MAP.**

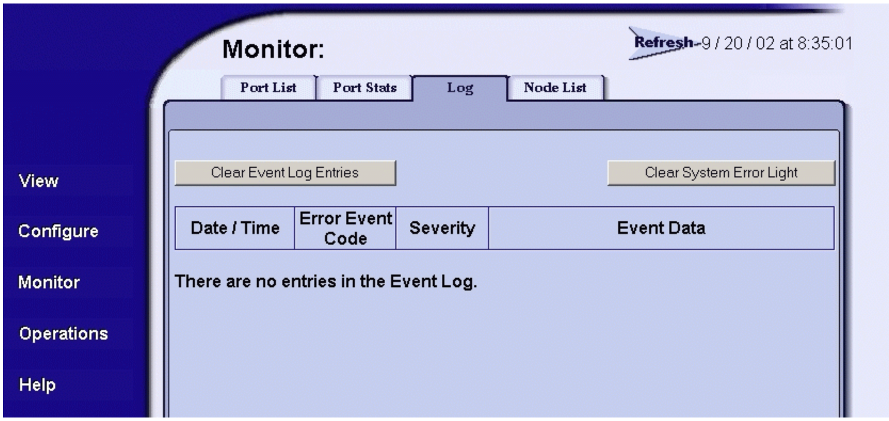
50

Obtain event codes from the EWS **Event Log**.

> If multiple event codes are found, note all codes and associated severity levels. Record the date, time, and listed sequence, and determine if the codes are related to the reported problem. Begin fault isolation with the most recent event code with the highest severity level. Other codes may accompany this event code, or may indicate a normal indication after a problem is recovered.

a. At the **View** panel, select **Monitor** at the left side of the panel. The **Monitor** panel opens with the **Status** page displayed.

b. At the **Monitor** panel, click the **Log** tab. The **Monitor** panel (**Log** tab) displays.



Date / Time	Error Event Code	Severity	Event Data

There are no entries in the Event Log.

Figure 2–7: Monitor Panel (Log)

c. Record the event code, date, time, and severity (**Informational**, **Minor**, **Major**, or **Severe**).

d. Record all event codes that may relate to the reported problem.

Were one or more event codes found?

NO **YES**

↓ **Go to** Table 2–3 on page 2-2**.**

Return to the MAP step that sent you here.

51

You are at the console of an open systems interconnection (OSI) server attached to the switch reporting the problem. If an incident occurs on the Fibre Channel link between the switch and server, a link incident record is generated and sent to the server using the reporting procedure defined in T11/99-017v0.

Was a link incident record generated and sent to the switch-attached OSI server?

YES **NO**

↓ Perform switch fault isolation at the HAFM server (or customer-supplied server).
Go to step 3**.**

52

The link incident record provides the attached switch port number(s) and one or more of the following event codes and messages. Record all event codes that may relate to the reported problem.

581 - Link interface incident - implicit incident.

582 - Link interface incident - bit-error threshold exceeded.

583 - Link failure - loss of signal or loss of synchronization.

584 - Link failure - not-operational primitive sequence (NOS) received.

585 - Link failure - primitive sequence timeout.

586 - Link failure - invalid primitive sequence received for the current link state.

Were one or more event codes found?

YES	NO
↓	Perform switch fault isolation at the HAFM server (or customer-supplied server). **Go to** step 3**.**

Go to Table 2–3 on page 2-2 to obtain event codes. **Exit MAP.**

MAP 0100: Power Distribution Analysis

This MAP describes fault isolation for the switch power distribution system, including defective AC power cords or redundant power supplies.

1

Was an event code **200**, **201**, **202**, or **208** observed at the Edge Switch 2/24 **Event Log** (HAFM server) or at the EWS **Event Log**?

YES **NO**

↓ **Go to step 10.**

2

Table 2–4 lists event codes, brief explanations of the codes, and the associated steps that describe fault isolation procedures.

Table 2–4: MAP 100: Event Codes

Event Code	Explanation	Action
200	Power supply AC voltage failure.	Go to step 3.
201	Power supply DC voltage failure.	Go to step 7.
202	Power supply thermal failure.	Go to step 7.
208	Power supply false shutdown.	Go to step 8.

3

A redundant power supply is disconnected from facility power, not properly installed, or has failed.

Verify the power supply is connected to facility power.

a. Ensure the AC power cord associated with the power supply (**PS0** or **PS1**) is connected to the rear of the switch and a facility power receptacle. If not, connect the cord as directed by the customer.

b. Ensure the associated facility circuit breaker is on. If not, ask the customer set the circuit breaker on.

c. Ensure the AC power cord is not damaged. If damaged, replace the cord.

Was a corrective action performed?

YES **NO**

↓ **Go to** step 5**.**

4

Verify redundant power supply operation.

a. Inspect the power supply and ensure all amber LEDs are extinguished.

b. At the **Hardware View**, observe the graphic representing the power supply and ensure a failure symbol (blinking red and yellow diamond) does not appear.

Is a failure indicated?

YES **NO**

↓ The switch appears operational. **Exit MAP.**

5

Ensure the indicated power supply is correctly installed and seated in the switch. If required, partially remove and reseat the power supply.

Was a corrective action performed?

YES **NO**

↓ **Go to** step 7**.**

6

Verify redundant power supply operation.

a. Inspect the power supply and verify all amber LEDs are extinguished.

b. At the **Hardware View**, observe the graphic representing the power supply and ensure a failure symbol (blinking red and yellow diamond) does not appear.

Is a failure indicated?

YES **NO**

↓ The switch appears operational. **Exit MAP.**

7

A redundant power supply failed and must be removed and replaced (See RRP 2: Redundant Power Supply on page 4–5).

- This procedure is concurrent and can be performed while switch power is on.
- Perform the data collection procedure as part of FRU removal and replacement.

Did power supply replacement solve the problem?

NO **YES**

↓ The switch appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

8

Power sense circuitry is defective in the indicated power supply or there is a problem with facility input power.

Have the customer inspect and verify that facility power is within specifications. These specifications are:

- One single-phase connection for each power supply.
- Input power between 90 and 264 VAC, and at least 15 amps.
- Input frequency between 47 and 63 Hz.

Is facility power within specifications?

NO **YES**

↓ **Go to** step 7**.**

Ask the customer to correct the facility power problem. When facility power is corrected, continue to the next step.

9

Verify switch operation:

a. Inspect the switch front bezel and ensure the green power LED illuminates.

b. At the **Hardware View**, observe all graphics representing FRUs and power supplies, and ensure emulated green LEDs illuminate.

Is a failure indicated?

YES **NO**

↓ The switch appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

10

Is fault isolation being performed at the switch?

YES **NO**

↓ Fault isolation is being performed at the HAFM server (or customer-supplied server) or EWS interface. **Go to** step 19**.**

11

Verify the switch is connected to facility power and is powered on.

a. Ensure AC power cords (**PS0** and **PS1**) are connected to the rear of the switch and to facility power receptacles. If not, connect the cords as directed by the customer.

b. Ensure associated facility circuit breakers are on. If not, ask the customer set the circuit breakers on.

c. Ensure the AC power cords are not damaged. If damaged, replace the cords.

Continue.

12

Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES **NO**

↓ **Go to** step 14**.**

13

Does inspection of a power supply indicate a failure (the amber LED is illuminated)?

NO **YES**

↓ A redundant power supply failed. **Go to** step 7**.**

The switch appears operational. **Exit MAP.**

14

The switch AC power distribution system failed. Possible causes include failure of:

- Both power supplies.
- CTP failure.

Does inspection of both power supplies indicate a dual failure one or more amber LEDs illuminated on each power supply?

YES **NO**

↓ One or both power supplies appear operational, but a power distribution failure through the CTP is indicated.
Go to step 18**.**

15

Ensure both power supplies are correctly installed and seated in the switch. If required, partially remove and reseat the power supplies.

Was a corrective action performed?

YES **NO**

↓ **Go to** step 17**.**

16

Verify operation of both power supplies.

a. Inspect the power supplies and ensure all amber LEDs are extinguished.

b. At the **Hardware View**, observe the graphics representing the power supplies and ensure failure symbols (blinking red and yellow diamonds) do not appear.

Is a dual power supply failure still indicated?

YES **NO**

↓ The switch appears operational. **Exit MAP.**

17

Both power supplies failed and must be removed and replaced. (See RRP 2: Redundant Power Supply on page 4–5.) Perform the data collection procedure as part of FRU removal and replacement.

Did dual power supply replacement solve the problem?

NO **YES**

↓ The switch appears operational. **Exit MAP.**

A dual power supply failure is not confirmed. Replace both original power supplies to avoid the cost of expending replacement FRUs. **Continue.**

18

One or both power supplies appear operational, but logic cards are not receiving dc power. In-card circuit breakers for all logic cards may have tripped due to a power surge, or the CTP failed.

Power cycle the switch to reset all logic cards (Power-On Procedure on page 3–28).

Did power cycling the switch solve the problem?

NO **YES**

↓ The switch appears operational. **Exit MAP.**

19

Is fault isolation being performed at the HAFM server (or customer-supplied server)?

YES **NO**

↓ Fault isolation is being performed at the EWS interface. **Go to** step 23**.**

20

At the **Hardware View**, does a yellow triangle appear at the alert panel and a blinking red and yellow diamond (failed FRU indicator) appear to overlay a power supply graphic?

NO **YES**

↓ A redundant power supply failed. **Go to** step 7**.**

21

At the **Hardware View**, does a grey square appear at the alert panel, a **No Link** status appear at the **Edge-24 Status** table, and graphical FRUs appear uninstalled?

YES **NO**

↓ A green circle appears at the alert panel and the switch appears operational. **Exit MAP.**

The grey square indicates the HAFM server (or customer-supplied server) cannot communicate with the switch because:

- The switch-to-server Ethernet link failed.
- AC power distribution in the switch failed, or AC power was disconnected.
- The switch CTP failed.

Continue.

22

Ensure the switch reporting the problem is connected to facility AC power. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES **NO**

↓ **Go to** step 14**.**

Analysis for an Ethernet link or a CTP failure is not described in this MAP. Go to MAP 0000: Start MAP on page 2-6. If this is the second time at this step, contact the next level of support. **Exit MAP.**

23

Does the EWS interface appear operational?

NO **YES**

↓ **Go to** step 26**.**

24

A `Page cannot be found, Unable to locate the server, HTTP 404 - file not found`, or other similar message appears. The message indicates the web browser PC cannot communicate with the switch because:

- The switch-to-PC Internet link could not be established.
- AC power distribution in the switch failed, or AC power was disconnected.
- The switch CTP failed.

Continue.

25

Ensure the switch reporting the problem is connected to facility AC power. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES **NO**

↓ **Go to** step 14**.**

Analysis for an Ethernet link or a CTP failure is not described in this MAP. Go to MAP 0000: Start MAP on page 2-6. If this is the second time at this step, contact the next level of support. **Exit MAP.**

26

Inspect power supply operational states at the EWS interface.

a. At the **View** panel, click the **FRU Properties** tab. The **View** panel (**FRU Properties** tab) displays.

b. Inspect the **Status** fields for both power supplies.

Does the **Status** field display a **Failed** message for either power supply?

NO **YES**

↓ A redundant power supply failed. **Go to** step 7**.**

The switch appears operational. **Exit MAP.**

MAP 0200: POST Failure Analysis

When the switch is powered on, it performs a series of power-on self-tests (POSTs). When POSTs complete, the switch performs an initial program load (IPL) that loads firmware and brings the unit online. This MAP describes fault isolation for problems that may occur during the POST/IPL process.

If an error is detected, the POST/IPL process continues in an attempt to initialize the switch and bring it online. An event code **400** is displayed when the switch completes the POST/IPL process.

1

Ensure the switch reporting the problem is connected to facility AC power. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES **NO**

↓ An AC power distribution problem is indicated, and analysis for the failure is not described in this MAP. Go to MAP 0100: Power Distribution Analysis on page 2-27. **Exit MAP.**

2

Was an event code **400**, or **411**, or **413** observed at the Edge Switch 2/24 **Event Log** or at the EWS **Event Log**?

YES **NO**

↓ Analysis for the failure is not described in this MAP. Go to MAP 0000: Start MAP on page 2–6. **Exit MAP.**

3

Table 2–5 lists event codes, brief explanations of the codes, and the associated steps that describe fault isolation procedures.

Table 2–5: MAP 200: Event Codes

Event Code	Explanation	Action
400	Power-up diagnostic failure.	Go to step 4.
411	Firmware fault.	Go to step 7.

4

POST/IPL diagnostics detected a FRU failure as indicated by an event code **400** with supplementary event data.

a. At the **Hardware View**, click **Logs** and select **Event Log**. The **Event Log** displays.

b. Examine the first two bytes (**0** and **1**) of event data.

c. Byte **0** is a FRU code that indicates the failed component. Byte **1** is the slot number of the failed FRU (**00** for a nonredundant FRU, and **00** or **01** for redundant FRUs.

Table 2–6 lists byte **0** FRU codes and associated steps that describe fault isolation procedures.

Table 2–6: MAP 200: Byte 0 FRU Codes

Byte 0	Failed FRU	Action
02	CTP.	Go to step 6.
05	Fan module.	Go to step 5.
06	Power supply.	Go to step 6.

5

A fan module failed POSTs (indicated by a **05** FRU code) and the power supply must be removed and replaced (See RRP 2: Redundant Power Supply on page 4–5).

- This procedure is concurrent and can be performed while switch power is on.
- Perform the data collection procedure as part of FRU removal and replacement.

Did fan module/power supply replacement solve the problem?

NO **YES**

↓ The switch appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

6

A power supply failed POSTs (indicated by a **06** FRU code) and must be removed and replaced (See RRP 2: Redundant Power Supply on page 4–5).

- This procedure is concurrent and can be performed while switch power is on.
- Perform the data collection procedure as part of FRU removal and replacement.

Did power supply replacement solve the problem?

NO **YES**

↓ The switch appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

7

POST/IPL diagnostics detected a firmware failure (as indicated by an event code **411**) and performed an online dump. All Fibre Channel ports reset after the failure and devices momentarily logout, login, and resume operation.

Perform the data collection procedure and return the Zip disk to HP for analysis. **Exit MAP.**

MAP 0300: Console Application Problem Determination

This map describes isolation of HAFM server (or customer-supplied server) application problems, including problems associated with the Windows NT operating system, HAFM, and Edge Switch 2/24 Product Manager applications.

1

Did the HAFM server (or customer-supplied server) lock up or crash without displaying a warning or error message?

YES	NO
↓	**Go to step 4.**

2

An application or operating system problem is indicated. Close the HAFM application.

a. Simultaneously press **Ctrl**, **Alt**, and **Delete**. The **Windows Security** dialog box displays.

b. At the **Windows Security** dialog box, click **Task Manager**. The **Windows Task Manager** dialog box displays with the **Applications** page open.

c. Select (highlight) the HP StorageWorks HA-Fabric Manager (HAFM) application and click **End Task**. The HAFM application closes.

Continue.

3

Attempt to clear the problem by rebooting the HAFM server (or customer-supplied server) PC.

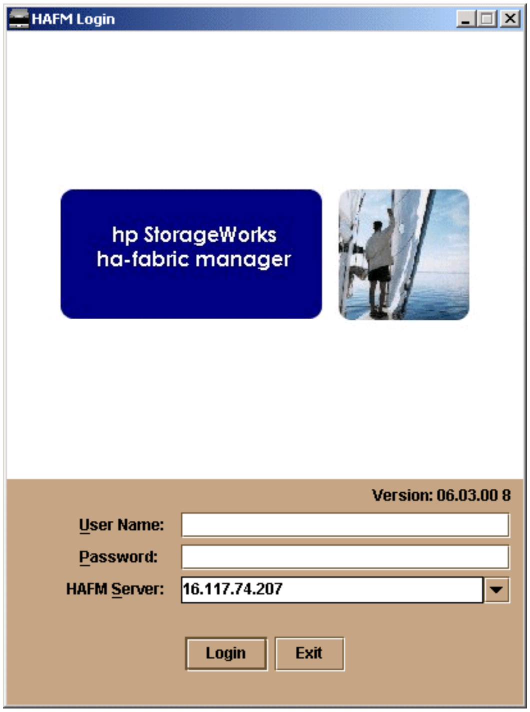
a. Click the Windows **Start** button. The **Windows Workstation** menu displays.

b. At the **Windows Workstation** menu, select **Shut Down**. The **Shut Down Windows** dialog box displays.

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

d. Wait approximately 30 seconds and power on the PC. After POSTs complete, the **Begin Logon** dialog box displays.

e. Simultaneously press **Ctrl**, **Alt**, and **Delete** to display the **Logon Information** dialog box. Type a user name and password (obtained in MAP 0000: Start MAP on page 2-6) and click **OK**. The HAFM application starts and the **HAFM Login** dialog box displays (Table 2–8).



Version: 06.03.00 8

HAFM Server: 16.117.74.207

Figure 2–8: HAFM Login Dialog Box

f. At the **HAFM Login** dialog box, type a user name, password, and HAFM server name (obtained in MAP 0000: Start MAP on page 2-6, and all are case sensitive), and click **Login**. The application opens and the **Products View** displays.

Did the **Products View** display and does the HAFM application appear operational?

NO **YES**

↓ The problem is transient and the HAFM server (or customer-supplied server) appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

4

Did the HAFM application display a dialog box with the message **Connection to HAFM server lost - click OK to exit application** or **HAFM error *n*** (where ***n*** is an error message number **1** through **8** inclusive)?

NO **YES**

↓ An HAFM application error occurred. Click **OK** to close the window and close the HAFM application. **Go to** step 3**.**

5

Did the HAFM application display a window with the message `The software version on this HAFM server is not compatible with the version on the remote HAFM server`?

YES **NO**

↓ **Go to** step 8**.**

6

The HAFM applications running on the HAFM server and client workstation are not at compatible release levels. Recommend to the customer that the downlevel version be upgraded.

Does the customer want the HAFM application upgraded?

YES **NO**

↓ Power off the client workstation. **Exit MAP.**

7

Upgrade the downlevel HAFM application (Install or Upgrade Software on page 3–42).

Did the software upgrade solve the problem?

NO **YES**

↓ The HAFM server (or customer-supplied server) appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

8

Did the Product Manager application display a window with the message `Product Manager error 5001` or `Product Manager error 5002`?

NO **YES**

↓ A Product Manager application error occurred. Click **OK** to close the window and close the HAFM and Product Manager applications. **Go to** step 3**.**

9

Did the Product Manager application display a window with the message **Send firmware failed**?

YES **NO**

↓ **Go to** step 11**.**

10

An attempt to download a firmware version from the HAFM server (or customer-supplied server) hard drive to the switch failed. Retry the operation (Manage Firmware Versions on page 3–32).

Did the firmware version download to the switch?

NO **YES**

↓ The HAFM server (or customer-supplied server) appears operational. **Exit MAP.**

A CTP failure is suspected. Go to MAP 0000: Start MAP on page 2-6 to isolate the problem. **Exit MAP.**

11

Did the Product Manager application display a window with the message `The data collection process failed`?

YES **NO**

↓ **Go to** step 13.

12

The data collection process failed. Retry the process using a new Zip disk (Collecting Maintenance Data on page 3–22).

Did the data collection process complete?

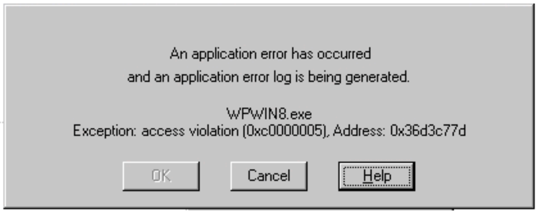
NO **YES**

↓ **Exit MAP.**

Contact the next level of support. **Exit MAP.**

13

Did the HAFM server (or customer-supplied server) lock up or crash and display a **Dr. Watson for Windows** dialog box (Figure 2–9)?



An application error has occurred
and an application error log is being generated.

WPWIN8.exe
Exception: access violation (0xc0000005), Address: 0x36d3c77d

Figure 2–9: Dr. Watson for Windows Dialog Box

NO **YES**

↓ A Windows operating system or HAFM application error occurred. Click **Cancel** to close the window and HAFM application. **Go to** step 3**.**

14

Did the HAFM server (or customer-supplied server) crash and display a blue screen with the system dump file in hexadecimal format (blue screen of death)?

YES **NO**

↓ The HAFM server (or customer-supplied server) appears operational. **Exit MAP.**

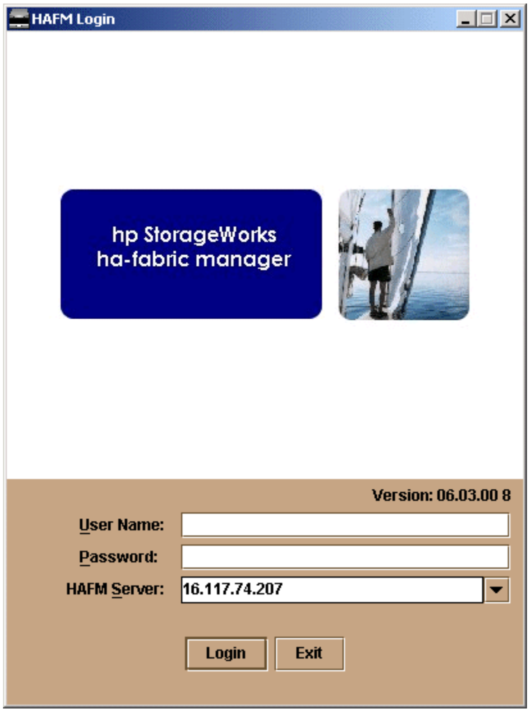
15

Attempt to clear the problem by power cycling the HAFM server (or customer-supplied server) PC.

a. Power off the PC.

b. Wait approximately 30 seconds and power on the PC. After POSTs complete, the **Begin Logon** dialog box displays.

c. Simultaneously press **Ctrl**, **Alt**, and **Delete** to display the **Logon Information** dialog box. Type a user name and password (obtained in MAP 0000: Start MAP on page 2-6) and click **OK**. The HAFM application starts and the **HAFM Login** dialog box displays (Figure 2–10).



Version: 06.03.00 8

User Name:

Password:

HAFM Server: 16.117.74.207

Figure 2–10: HAFM Login Dialog Box

d. At the **HAFM Login** dialog box, type a user name, password, and HAFM server name (obtained in MAP 0000: Start MAP on page 2-6, and all are case sensitive), and click **Login**. The application opens and the **Products View** displays.

Did the **Products View** display and does the HAFM application appear operational?

NO **YES**

↓ The problem is transient and the HAFM server (or customer-supplied server) appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

MAP 0400: Loss of Console Communication

This MAP describes fault isolation of the Ethernet communication link between a switch and the HAFM server (or customer-supplied server), or between a switch and a web browser PC running the EWS interface. Failure indicators include:

- At the **Products View**, a grey square at the alert panel and as the background to the icon representing the switch reporting the problem.
- At the **Hardware View**, a grey square at the alert panel, a **No Link** status and reason at the **Edge-24 Status** table, and no FRUs visible for the switch.
- At the web browser PC, A `Page cannot be found, Unable to locate the server, HTTP 404 - file not found`, or other similar message.
- Event codes recorded at the Edge Switch 2/24 **Event Log** or EWS **Event Log**.

When the logical connection between the switch and HAFM server (or customer-supplied server) is initiated, it may take up to five minutes for the link to activate at the **Products View**, and a green circle to appear at the alert panel and the background to the icon representing the switch. This delay is normal.

CAUTION: Prior to servicing a switch or HAFM server (or customer-supplied server), determine the Ethernet LAN configuration. Installation of switches and the server on a public customer intranet can complicate problem determination and fault isolation.

1

Was an event code **430**, **431**, or **432** observed at the Edge Switch 2/24 **Event Log** or at the EWS **Event Log**?

YES **NO**

↓ **Go to** step 3**.**

2

Table 2–7 lists event codes, brief explanations of the codes, and associated steps that describe fault isolation procedures.

Table 2–7: MAP 400: Event Codes

Event Code	Explanation	Action
430	Excessive Ethernet transmit errors.	Go to step 8.
431	Excessive Ethernet receive errors.	Go to step 8.
432	Ethernet adapter reset.	Go to step 14.

3

Is fault isolation being performed at the HAFM server (or customer-supplied server)?

YES **NO**

↓ Fault isolation is being performed through the EWS interface. **Go to** step 25**.**

4

At the **Products View**, does a grey square appear at the alert panel and as the background to the icon representing the switch reporting the problem?

YES **NO**

↓ The switch-to-server connection is restored and appears operational. **Exit MAP.**

The grey square indicates the HAFM server (or customer-supplied server) cannot communicate with the switch because:

- The switch-to-server Ethernet link failed.
- AC power distribution in the switch failed, or AC power was disconnected.
- The switch CTP failed.

Continue.

5

Ensure the switch reporting the problem is connected to facility AC power. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES	NO
↓	A power distribution problem is indicated. Go to MAP 0100: Power Distribution Analysis on page 2-27. **Exit MAP.**

6

At the switch, inspect the amber for the switch.

Is the amber LED illuminated?

NO	YES
↓	Failure of the CTP is indicated. Go to MAP 0500: FRU Failure Analysis on page 2-59. **Exit MAP.**

7

The switch-to-server Ethernet link failed. Double-click the icon with the grey square representing the switch reporting the problem. The **Hardware View** displays. At the **Hardware View**:

- A grey square appears at the alert panel.
- No FRUs are visible for the switch.
- The **Edge-24 Status** table is yellow, the **Status** field displays `No Link`, and the **Reason** field displays an error message.

Table 2–8 lists the error messages and associated steps that describe fault isolation procedures.

Table 2–8: MAP 400: Error Messages

Error Message	Action
Never connected.	Go to step 8.
Link timeout.	Go to step 8.
Protocol mismatch.	Go to step 15.

Table 2–8: MAP 400: Error Messages (Continued)

Error Message	Action
Duplicate session.	Go to step 18.
Unknown network address.	Go to step 21.
Incorrect product type.	Go to step 23.

8

Transmit or receive errors for a switch's Ethernet adapter exceeded a threshold, the switch-to-server link was not connected, or the switch-to-server link timed out. A problem with the Ethernet cable, Ethernet hub or hubs, or other LAN-attached device is indicated.

Verify the switch is connected to the HAFM server (or customer-supplied server) through one or more Ethernet hubs.

a. Ensure an RJ-45 Ethernet cable connects the switch to an Ethernet hub. If not, connect the cables as directed by the customer.

b. Ensure an RJ-45 Ethernet cable connects the HAFM server adapter card to an Ethernet hub. If not, connect the cable as directed by the customer.

c. Ensure the Ethernet cables are not damaged. If damaged, replace the cables.

Was a corrective action performed?

NO **YES**

↓ **Go to step 1.**

9

Does the LAN configuration use multiple (up to four) Ethernet hubs that are daisy-chained?

YES **NO**

↓ **Go to step 11.**

10

Verify the hubs are correctly daisy-chained (Figure 2–11.)

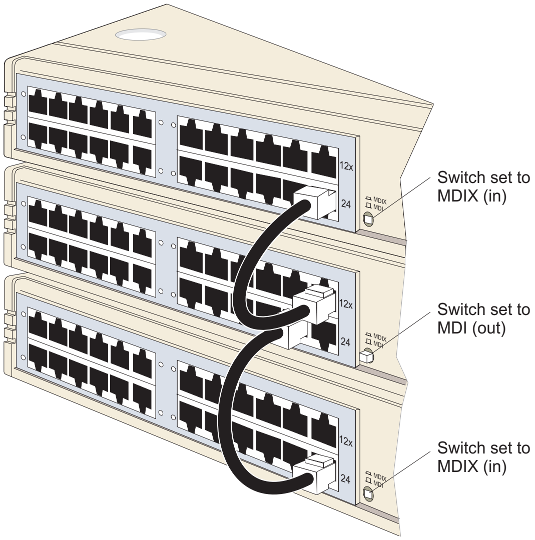


Figure 2–11: Ethernet Hubs, daisy-chained

To check two hubs, use step a and step b (top and middle hub instructions only).

a. At the first (top) Ethernet hub, ensure an RJ-45 Ethernet patch cable connects to port **24** and the medium-dependent interface (MDI) switch is set to **MDIX** (in).

b. At the middle Ethernet hub, ensure the patch cable from the top hub connects to port **12x,** the patch cable from the bottom hub connects to port **23x**, and the MDI switch is set to **MDI** (out).

c. At the bottom Ethernet hub, ensure the patch cable from the middle hub connects to port **24** and the MDI switch is set to **MDIX** (in).

Was a corrective action performed?

NO	YES
↓	**Go to step 1.**

11

Verify operation of the Ethernet hub or hubs. Inspect each hub for indications of being powered on, such as:

- Green **Power** LED illuminated.
- Green **Status** LEDs illuminated.

Is a hub failure indicated?

YES **NO**

↓ **Go to** step 13**.**

12

Remove and replace the Ethernet hub. Refer to the supporting documentation shipped with the hub for instructions.

Did hub replacement solve the problem?

NO **YES**

↓ The switch-to-server connection is restored and appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

13

A problem with another LAN-attached device is indicated.

- If the problem is associated with another switch or HAFM server (or customer-supplied server), go to MAP 0000: Start MAP on page 2-6 to isolate the problem for that device. **Exit MAP.**
- If the problem is associated with an unrelated device, notify the customer and have the system administrator correct the problem.

Did repair of an unrelated LAN-attached device solve the problem?

NO **YES**

↓ The switch-to-server connection is restored and appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

14

The Ethernet adapter on the switch CTP reset in response to an error. The connection to the HAFM server (or customer-supplied server) terminated briefly, then recovered upon reset.

Perform the data collection procedure and return the Zip disk to HP for analysis. **Exit MAP.**

15

A protocol mismatch occurred because the HAFM application and the switch firmware are not at compatible release levels. Recommend to the customer that the downlevel version (software or firmware) be upgraded.

Does the HAFM application require upgrade?

YES **NO**

↓ **Go to** step 17**.**

16

Upgrade the HAFM application (Install or Upgrade Software on page 3–42).

Did the switch-to-server Ethernet connection recover?

NO **YES**

↓ The switch-to-server connection is restored and appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

17

A switch firmware upgrade is required (Manage Firmware Versions on page 3–32). Perform the data collection procedure after the download.

Did the switch-to-server Ethernet connection recover?

NO **YES**

↓ The switch-to-server connection is restored and appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

18

An instance of the HAFM application is open at another HAFM server (or customer-supplied server) and communicating with the switch (duplicate session). Notify the customer and either:

- Power off the HAFM server (or customer-supplied server) running the second instance of the application, or
- Configure the HAFM server (or customer-supplied server) running the second instance of the application as a client workstation.

Does the customer want the second HAFM server (or customer- supplied server) configured as a client?

YES **NO**

↓ Power off the HAFM server (or customer-supplied server) reporting the **Duplicate Session** communication problem. **Exit MAP.**

19

Determine the internet protocol (IP) address of the HAFM server (or customer-supplied server) running the first instance of the HAFM application.

a. Click the Windows **Start** button. The **Windows Workstation** menu displays.

b. At the **Windows Workstation** menu, select **Settings**. From the menu that displays, select **Control Panel**. The **Control Panel** window displays.

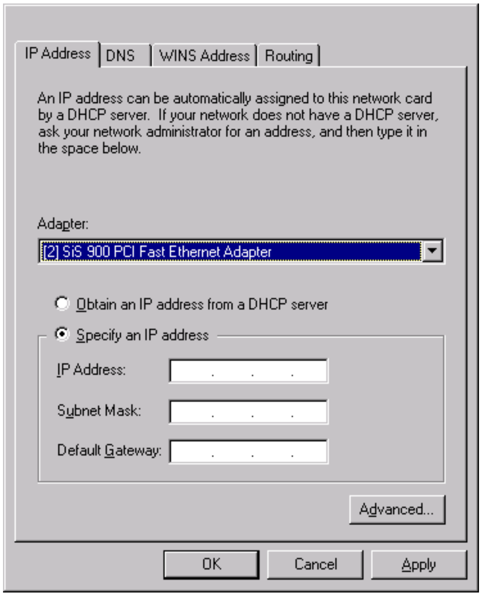
c. At the **Control Panel** window, double-click the **Network** icon. The **Network** dialog box displays with the **Identification** page open.

d. Click the **Protocols** tab. The **Protocols** page opens.

e. Select (highlight) the **TCP/IP Protocol** entry from the list box and click **Properties**. The **Microsoft TCP/IP Properties** dialog box displays (Figure 2–12) with the **IP Address** page open.

f. Record the IP address, then click **OK** to close the dialog box.

g. At the **Network** dialog box, click **OK** to close the dialog box.



An IP address can be automatically assigned to this network card by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.

Adapter:
[2] SiS 900 PCI Fast Ethernet Adapter

○ Obtain an IP address from a DHCP server
● Specify an IP address

IP Address: . . .
Subnet Mask: . . .
Default Gateway: . . .

Figure 2–12: Microsoft TCP/IP Properties Dialog Box

Continue.

20

Configure the HAFM server (or customer-supplied server) reporting the **Duplicate Session** communication problem as a client.

a. At the **Products View**, click **Logout/Exit** and select **Logout**. The **HAFM Login** dialog box displays.

b. At the **HAFM Login** dialog box, type a user name and password (obtained in MAP 0000: Start MAP on page 2-6, and both are case sensitive).

c. Type the IP address of the HAFM server (or customer-supplied server) running the first instance of the HAFM application in the **HAFM server** field.

d. Click **Login**. The HAFM application opens as a client and the **Products View** displays.

Did the HAFM server (or customer-supplied server) reconfigure as a client and did the Ethernet connection recover?

NO **YES**

↓ The switch-to-server connection is restored and the second HAFM server (or customer-supplied server) appears operational as a client. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

21

The IP address defining the switch to the HAFM application is incorrect or unknown and must be verified. A maintenance terminal (PC) and asynchronous RS-232 null modem cable are required to verify the switch IP address. The tools are provided with the switch or by service personnel. To verify the IP address:

a. Remove the protective cap from the 9-pin maintenance port at the rear of the switch (a phillips-tip screwdriver may be required). Connect one end of the RS-232 null modem cable to the port.

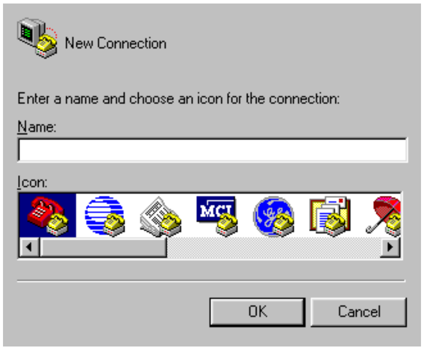
b. Connect the other cable end to a 9-pin communication port (**COM1** or **COM2**) at the rear of the maintenance terminal PC.

c. Power on the maintenance terminal. After the PC powers on, the Windows desktop displays.

d. At the Windows desktop, click the Windows **Start** button. The **Windows Workstation** menu displays.

NOTE: The following steps describe inspecting the IP address using HyperTerminal serial communication software.

e. At the **Windows Workstation** menu, sequentially select **Programs** > **Accessories** > **HyperTerminal**. The **Connection Description** dialog box displays.



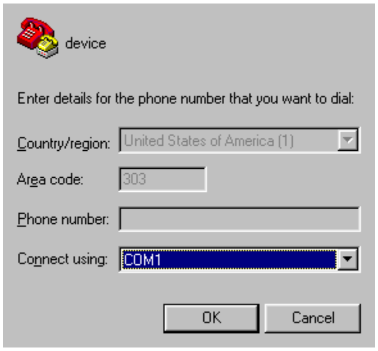
New Connection

Enter a name and choose an icon for the connection:

Name:

Icon:

f. Type Edge-32 in the **Name** field. Click **OK**. The **Connect To** dialog box displays.



device

Enter details for the phone number that you want to dial:

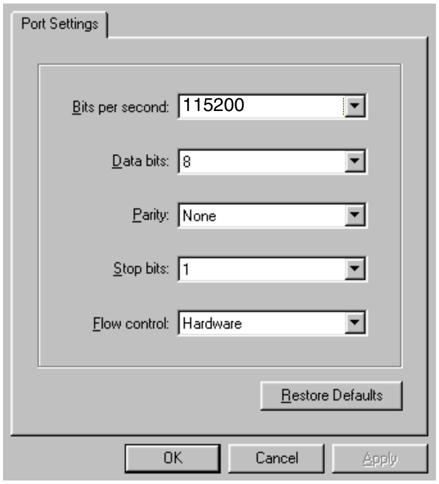
Country/region: United States of America (1)

Area code: 303

Phone number:

Connect using: COM1

g. Ensure the **Connect using** field displays COM1 or COM2 (depending on the serial communication port connection to the switch) and click **OK**. The **COMn** dialog box displays (where n is 1 or 2).



Port Settings

Bits per second: 115200

Data bits: 8

Parity: None

Stop bits: 1

Flow control: Hardware

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

— Bits per second - 115200.

— Data bits - 8.

— Parity - None.

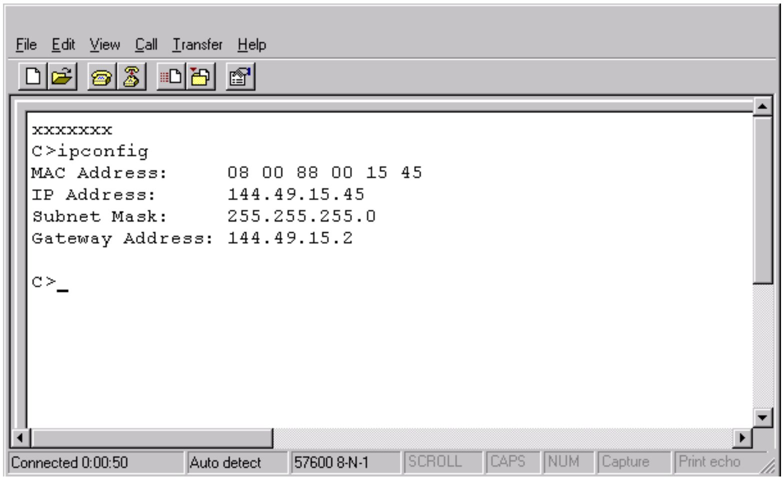
— Stop bits - 1.

— Flow control - Hardware.

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

i. 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 software and hardware version information for the switch, and an `C>` prompt at the bottom of the window.

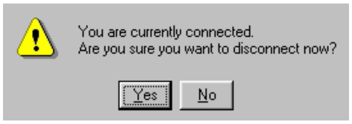
j. At the `C>` prompt, type the `ipconfig` command and press **Enter**. The **HyperTerminal** window displays with configuration information listed (including the IP address).



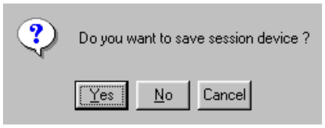
```
xxxxxxx
C>ipconfig
MAC Address:     08 00 88 00 15 45
IP Address:      144.49.15.45
Subnet Mask:     255.255.255.0
Gateway Address: 144.49.15.2

C>_
```

k. Record the switch IP address.

l. Select **Exit** from the **File** pull-down menu to close the HyperTerminal application. The following message box appears:


You are currently connected.
Are you sure you want to disconnect now?

m. Click **Yes**. The following message box appears:


Do you want to save session device ?

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

o. Power off the maintenance terminal.

p. Disconnect the RS-232 modem cable from the switch and the maintenance terminal. Replace the protective cap over the maintenance port.

Continue.

22

Define the switch's correct IP address to the HAFM server (or customer-supplied server).

a. At the **Products View**, right-click the icon with the grey square representing the switch reporting the problem. A pop-up menu displays.

b. Select **Modify**. The **Modify Network Address** dialog box displays (Figure 2–13).

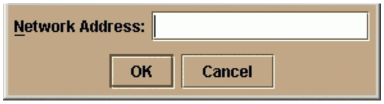


Figure 2–13: Modify Network Address Dialog Box

c. Type the correct IP address and click **OK**.

Did the IP address below the switch icon change to the new entry and did the Ethernet connection recover?

NO **YES**

↓ The switch-to-server connection is restored and appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

23

An incorrect product type is defined to the HAFM server (or customer-supplied server).

a. At the **Products View**, right-click the icon with the grey square representing the product reporting the problem. A pop-up menu displays.

b. Select **Delete**. A Warning dialog box displays asking if the product is to be deleted.

c. Click **Yes** to delete the product.

d. At the **Products View**, click Configure and select **New Product**. The **New Product** dialog box displays.

e. Type the configured IP address in the **Network Address** field.

f. Select Edge Switch 2/24 from the **Product Type** list box and click **OK**.

Did the IP address below the switch icon change to the new entry and did the Ethernet connection recover?

NO **YES**

↓ The switch-to-server connection is restored and appears operational. **Exit MAP.**

24

The product at the configured IP address is not a HP managed product. Notify the customer of the problem.

a. At the **Products View**, right-click the icon with the grey square representing the product reporting the problem. A pop-up menu displays.

b. Select **Delete**. A Warning dialog box displays asking if the product is to be deleted.

c. Click **Yes** to delete the product.

Exit MAP.

25

Does the EWS interface appear operational?

NO **YES**

↓ The switch-to-EWS PC connection is restored and appears operational. **Exit MAP.**

26

A `Page cannot be found, Unable to locate the server, HTTP 404 - file not found`, or other similar message appears. The message indicates the web browser PC cannot communicate with the switch because:

- The switch-to-PC Internet (Ethernet) link could not be established.
- AC power distribution in the switch failed, or AC power was disconnected.
- The switch CTP failed.

Continue.

27

Ensure the switch reporting the problem is connected to facility AC power. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated green power LED or amber system error LED.
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES **NO**

↓ A power distribution problem is indicated. Go to MAP 0100: Power Distribution Analysis on page 2-27. **Exit MAP.**

28

At the switch, inspect the amber LED at the top of the CTP. Is the amber LED illuminated on the switch?

NO **YES**

↓ Failure of the CTP is indicated. Go to MAP 0500: FRU Failure Analysis on page 2-59. **Exit MAP.**

29

Either a switch-to-PC Internet link problem (Internet too busy or IP address typed incorrectly) or a switch Ethernet port failure is indicated.

a. Wait approximately five minutes, then attempt to login to the switch again.

b. At the **Netsite** field (Netscape Navigator) or **Address** field (Internet Explorer), type `http://xxx.xxx.xxx.xxx`, where *`xxx.xxx.xxx.xxx`* is the IP address of the switch (obtained in MAP 0000: Start MAP on page 2-6). The **Username and Password Required** dialog box appears.

c. Type the user name and password obtained in MAP 0000: Start MAP on page 2-6, and click **OK**. If the **View** panel does not display, wait five minutes and perform this step again.

Does the EWS interface appear operational with the **View** panel displayed?

NO **YES**

↓ The switch-to-EWS PC connection is restored and appears operational. **Exit MAP.**

Failure of the switch Ethernet port is indicated. Go to MAP 0500: FRU Failure Analysis on page 2-59. **Exit MAP.**

MAP 0500: FRU Failure Analysis

This MAP describes fault isolation for the switch and FRUs. Failure indicators include:

- The amber LED on the FRU illuminates.
- The amber emulated LED on a power supply at the **Hardware View** illuminates.
- A blinking red and yellow diamond (failed FRU indicator) appears over a FRU graphic; or a grey square (status unknown indicator) or yellow triangle (attention indicator) appears at the alert panel of the **Products View** or **Hardware View**.
- An event code recorded at the Edge Switch 2/24 **Event Log** or the EWS **Event Log**.
- A `Failed` message associated with a FRU at the EWS interface.

1

Was an event code **300**, **301**, **302**, **303**, **304**, **305**, **433**, **440**, **810**, or **811** observed at the Edge Switch 2/24 **Event Log** or at the EWS **Event Log**?

YES **NO**

↓ **Go to** step 3**.**

2

Table 2–9 lists event codes, brief explanations of the codes, and associated steps that describe fault isolation procedures.

Table 2–9: MAP 500: Event Codes

Event Code	Explanation	Action
300	Cooling fan propeller failed.	Go to step 5.
301	Cooling fan propeller failed.	Go to step 5.
302	Cooling fan propeller failed.	Go to step 5.
303	Cooling fan propeller failed.	Go to step 5.
304	Cooling fan propeller failed.	Go to step 5.
305	Cooling fan propeller failed.	Go to step 5.
433	Non-recoverable Ethernet fault.	Go to step 7.
440	Embedded port hardware failed.	Go to step 7.

Table 2–9: MAP 500: Event Codes (Continued)

Event Code	Explanation	Action
810	High temperature warning (CTP thermal sensor).	Go to step 7.
811	Critically hot temperature warning (CTP thermal sensor).	Go to step 7.

3

Is fault isolation being performed at the switch?

YES **NO**

↓ Fault isolation is being performed at the HAFM server (or customer-supplied server) or EWS interface.
Go to step 7**.**

4

Inspect both power supplies at the rear of the switch. Does inspection of switch fan module/power supply indicate a failure? Indicators include:

- The amber LED is illuminated on one or both power supplies.
- One or more cooling fans are not rotating.

YES **NO**

↓ **Go to** step 6**.**

5

One or more cooling fans failed, and one or both power supplies must be removed and replaced (See RRP 2: Redundant Power Supply on page 4–5).

- If one or more fans in a module are operating, do not remove the power supply unless the replacement is immediately available.
- If a multiple fan failure caused a thermal shutdown, power on the switch after the power supply(s) are replaced (Power-On Procedure on page 3–28).

Do the fan module(s) appear to function?

NO **YES**

↓ The switch appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

6

Inspect the front of the switch.

Is the amber LED illuminated but not blinking (beaconing)?

YES **NO**

↓ **Go to** step 7**.**

Contact the next level of support. **Exit MAP.**

7

Is fault isolation being performed at the HAFM server (or customer-supplied server)?

YES **NO**

↓ Fault isolation is being performed at the EWS interface. **Go to** step 11**.**

8

Does a blinking red and yellow diamond (failed FRU indicator) appear to overlay a fan module/power supply graphic at the **Hardware View**?

NO **YES**

↓ A fan module failure is indicated. **Go to** step 5**.**

9

At the **Hardware View**, does a grey square appear at the alert panel, a **No Link** status appear at the **Edge-24 Status** table, and graphical FRUs appear uninstalled?

YES **NO**

↓ A green circle appears at the alert panel and the switch appears operational. **Exit MAP.**

The grey square indicates the HAFM server (or customer-supplied server) cannot communicate with the switch because:

- The switch-to-server Ethernet link failed.
- AC power distribution in the switch failed, or AC power was disconnected.
- The switch CTP failed.

Continue.

10

At the switch, inspect the amber LED. Is the amber LED illuminated?

NO **YES**

↓ A CTP card failure is indicated. Replace the switch.
Exit MAP.

Analysis for an Ethernet link or AC power distribution failure is not described in this MAP. Go to MAP 0000: Start MAP on page 2-6. If this is the second time at this step, contact the next level of support. **Exit MAP.**

11

Does the EWS interface appear operational?

NO **YES**

↓ **Go to** step 15**.**

12

A `Page cannot be found, Unable to locate the server, HTTP 404 - file not found`, or other similar message appears. The message indicates the web browser PC cannot communicate with the switch because:

- The switch-to-PC Internet link could not be established.
- AC power distribution in the switch failed, or AC power was disconnected.
- The switch CTP failed.

Continue.

13

Ensure the switch reporting the problem is connected to facility AC power. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated green power LED or amber system error LED.
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES **NO**

↓ Analysis for an AC power distribution failure is not described in this MAP. Go to MAP 0000: Start MAP on page 2-6. If this is the second time at this step, contact the next level of support. **Exit MAP.**

14

At the switch, inspect the amber LED.

Is the amber LED illuminated?

NO **YES**

↓ A CTP card failure is indicated. Replace the switch.
Exit MAP.

Analysis for an Ethernet link failure is not described in this MAP. Go to MAP 0000: Start MAP on page 2-6. If this is the second time at this step, contact the next level of support. **Exit MAP.**

15

Inspect fan module operational states at the EWS interface.

a. At the **View** panel, click the **FRU Properties** tab. The **View** panel (**FRU Properties** tab) displays.

b. Inspect the **Status** fields for both power supplies.

Does the **Status** field display a `Failed` message for either fan module?

NO **YES**

↓ A fan module failure is indicated. **Go to** step 5**.**

16

Inspect switch CTP operational states at the EWS interface. Inspect the **Status** fields for the switch CTP.

Does the **Status** field display a `Failed` message for the CTP?

NO **YES**

↓ A CTP card failure is indicated. Replace the switch.
Exit MAP.

Additional analysis is not described in this MAP. Go to MAP 0000: Start MAP on page 2-6. If this is the second time at this step, contact the next level of support. **Exit MAP.**

MAP 0600: Port Failure and Link Incident Analysis

This MAP describes fault isolation shortwave laser small form factor pluggable (SFP) optical transceivers, and longwave laser SFP optical transceivers; and for Fibre Channel link incidents. Failure indicators include:

- One or more amber LEDs on the ports illuminate.
- One or more emulated amber LEDs on a port graphic at the **Hardware View** illuminate.
- A blinking red and yellow diamond (failed FRU indicator) appears over a port graphic or a yellow triangle (attention indicator) appears at the alert panel of the **Products View** or **Hardware View**.
- An event code recorded at the **Event Log** or the EWS **Event Log**.
- A port operational state message or a `Failed` message associated with a port at the EWS interface.
- A link incident message recorded in the **Link Incident Log** or **Port Properties** dialog box.
- A link incident event code recorded at the console of an OSI server attached to the switch reporting the problem.

1

Was an event code **080, 081, 504**, **505**, **506**, **507**, **512**, **514**, or **802** observed at the HAFM **Event Log** or at the EWS **Event Log**?

NO **YES**

↓ **Go to** step 3**.**

2

Was an event code **581**, **582**, **583**, **584**, **585**, or **586** observed at the console of an OSI server attached to the switch reporting the problem?

YES **NO**

↓ **Go to** step 4**.**

3

Table 2–10 lists event codes, brief explanations of the codes, and associated steps that describe fault isolation procedures.

Table 2–10: MAP 600: Event Codes

Event Code	Explanation	Action
080	Unauthorized worldwide name.	Go to step 21.
081	Invalid attachment.	Go to step 16.
506	Fibre Channel port failure.	Go to step 6.
507	Loopback diagnostics port failure.	Go to step 13.
512	SFP optical transceiver nonfatal error.	Go to step 6.
514	SFP optical transceiver failure.	Go to step 6.
581	Implicit incident.	Go to step 25.
582	Bit error threshold exceeded.	Go to step 25.
583	Loss of signal or loss of synchronization.	Go to step 25.
584	Not operational primitive sequence received.	Go to step 25.
585	Primitive sequence timeout.	Go to step 25.
586	Invalid primitive sequence received for current link state.	Go to step 25.

4

Is fault isolation being performed at the switch?

YES **NO**

↓ Fault isolation is being performed at the HAFM server (or customer-supplied server) or EWS interface.
Go to step 7**.**

5

Each port has an amber and green LEDs next to the ports. The amber LED illuminates and the green LED extinguishes if the port fails.

Are an amber port LED and the amber LED illuminated but not blinking (beaconing)?

YES **NO**

↓ The switch appears operational, however a link incident or other problem may have occurred. Perform fault isolation at the HAFM server (or customer-supplied server). **Go to** step 12**.**

6

A Fibre Channel port failed, and the SFP optical transceiver must be removed and replaced (RRP 1: SFP Optical Transceiver on page 4–2).

- This procedure is concurrent and can be performed while switch power is on.
- Verify location of the failed port.
- Replace the optical transceiver with a transceiver of the same type (shortwave or longwave).
- Perform an external loopback test for the port as part of FRU removal and replacement.

Did optical transceiver replacement solve the problem?

NO **YES**

↓ The switch appears operational. **Exit MAP.**

7

Is fault isolation being performed at the HAFM server (or customer- supplied server)?

YES **NO**

↓ Fault isolation is being performed at the EWS interface. **Go to** step 32**.**

8

Does a blinking red and yellow diamond (failed FRU indicator) appear adjacent to a Fibre Channel port graphic at the **Hardware View**?

NO **YES**

↓ A port failure is indicated. **Go to** step 6**.**

9

Did a Fibre Channel port fail a loopback test?

NO **YES**

↓ **Go to step 13.**

10

Does a yellow triangle (attention indicator) appear adjacent to a port graphic at the **Hardware View**?

YES **NO**

↓ **Go to step 12.**

11

Inspect the port state and LED status for all ports with an attention indicator.

a. At the **Hardware View**, double-click the port graphic with the attention indicator. The **Port Properties** dialog box displays.

b. Inspect the **Operational State** field at the **Port Properties** dialog box, and the emulated green and amber LEDs adjacent to the port at the **Hardware View**.

c. Table 2–11 lists LED and port operational state combinations and associated MAP 0600 (or other) steps that describe fault isolation procedures.

Table 2–11: Port Operational and LED States

Operational State	Green LED	Amber LED	Action
Offline	Off	Off	Go to step 14.
Not Operational	Off	Off	Go to step 14.
Testing	Off	Blinking	Internal loopback test in process. **Exit MAP.**
Testing	On	Blinking	External loopback test in process. **Exit MAP.**
Beaconing	Off or On	Blinking	Go to step 15.
Invalid Attachment	On	Off	Go to step 16.
Link Reset	Off	Off	Go to step 24.

Table 2–11: Port Operational and LED States (Continued)

Operational State	Green LED	Amber LED	Action
Link Incident	Off	Off	Go to step 25.
Segmented E_Port	On	Off	Go to MAP 0700.

12

A link incident may have occurred, but the LIN alerts option is not enabled for the port and the attention indicator does not appear.

At the **Hardware View**, click **Logs** and select **Link Incident Log**. The **Link Incident Log** displays. If a link incident occurred, the affected port number is listed with one of the following messages.

```
Link interface incident - implicit incident.

Link interface incident - bit-error threshold exceeded.

Link failure - loss of signal or loss of synchronization.

Link failure - not-operational primitive sequence (NOS)
received.

Link failure - primitive sequence timeout.

Link failure - invalid primitive sequence received for the
current link state.
```

Did one of the listed messages appear in the **Link Incident Log**?

YES **NO**

↓ The switch appears operational. **Exit MAP.**

Go to step 25**.**

13

A Fibre Channel port failed an internal or external loopback test.

a. Reset each port that failed the loopback test.

   1. At the **Hardware View**, right-click the port. A pop-up menu appears.
   2. Select **Reset Port**. A **Reset Port *n*** message box displays, where ***n*** is the port number.
   3. Click **OK**. The port resets.

b. Perform an external loopback test for all ports that were reset.

Did resetting ports solve the problem?

NO   **YES**

↓   The switch appears operational. **Exit MAP.**

14

A switch port is unblocked and receiving the offline sequence (OLS) or not operational sequence (NOS) from an attached device.

Inform the customer that the attached device failed or is set offline. **Exit MAP.**

15

Beaconing is enabled for the port.

a. Consult the customer and next level of support to determine the reason port beaconing is enabled.

b. Disable port beaconing.

   1. At the **Hardware View**, right-click the port graphic. A pop-up menu appears.
   2. Click the **Enable Beaconing** option. The check mark disappears from the box adjacent to the option, and port beaconing is disabled.

Was port beaconing enabled because port failure or degradation was suspected?

YES   **NO**

↓   The switch appears operational. **Exit MAP.**

Go to step 1**.**

16

The port has an invalid attachment. The information in the **Port Properties** dialog box specifies the reason (Table 2–12).

Table 2–12: Port Properties, Invalid Attachment Reasons and Actions

Reason	Action
Unknown	Contact the next level of support.
ISL connection not allowed on this port.	Go to step 17.
Incompatible switch at other end of ISL.	Go to step 18.
External loopback adapter connected to the port.	Go to step 19.
N-Port connection not allowed on this port.	Go to step 17.
Non-HP switch at other end of the ISL.	Go to step 18.
Port binding violation - Unauthorized WWN.	Go to step 21.
Unresponsive node connected to port.	Go to step 22.

17

The port connection conflicts with the configured port type. Either an expansion port (E_Port) is incorrectly cabled to a Fibre Channel device or a fabric port (F_Port) is incorrectly cabled to a fabric element (switch or switch).

a. At the HAFM server's **Hardware View** for the selected switch, click **Configure** and select **Ports**. The **Configure Ports** dialog box displays.

b. Use the vertical scroll bar as necessary to display the information row for the port indicating an invalid attachment.

c. Select (click) the **Type** field and configure the port from the list box as follows:

- Select fabric port (**F_Port**) if the port is cabled to a device (node).
- Select expansion port (**E_Port**) if the port is cabled to a fabric element (switch or switch) to form an ISL.

d. Click **Activate** to save the configuration information and close the window.

Did reconfiguring the port type solve the problem?

NO **YES**

↓ The switch appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

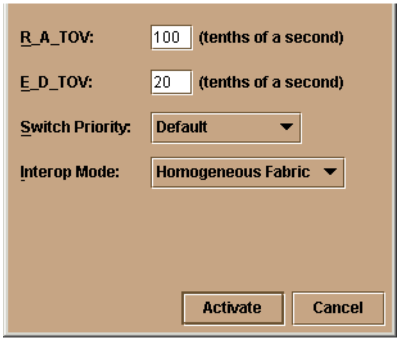
18

The switch is configured for Open Fabric mode but the switch or switch at the other end of the ISL is not configured to Open Fabric mode, or switch is connected to a non-HP switch and the interop mode is set to homogeneous fabric mode.

Configure the switch operating mode:

a. Ensure the switch is set offline (Set the Switch Online or Offline on page 3–23).

b. At the **Hardware View** for the selected switch, click **Configure** and select **Fabric Parameters**. The **Configure Fabric Parameters** dialog box displays (Figure 2–14).



R_A_TOV: 100 (tenths of a second)

E_D_TOV: 20 (tenths of a second)

Switch Priority: Default

Interop Mode: Homogeneous Fabric

Figure 2–14: Configure Fabric Parameters Dialog Box

c. Select the operating mode as follows:

- Select the **Interop Mode** radio button to set the switch to open systems operating mode, then select **Homogeneous Fabric 1.0** or **Open Fabric 1.0** from the **Interop Mode** list box.
- Select the homogeneous fabric option if the switch is fabric- attached **only** to other HP switches or switches that are also operating in Homogeneous Fabric 1.0 mode. Select the open fabric option if the switch is fabric-attached to switches or switches produced by other original equipment manufacturers (OEMs) that are open-fabric compliant.

d. Click **Activate** to save the selection and close the window.

Did configuring the operating mode solve the problem?

NO **YES**

↓ The switch appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

19

A loopback (wrap) plug is connected to the port and there is no diagnostic test running. Is a loopback plug in the port receptacle?

YES **NO**

↓ Contact the next level of support. **Exit MAP.**

20

Remove the loopback plug from the port receptacle. If directed by the customer, connect a fiber-optic jumper cable attaching a device to the switch.

- If the port is operational and a device is not attached, both LEDs adjacent to the port extinguish and the port state is **No Light**.
- If the port is operational and a device is attached, the green LED illuminates, the amber LED extinguishes, and the port state is **Online**.

Did removing the loopback plug solve the problem?

NO **YES**

↓ The switch appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

21

The WWN entered to configure port binding for this port is not valid or a nickname was used that was not configured for the attached device in the Product Manager.

From the **Hardware View, c**lick **Node List**. Note the **Port WWN** column. This is the eight-byte (16-digit) worldwide name (WWN) assigned to the port or Fibre Channel interface installed on the attached device.

- If nickname is not assigned to the WWN, the WWN is prefixed by the device manufacturer's name.
- If a nickname is assigned to the WWN, it appears in place of the WWN.

The Bound WWN must be in the form of the raw WWN format (xx:xx:xx:xx:xx:xx:xx:xx) or must be a valid nickname.

Did configuring the WWN or nickname solve the problem?

NO **YES**

↓ The switch appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

22

Clean the fiber-optic connectors on the cable.

a. Notify the customer the port will be blocked. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the port and sets the attached device offline.

b. Block the port (Block and Unblock Ports on page 3–25).

c. Disconnect both ends of the fiber-optic cable.

d. Clean the fiber-optic connectors (Clean Fiber-Optic Components on page 3–27).

e. Reconnect the fiber-optic cable.

f. Unblock the port (Block and Unblock Ports on page 3–25).

g. Monitor port operation for approximately five minutes.

Did the link incident recur?

YES **NO**

↓ The Fibre Channel link and switch appear operational.
Exit MAP.

23

Inspect and service the host bus adapters (HBAs), as necessary.

Did service of the HBAs solve the problem?

NO **YES**

↓ **Exit MAP.**

Contact the next level of support. **Exit MAP.**

24

The switch and attached device are performing a Fibre Channel link reset. This is a transient state. Wait approximately 30 seconds and inspect port state and LED behavior.

Did the link recover and resume operation?

NO **YES**

↓ The Fibre Channel link and switch appear operational. **Exit MAP.**

Go to step 1.

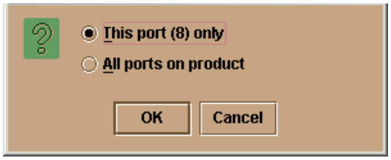
25

A link incident message appeared in the **Link Incident Log** or in the **Link Incident** field of the **Port Properties** dialog box; or an event code **581**, **582**, **583**, **584**, **585**, or **586** was observed at the console of an OSI server attached to the switch reporting the problem.

Clear the link incident for the port.

a. At the **Hardware View**, right-click the port. A pop-up menu appears.

b. Select **Clear Link Incident Alert(s)**. The **Clear Link Incident Alert(s)** dialog box displays (Figure 2–15).



● This port (8) only
○ All ports on product

Figure 2–15: Clear Link Incident Alert(s)

c. Select the **This port (*n*) only** radio button (where ***n*** is the port number) and click **OK**. The link incident clears.

d. Monitor port operation for approximately five minutes.

Did the link incident recur?

YES	NO
↓	The problem is transient and the Fibre Channel link and switch appear operational. **Exit MAP.**

26

Inspect the fiber-optic jumper cable attached to the port and ensure the cable is not bent and connectors are not damaged. If the cable is bent or connectors are damaged:

a. Notify the customer the port will be blocked. Ensure the customer’s system administrator quiesces Fibre Channel frame traffic through the port and sets the attached device offline.

b. Block the port (Block and Unblock Ports on page 3–25).

c. Remove and replace the fiber-optic jumper cable.

d. Unblock the port (Block and Unblock Ports on page 3–25).

Was a corrective action performed?

YES **NO**

↓ **Go to** step 28**.**

27

Monitor port operation for approximately five minutes.

Did the link incident recur?

YES **NO**

↓ The Fibre Channel link and switch appear operational.
Exit MAP.

28

Clean fiber-optic connectors on the jumper cable.

a. Notify the customer the port will be blocked. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the port and sets the attached device offline.

b. Block the port (Block and Unblock Ports on page 3–25).

c. Disconnect both ends of the fiber-optic jumper cable.

d. Clean the fiber-optic connectors (Clean Fiber-Optic Components on page 3–27).

e. Reconnect the fiber-optic jumper cable.

f. Unblock the port (Block and Unblock Ports on page 3–25).

g. Monitor port operation for approximately five minutes.

Did the link incident recur?

YES **NO**

↓ The Fibre Channel link and switch appear operational.
Exit MAP.

29

Disconnect the fiber-optic jumper cable from the switch port and connect the cable to a spare port.

Is a link incident reported at the new port?

YES **NO**

↓ **Go to** step 31**.**

30

The attached device is causing the recurrent link incident. Notify the customer of the problem and have the system administrator:

a. Inspect and verify operation of the attached device.

b. Repair the attached device if a failure is indicated.

c. Monitor port operation for approximately five minutes.

Did the link incident recur?

YES **NO**

↓ The attached device, Fibre Channel link, and switch appear operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

31

The switch port reporting the problem is causing the recurrent link incident. The recurring link incident indicates port degradation and a possible pending failure. **Go to** step 6**.**

32

Does the EWS interface appear operational?

NO **YES**

↓ **Go to** step 36**.**

33

A **Page cannot be found**, **Unable to locate the server**, **HTTP 404 - file not found**, or other similar message appears. The message indicates the web browser PC cannot communicate with the switch because:

- The switch-to-PC Internet link could not be established.
- AC power distribution in the switch failed, or AC power was disconnected.
- The switch CTP failed.

Continue.

34

Ensure the switch reporting the problem is connected to facility AC power. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES **NO**

↓ Analysis for an Ethernet link, AC power distribution, or CTP failure is not described in this MAP. Go to MAP 0000: Start MAP on page 2-6. If this is the second time at this step, contact the next level of support. **Exit MAP.**

35

Inspect Fibre Channel port operational states at the EWS interface.

a. At the **View** panel, click the **Port Properties** tab. The **View** panel (**Port Properties** tab) displays with port **0** highlighted in red.

b. Click the port number (**0** through (**139**) for which a failure is suspected to display properties for that port.

c. Inspect the **Operational State** field. Scroll down the **View** panel as necessary.

d. Table 2–13 lists port operational states and associated MAP 0600 steps that describe fault isolation procedures.

Table 2–13: MAP 600: Port Operational States and Actions

Operational State	Action
Offline	Go to step 14.
Not Operational	Go to step 14.
Port Failure	Go to step 6.
Testing	Internal or external loopback test in process. **Exit MAP.**
Invalid Attachment	Go to step 16.
Link Reset	Go to step 24.
Not Installed	Go to step 36.

36

Install an SFP optical transceiver in the port receptacle (RRP 1: SFP Optical Transceiver on page 4–2).

a. This procedure is concurrent and can be performed while switch power is on.

b. Verify the location of the failed port.

c. Perform an external loopback test for the port as part of FRU removal and replacement.

Exit MAP.

MAP 0700: Fabric, ISL, and Segmented Port Problem Determination

This MAP describes isolation of fabric logout, interswitch link (ISL), and E_Port segmentation problems. Failure indicators include:

- An event code recorded at the Edge Switch 2/24 **Event Log** or the EWS **Event Log**.
- A segmentation reason associated with a Fibre Channel port at the EWS interface.
- A yellow triangle (attention indicator) appears port graphic or at the alert panel of the **Products View** or **Hardware View**.
- A link incident message recorded in the **Link Incident Log** or **Port Properties** dialog box.

1

Was an event code **011**, **021**, **051**, **052**, **061**, **062**, **063**, **070**, **071**, or **072** observed at the Edge Switch 2/24 **Event Log** (HAFM server) or at the EWS **Event Log**?

YES	NO
↓	**Go to step 3.**

2

Table 2–14 lists event codes, brief explanations of the codes, and associated steps that describe fault isolation procedures.

Table 2–14: MAP 600: Event Codes

Event Code	Explanation	Action
011	Login server database invalid.	Go to step 7.
021	Name server database invalid.	Go to step 7.
051	Management server database invalid.	Go to step 8.
052	Management server internal error.	Go to step 8.
061	Fabric controller database invalid.	Go to step 9.
062	Maximum interswitch hop count exceeded.	Go to step 10.
063	Received link state record too large.	Go to step 11.
070	E_Port is segmented.	Go to step 12.

Table 2–14: MAP 600: Event Codes (Continued)

Event Code	Explanation	Action
071	switch is isolated.	Go to step 12.
072	E_Port connected to unsupported switch.	Go to step 13.

3

Is fault isolation being performed at the HAFM server (or customer-supplied server)?

YES **NO**

↓ Fault isolation is being performed through the EWS interface. **Go to** step 22**.**

4

Does a yellow triangle (attention indicator) appear adjacent to a Fibre Channel port graphic at the **Hardware View**?

YES **NO**

↓ The problem is transient and the switch-to-fabric element connection appears operational. **Exit MAP.**

5

Inspect the port state and LED status for all ports with an attention indicator.

a. At the **Hardware View**, double-click the port graphic with the attention indicator. The **Port Properties** dialog box displays.

b. Inspect the **Operational State** field at the **Port Properties** dialog box.

Does the **Operational State** field indicate **Segmented E_Port**?

YES **NO**

↓ Analysis for other link incident is not described in this MAP. Go to MAP 0600: Port Failure and Link Incident Analysis on page 2–64. **Exit MAP.**

6

Inspect the **Segmentation Reason** field at the **Port Properties** dialog box. Table 2–15 lists port segmentation reasons and associated steps that describe fault isolation procedures.

Table 2–15: Port Segmentation Reasons and Actions

Segmentation Reason	Action
Incompatible operating parameters.	Go to step 14.
Duplicate domain IDs.	Go to step 15.
Incompatible zoning configurations.	Go to step 16.
Build fabric protocol error.	Go to step 17.
No principal switch.	Go to step 19.
No response from attached switch.	Go to step 20.
ELP retransmission failure timeout	Go to step 21.

7

A minor error occurred that caused fabric services database to be re-initialized to an empty state. As a result, a disruptive fabric logout and login occurred for all attached devices. The following list explains the errors.

- **Event code 011 -** The login server database failed cyclic redundancy check (CRC) validation.
- **Event code 021 -** The name server database failed CRC validation.

All attached devices resume operation after fabric login. Perform the data collection procedure and return the Zip disk to HP for analysis. **Exit MAP.**

8

A minor error occurred that caused management server database to be re-initialized to an empty state. As a result, a disruptive server logout and login occurred for all attached devices. The following list explains the errors.

- **Event code 051 -** The management server database CRC validation.
- **Event code 052 -** An internal operating error was detected by the management server subsystem.

All attached devices resume operation after management server login. Perform the data collection procedure and return the Zip disk to HP for analysis. **Exit MAP.**

9

A minor error occurred that caused fabric controller database to be re-initialized to an empty state. As a result, the switch briefly lost interswitch link capability. The following explains the error.

- **Event code 061 -** The fabric controller database failed CRC validation.

All interswitch links resume operation after CTP reset. Perform the data collection procedure and return the Zip disk to HP for analysis. **Exit MAP.**

10

As indicated by an event code **062**, the fabric controller software detected a path to another switch (or fabric element) in a multiswitch fabric that traverses more than three interswitch links (hops). Fibre Channel frames may persist in the fabric longer than timeout values allow.

Advise the customer of the problem and work with the system administrator to reconfigure the fabric so the path between any two fabric elements does not traverse more than three hops.

Did fabric reconfiguration solve the problem?

NO **YES**

↓ The switch and multiswitch fabric appear operational.
Exit MAP.

Contact the next level of support. **Exit MAP.**

11

As indicated by an event code **063**, the fabric controller software detected a fabric element (switch or switch) in a multiswitch fabric that has more than 32 ISLs attached. Fibre Channel frames may be lost or routed in loops because of potential fabric routing problems.

Advise the customer of the problem and work with the system administrator to reconfigure the fabric so that no switch or switch elements have more than 32 ISLs.

Did fabric reconfiguration solve the problem?

NO **YES**

↓ The switch and multiswitch fabric appear operational.
Exit MAP.

Contact the next level of support. **Exit MAP.**

12

A **070** event code indicates an E_Port detected an incompatibility with an attached switch and prevented the switches from forming a multiswitch fabric. A segmented E_Port cannot transmit Class 2 or Class 3 Fibre Channel traffic.

A **071** event code indicates the switch is isolated from all switches in a multiswitch fabric, and is accompanied by a **070** event code for each segmented E_Port. The **071** event code is resolved when all **070** events are corrected.

Obtain supplementary event data for each **070** event code.

a. At the **Hardware View**, click Logs and select **Event Log**. The **Event Log** displays.

b. Examine the first five bytes (**0** through **4**) of event data.

c. Byte **0** specifies the switch port number (**00** through **139**) of the segmented E_Port. Byte **4** specifies the segmentation reason (Table 2–16).

Table 2–16: Byte 4, Segmentation Reasons, and Actions

Byte 4	Segmentation Reason	Action
01	Incompatible operating parameters.	Go to step 14.
02	Duplicate domain IDs.	Go to step 15.
03	Incompatible zoning configurations.	Go to step 16.
04	Build fabric protocol error.	Go to step 17.
05	No principal switch.	Go to step 19.
06	No response from attached switch.	Go to step 20.
07	ELP retransmission failure timeout.	Go to step 21.

13

As indicated by an event code **072**, a switch E_Port is connected to an unsupported switch or fabric element.

Advise the customer of the problem and disconnect the interswitch link to the unsupported switch. **Exit MAP.**

14

A switch E_Port segmented because the error detect time out value (E_D_TOV) or resource allocation time out value (R_A_TOV) is incompatible with the attached fabric element.

a. Contact HP customer support or engineering personnel to determine the recommended E_D_TOV and R_A_TOV values for both switches.

b. Notify the customer both switches will set offline. Ensure the system administrator quiesces Fibre Channel frame traffic through the switches and sets attached devices offline.

c. Set both switches offline (Set the Switch Online or Offline on page 3–23).

d. At the **Hardware View** for the first switch reporting the problem, click **Configure** and select **Operating Parameters**. The **Configure Operating Parameters** dialog box displays.

e. Type the recommended E_D_TOV and R_A_TOV values, then click **Activate**.

f. Repeat steps d and e at the **Hardware View** for the switch attached to the segmented E_Port (second switch). Use the same E_D_TOV and R_A_TOV values.

g. Set both switches online (Set the Switch Online or Offline on page 3–23).

Did the operating parameter change solve the problem and did both switches join through the ISL to form a fabric?

NO	YES
↓	The switch, associated ISL, and multiswitch fabric appear operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

15

A switch E_Port segmented because two fabric elements had duplicate domain IDs.

a. Work with the system administrator to determine the desired domain ID (**1** through **31** inclusive) for each switch.

b. Notify the customer both switches will set offline. Ensure the system administrator quiesces Fibre Channel frame traffic through the switch and sets attached devices offline.

c. Set both switches offline (Set the Switch Online or Offline on page 3–23).

d. At the **Hardware View** for the first switch reporting the problem, click **Configure** and select **Operating Parameters**. The **Configure Operating Parameters** dialog box displays.

e. Type the customer-determined preferred domain ID value, then click **Activate**.

f. Repeat steps d and e at the **Hardware View** for the switch attached to the segmented E_Port (second switch). Use a different preferred domain ID value.

g. Set both switches online (Set the Switch Online or Offline on page 3–23).

Did the domain ID change solve the problem and did both switches join through the ISL to form a fabric?

NO **YES**

↓ The switch, associated ISL, and multiswitch fabric appear operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

16

A switch E_Port segmented because two switches had incompatible zoning configurations. An identical zone name is recognized in the active zone set for both switches, but the zones contain different members.

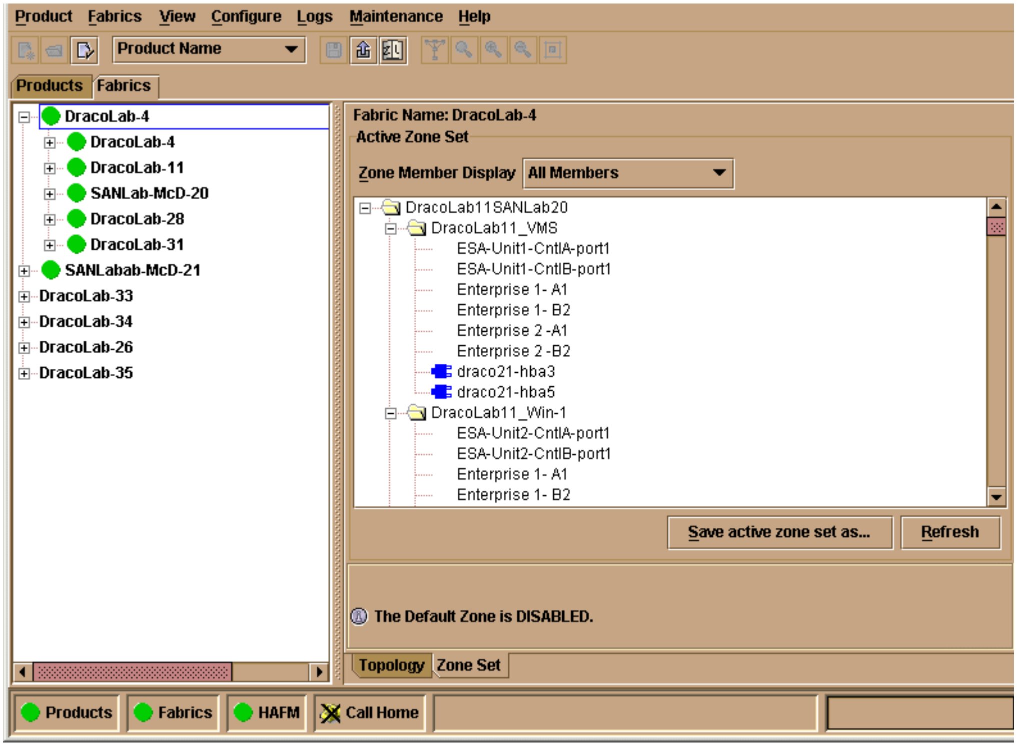
a. Work with the system administrator to determine the desired zone name change for one of the affected switches. Zone names must conform to the following rules:

   - The name must be 64 characters or fewer in length.
   - The first character must be a letter (**a** through **z**), upper or lower case.
   - Other characters are alphanumeric (**a** through **z** or **0** through **9**), dollar sign (**$**), hyphen (**-**), caret (**^**), or underscore (_).

b. Close the Product Manager application (**Hardware View**). The main HAFM window or **Products View** (still active) displays.

c. Select the Fabrics tab. In the left pane of the **Fabrics View** window, select the fabric of which the switch is a member. The **Fabrics View** displays with the default **Topology** tab active.

d. Select the **Zone Set** tab at the bottom of the window. The **Zone Set View** displays with the active zone set shown (Figure 2–16).



Product Name

- DracoLab-4
  - DracoLab-4
  - DracoLab-11
  - SANLab-McD-20
  - DracoLab-28
  - DracoLab-31
- SANLabab-McD-21
- DracoLab-33
- DracoLab-34
- DracoLab-26
- DracoLab-35

Fabric Name: DracoLab-4

Active Zone Set

Zone Member Display: All Members

- DracoLab11SANLab20
  - DracoLab11_VMS
    - ESA-Unit1-CntlA-port1
    - ESA-Unit1-CntlB-port1
    - Enterprise 1- A1
    - Enterprise 1- B2
    - Enterprise 2 -A1
    - Enterprise 2 -B2
    - draco21-hba3
    - draco21-hba5
  - DracoLab11_Win-1
    - ESA-Unit2-CntlA-port1
    - ESA-Unit2-CntlB-port1
    - Enterprise 1- A1
    - Enterprise 1- B2

The Default Zone is DISABLED.

Figure 2–16: Zone Set View

e. Inspect zone names in the active zone set to determine the incompatible name.

f. Modify the incompatible zone name as directed by the customer:

1. Click **Configure** and select **Zoning Library**. The **Zoning Library** dialog box displays.
2. Click the **Zones** tab.
3. Right click the zone name to be changed and select **Rename**. The **Rename** dialog box displays. Type the new zone name (specified by the customer) and click OK.
4. Close the **Zoning Library** dialog box.
5. In the left pane of the **Fabric View** window, select the fabric containing the zone name that was changed. Click the **Zone Set** tab. Verify that the message area below the **Active Zone Set** contains the message “The active zone set does not currently match the configured zone set.”

6. To activate the zone set, click **Configure** and select **Active Zone Set**. The **Active Zone Set** dialog box displays. Select the zone to be activated and click **Next**.
7. The new display summarizes the zone member changes that will be made by activating the new zone set. Click **Next** if this reflects the desired zone change.
8. The new display summarizes switches that will be affected by activating the new zone set. Click **Next** if this reflects the desired zone change.
9. The new display directs the user to press **Start** to activate the zone set. Click **Start** to activate the zone set.

Did the zone name change solve the problem and did both switches join through the ISL to form a fabric?

NO **YES**

↓ The switch, associated ISL, and fabric appear operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

17

A switch E_Port segmented because a build fabric protocol error was detected.

a. Disconnect the fiber-optic jumper cable from the segmented E_Port.

b. Reconnect the cable to the same port.

Did disconnecting and reconnecting the cable solve the problem and did both switches join through the ISL to form a fabric?

NO **YES**

↓ The switch, associated ISL, and multiswitch fabric appear operational. **Exit MAP.**

18

Initial program load (IPL) the switch (IML, IPL or Reset the Switch on page 3–29).

Did the IPL solve the problem and did both switches join through the ISL to form a fabric?

NO **YES**

↓ The switch, associated ISL, and multiswitch fabric appear operational. **Exit MAP.**

Perform the data collection procedure and contact the next level of support. **Exit MAP.**

19

A switch E_Port segmented because no switch in the fabric is capable of becoming the principal switch.

a. Notify the customer the switch will set offline. Ensure the system administrator quiesces Fibre Channel frame traffic through the switch and sets attached devices offline.

b. Set the switch offline (Set the Switch Online or Offline on page 3–23).

c. At the **Hardware View** for the switch, click **Configure** and select **Operating Parameters**. The **Configure Operating Parameters** dialog box displays.

d. At the **Switch Priority** field, select **Principal**, **Never Principal**, or **Default** (the default setting is **Default**. The switch priority 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 switches (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 that 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 multiswitch fabric must be set as **Principal** or **Default**. If all switches are set to **Never Principal**, all ISLs segment and the message **No Principal Switch** appears in the **Reason** field of the **Port Properties** dialog box.

e. Set the switch online (Set the Switch Online or Offline on page 3–23).

Did the switch priority change solve the problem and did both switches join through the ISL to form a fabric?

NO	YES
↓	The switch, associated ISL, and multiswitch fabric appear operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

20

A switch E_Port segmented (at an operational switch) because a response to a verification check indicates an attached switch is not operational.

a. Perform the data collection procedure at the operational switch and return the Zip disk to HP for analysis. This information may assist in fault isolating the failed switch.

b. Go to MAP 0000: Start MAP on page 2-6 and perform fault isolation for the failed switch.

Exit MAP.

21

A switch E_Port segmented because the switch was unable to receive a response (from an operational fabric element) to multiple exchange link protocol (ELP) frame transmissions, and unable to receive a fabric login (FLOGI) frame. The switch's inability to receive responses is caused by a hardware or link failure. Port segmentation occurs after five ELP transmissions, and prevents the failed switch from joining an operational Fibre Channel fabric.

The switch exhibits other failure symptoms and one or more other failure event codes are recorded in addition to the **070** event code (E_Port is segmented). Go to MAP 0000: Start MAP on page 2–6 and perform fault isolation for the failed switch.

Exit MAP.

22

Does the EWS interface appear operational?

YES	NO
↓	Analysis for an Ethernet link, AC power distribution, or CTP failure is not described in this MAP. Go to MAP 0000: Start MAP on page 2-6. If this is the second time at this step, contact the next level of support. **Exit MAP.**

23

Inspect the Fibre Channel port segmentation reason at the EWS interface.

a. At the **View** panel, click the **Port Properties** tab. The **View** panel (**Port Properties** tab) displays.

b. Click the port number (**0** through **139**) of the segmented port.

c. Inspect the **Segmentation Reason** field for the selected port.

Is the **Segmentation Reason** field blank or does it display an `N/A` message?

NO **YES**

↓ The switch ISL appears operational. **Exit MAP.**

The **Segmentation Reason** field displays a reason message. Table 2–17 lists segmentation reasons and associated steps that describe fault isolation procedures.

Table 2–17: Segmentation Reasons and Actions

Segmentation Reason	Action
Incompatible operating parameters.	Go to step 14.
Duplicate domain IDs.	Go to step 15.
Incompatible zoning configurations.	Go to step 16.
Build fabric protocol error.	Go to step 17.
No principal switch.	Go to step 19.
No response from attached switch.	Go to step 20.
ELP retransmission failure timeout	Go to step 21.

MAP 0800: Console PC Problem Determination

This MAP describes isolation of hardware-related problems with the HAFM server (or customer-supplied server) platform. Although this MAP provides high-level fault isolation instructions, refer to the documentation provided with the PC for detailed problem determination and resolution.

1

At the HAFM server, close the HAFM application.

a. At the navigation control panel of the **Product View**, select **Exit** from the **Logout/Exit** icon. The HAFM application closes.

b. Close any other applications that are running.

Continue.

2

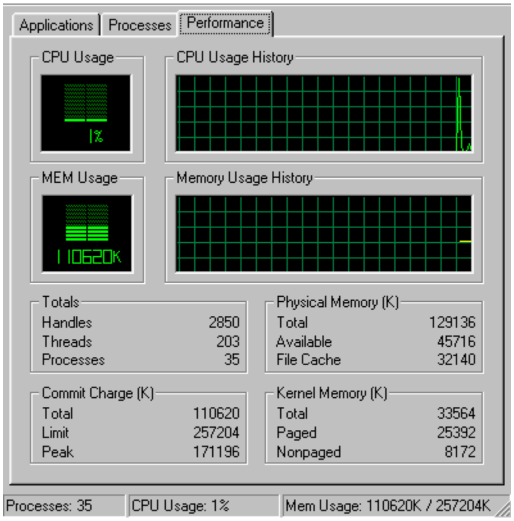
Inspect the available random access memory (RAM). The computer must have a minimum of 64 megabytes (MB) of memory to run the Windows operating system and HAFM application.

a. Right-click anywhere in the Windows task bar at the bottom of the desktop. A pop-up menu appears.

b. Select **Task Manager**. The **Windows Task Manager** dialog box displays with the **Performance** page open.

c. At the **Physical Memory (K)** portion of the dialog box, inspect the total amount of physical memory.

d. Close the dialog box by clicking **Close** at the upper right corner of the window.



1%

110620K

Totals

Handles	2850
Threads	203
Processes	35

Physical Memory (K)

Total	129136
Available	45716
File Cache	32140

Commit Charge (K)

Total	110620
Limit	257204
Peak	171196

Kernel Memory (K)

Total	33564
Paged	25392
Nonpaged	8172

Processes: 35 CPU Usage: 1% Mem Usage: 110620K / 257204K

Does the computer have sufficient memory?

YES **NO**

↓ A memory upgrade is required. Inform the customer of the problem and contact the next level of support.

3

Reboot the HAFM server PC and perform system diagnostics.

a. Click the Windows **Start** button. The **Windows Workstation** menu displays.

b. At the **Windows Workstation** menu, select **Shut Down**. The **Shut Down Windows** dialog box appears.

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

d. Wait approximately 30 seconds and power on the PC. After POSTs complete, the **Begin Logon** dialog box displays.

e. Simultaneously press **Ctrl**, **Alt**, and **Delete** to display the **Logon Information** dialog box. Type a user name and password (obtained in MAP 0000: Start MAP on page 2–6) and click **OK**. The Windows desktop displays.

Did POSTs detect a problem?

NO **YES**

↓ A computer hardware problem exists. Refer to the supporting documentation shipped with the PC for instructions on resolving the problem.

4

After rebooting the PC, the HAFM application starts and the **HAFM Login** dialog box displays.

Did the **HAFM Login** dialog box display?

YES **NO**

↓ **Go to** step 6.

5

At the **HAFM Login** dialog box, type a user name, password, and HAFM server name (obtained in MAP 0000: Start MAP on page 2–6, and all are case sensitive), and click **Login**. The application opens and the **Product View** displays.

Did the **Product View** display and does the HAFM application appear operational?

NO **YES**

↓ The PC appears operational.

6

Perform one of the following:

- If the PC has standalone diagnostic test programs resident on the hard drive, perform the diagnostics. Refer to supporting documentation shipped with the PC for instructions.
- If the PC does not have standalone diagnostic test programs resident on fixed disk, **go to** step 7.

Did diagnostic test programs detect a problem?

NO **YES**

↓ Refer to the supporting documentation shipped with the PC for instructions to resolve the problem.

7

Reboot the HAFM server PC.

a. Click the Windows **Start** button. The **Windows Workstation** menu displays.

b. At the **Windows Workstation** menu, select **Shut Down**. The **Shut Down Windows** dialog box appears.

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

d. Wait approximately 30 seconds and power on the PC. After POSTs complete, the **Begin Logon** dialog box displays.

e. Simultaneously press **Ctrl**, **Alt**, and **Delete** to display the **Logon Information** dialog box. Type a user name and password (obtained in MAP 0000: Start MAP on page 2–6) and click **OK**. The HAFM application starts and the **HAFM Login** dialog box displays.

f. At the **HAFM Login** dialog box, type a user name, password, and HAFM server name (obtained in MAP 0000: Start MAP on page 2–6, and all are case sensitive), and click **Login**. The application opens and the **Product View** displays.

Did the **Product View** display and does the HAFM application appear operational?

NO **YES**

↓ The PC appears operational.

8

Re-install the HAFM application (Install or Upgrade Software on page 3–42).

Did the HAFM application install and open successfully?

NO **YES**

↓ The PC appears operational.

9

Advise the customer and next level of support that the PC hard drive should be formatted. If the customer and support personnel do not concur, **go to** step 10.

a. Format the PC hard drive. Refer to supporting documentation shipped with the PC for instructions.

b. Install the Windows operating system and HAFM application.

Did the PC hard drive format, and did the operating system and HAFM application install and open successfully?

NO	YES
↓	The PC appears operational.

10

Additional analysis for the failure is not described in this MAP. **Contact the next level of support.**

3

Repair Information

This chapter describes the repair and repair-related procedures for the HP StorageWorks Edge Switch 2/24, and associated field-replaceable units (FRUs). These procedures are described:

- Obtaining log information at the HP StorageWorks HA-Fabric Manager (HAFM) server.
- Obtaining and interpreting port diagnostic and performance data, and performing port diagnostic loopback tests.
- Collecting maintenance data.
- Setting the switch online or offline.
- Blocking or unblocking Fibre Channel ports.
- Cleaning fiber-optic components.
- Powering the switch on and off.
- Performing an initial machine load (IML).
- Performing an initial program load (IPL).
- Performing a switch reset.
- Managing firmware versions.
- Managing configuration data.
- Installing or upgrading software.

Do not perform repairs until a failure is isolated to a FRU. If fault isolation was not performed, refer to "MAP 0000: Start MAP" on page 2-6.

Factory Defaults

Table 3–1 lists the defaults for the passwords, and IP, subnet, and gateway addresses.

Table 3–1: 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

Procedural Notes

NOTE: HAFM and Product Manager screens in this manual may not match the screens on your server and workstation. The title bars have been removed and the fields may contain data that does not match the data seen on your system.

The following procedural notes are referenced in applicable repair procedures. The notes do not necessarily apply to all procedures in the chapter.

1. Before performing a repair procedure, read the procedure carefully and thoroughly to familiarize yourself with the information and reduce the possibility of problems or customer down time.
2. When performing procedures described in this chapter, heed all **WARNING** and **CAUTION** statements, and other statements listed in the preface of this manual.
3. After completing steps of a detailed procedure that is referenced from another procedure, return to the initial (referencing) procedure and continue to the next step of that procedure.

Using Log Information

The HAFM and switch product manager provide access to ten logs that provide information for administration, operation, and maintenance personnel. Each log stores up to 1,000 entries. The most recent entry appears at the top of a log. If a log is full, a new entry overwrites the oldest entry.

Five logs are accessed through the HAFM application:

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

Five logs are accessed through the Product Manager application:

- Switch Audit Log.
- Switch Event Log.
- Hardware Log.
- Link Incident Log.
- Threshold Alert Log.

HAFM Audit Log

The HAFM **Audit Log** displays a history of user actions performed through the HAFM application. This information is useful for system administrators and users. To open the HAFM **Audit Log**, select **Audit Log** from the **Logs** menu on the navigation control panel.

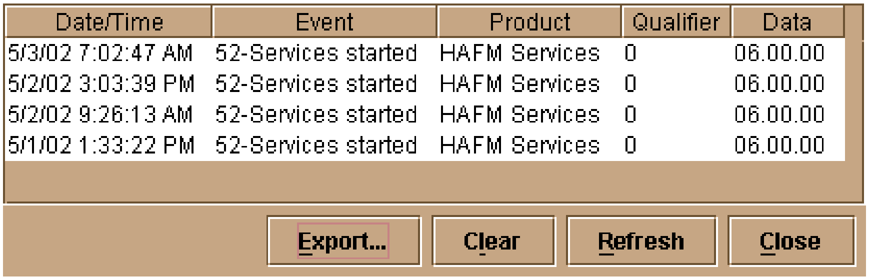
For a description of the HAFM **Audit Log** and an explanation of button functions at the bottom of the log window, refer to the *hp StorageWorks ha-fabric manager user guide*.

HAFM Event Log

The HAFM **Event Log** (Figure 3–1) displays events or error conditions recorded by the HAFM services application. Entries reflect the status of the application and managed switches.

Information associated with a call-home failure is intended for maintenance personnel to fault isolate the problem (modem failure, no dial tone, etc.), while information provided in all other entries is generally intended for use by third-level support personnel to isolate more significant problems.

To open the HAFM **Event Log**, select **Event Log** from the **Logs** menu on the navigation control panel.



Date/Time	Event	Product	Qualifier	Data
5/3/02 7:02:47 AM	52-Services started	HAFM Services	0	06.00.00
5/2/02 3:03:39 PM	52-Services started	HAFM Services	0	06.00.00
5/2/02 9:26:13 AM	52-Services started	HAFM Services	0	06.00.00
5/1/02 1:33:22 PM	52-Services started	HAFM Services	0	06.00.00

Figure 3–1: HAFM Event Log

The Event Log contains the following columns:

- **Date/Time -** the date and time the event was reported to the HAFM server.
- **Event -** an event number and brief description of the event. Include both the event number and description when reporting an event to third-level customer support.
- **Product -** the product associated with the event. Some events are associated with the HAFM services application, while others are associated with a specific instance of the HAFM application. In the latter case, the product and configured name (or internet protocol (IP) address) associated with the instance are displayed.
- **Qualifier -** this column provides an event qualifier for use by engineering personnel. Include this number when reporting an event to third-level customer support.

- **Data -** additional event data for fault isolating a problem. Use the information when fault isolating a call-home problem, or include the information when reporting an event to third-level customer support.

To ensure recently-created events appear in the log, periodically refresh the log display. This is important when inspecting the log to verify a repair procedure. To refresh the log, click **Refresh**.

Session Log

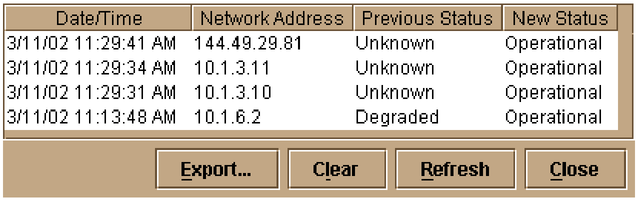
The **Session Log** displays a session (login and logout) history for the HAFM server, including the date and time, user name, and network address of each session. This information is useful for system administrators and users. To open the **Session Log**, select **Session Log** from the **Logs** menu on the navigation control panel.

For a description of the **Session Log** and an explanation of button functions at the bottom of the log window, refer to the *hp StorageWorks ha-fabric manager user guide*.

Product Status Log

The **Product Status Log** (Figure 3–2) records an entry when the status of a switch changes. The log reflects the previous status and current status of the switch, and indicates the instance of a switch Product Manager application that should be opened to investigate a problem. The information is useful to maintenance personnel for fault isolation and repair verification.

To open the **Product Status Log**, select **Product Status Log** from the **Logs** menu on the navigation control panel.



Date/Time	Network Address	Previous Status	New Status
3/11/02 11:29:41 AM	144.49.29.81	Unknown	Operational
3/11/02 11:29:34 AM	10.1.3.11	Unknown	Operational
3/11/02 11:29:31 AM	10.1.3.10	Unknown	Operational
3/11/02 11:13:48 AM	10.1.6.2	Degraded	Operational

Figure 3–2: Product Status Log

The log contains the following columns:

- **Date/Time -** the date and time the switch status change occurred.
- **Network Address -** the IP address or configured name of the switch. This address or name corresponds to the address or name displayed under the switch icon at the Product View.
- **Previous Status -** the status of the switch prior to the reported status change (Operational, Degraded, Failed, or Unknown). An Unknown status indicates the HAFM application cannot communicate with the switch.
- **New Status -** the status of the switch after to the reported status change (Operational, Degraded, Failed, or Unknown).

To ensure recently-created events appear in the log, periodically refresh the log display. This is important when inspecting the log to verify a repair procedure. To refresh the log, click **Refresh**.

Fabric Log

The **Fabric Log** reflects the time and nature of significant changes in the managed fabric.

To display the **Fabric Log**, choose **Fabric Log** from the **Logs** menu.

- The **Date/Time** column displays the date and time of the change in the fabric.
- The **Fabric Status Changed** column displays the type of change in the fabric (for example, a switch was added or removed, an ISL was added or removed, the fabric was renamed or persisted, or a zone set became active).
- The **Description** column displays a description of the change in the fabric.

For a description of the **Audit Log** and an explanation of button functions at the bottom of the log window, refer to the switch *hp StorageWorks ha-fabric manager user guide*.

Edge Switch 2/24 Audit Log

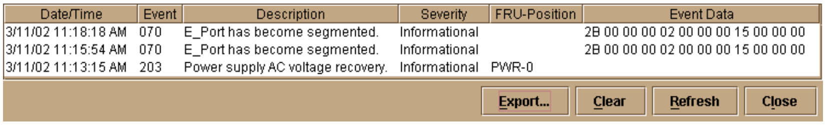
The switch **Audit Log** displays a history of all configuration changes made to a switch from the Product Manager or a simple network management protocol (SNMP) management workstation. This information is useful for system administrators and users. To open the **Audit Log** from the **Hardware View**, **Port List View**, or **Performance View**, select **Audit Log** from the **Logs** menu on the navigation control panel.

For a description of the **Audit Log** and an explanation of button functions at the bottom of the log window, refer to the switch *hp StorageWorks edge switch 2/24 product manager user guide*.

Edge Switch 2/24 Event Log

The switch **Event Log** (Figure 3–3) displays a history of events for the switch, such as system events, degraded operation, FRU failures, FRU removals and replacements, port problems, Fibre Channel link incidents, and HAFM server-to-switch communication problems. All detected software and hardware failures are recorded in the **Event Log**. The information is useful to maintenance personnel for fault isolation and repair verification.

To open the **Event Log**, select **Event Log** from the **Logs** menu on the navigation control panel.



Date/Time	Event	Description	Severity	FRU-Position	Event Data
3/11/02 11:18:18 AM	070	E_Port has become segmented.	Informational		2B 00 00 00 02 00 00 00 15 00 00 00
3/11/02 11:15:54 AM	070	E_Port has become segmented.	Informational		2B 00 00 00 02 00 00 00 15 00 00 00
3/11/02 11:13:15 AM	203	Power supply AC voltage recovery.	Informational	PWR-0	

Figure 3–3: Switch Event Log

The log contains the following columns:

- **Date/Time -** the date and time the switch event occurred.
- **Event -** the three-digit event code associated with the event. Refer to Appendix B for an explanation of event codes.
- **Description -** a brief description of the event.
- **Severity -** the severity of the event (Informational, Minor, Major, or Severe).

- **FRU-Position -** an acronym representing the FRU or non-FRU elements, followed by a number representing the FRU or chassis position. The acronyms are:

  — **CTP -** control processor (CTP) card. The chassis slot is 0. The CTP card is not a FRU.

  — **PWR** - power supply. Chassis slots for redundant power supplies are 0 and 1.

NOTE: Three cooling fans are integrated in each power supply. Cooling fans are not FRUs. A failed cooling fan requires replacement of the power supply.

- **Event Data -** up to 32 bytes of supplementary event data (if available for the event) in hexadecimal format. Refer to Appendix B for an explanation of the supplementary event data.

Refresh the Event Log

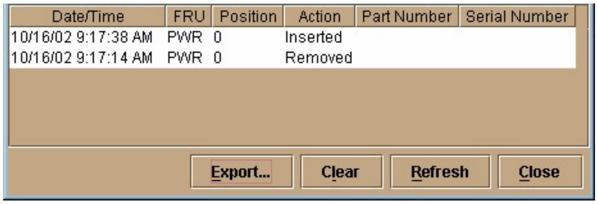
To ensure recently-created events appear in the **Event Log**, periodically refresh the log display. This is particularly important when inspecting the log for informational event codes to verify a repair procedure. To refresh the log, click **Refresh** at the bottom of the log window.

Clear the Event Log

To ensure the **Event Log** is up-to-date and not filled with archived events, periodically clear the log display. To clear the log, click **Clear** at the bottom of the log window.

Hardware Log

The **Hardware Log** (Figure 3–4) displays a history of FRU removals and replacements (insertions) for the switch. The information is useful to maintenance personnel for fault isolation and repair verification.



Date/Time	FRU	Position	Action	Part Number	Serial Number
10/16/02 9:17:38 AM	PWR	0	Inserted		
10/16/02 9:17:14 AM	PWR	0	Removed		

Figure 3–4: Hardware Log

To open the **Hardware Log**, select **Hardware Log** from the **Logs** menu on the navigation control panel.

The log contains the following columns:

- **Date/Time -** the date and time the FRU was inserted or removed.
- **FRU -** an acronym representing the FRU type or non-FRU element. The acronyms are:
  - **CTP -** control processor (CTP) card. The CTP card is not a FRU. A failed CTP card requires replacement of the switch
  - **PWR** - power supply.

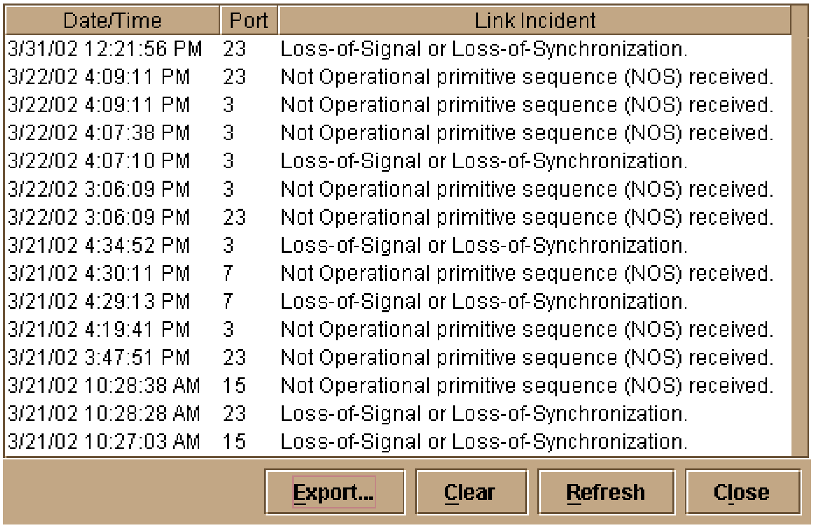
NOTE: Three cooling fans are integrated in each power supply. Cooling fans are not FRUs. A failed cooling fan requires replacement of the power supply.

- Position - a number representing the FRU chassis position. The chassis (slot) position for a nonredundant CTP card is 0. Chassis slots for redundant power supplies are 0 and 1.
- **Action -** the action performed (Inserted or Removed).
- **Part Number -** the part number of the inserted or removed FRU.
- **Serial Number -** the serial number of the inserted or removed FRU.

Link Incident Log

The **Link Incident Log** (Figure 3–5) displays a history of Fibre Channel link incidents and associated port numbers for the switch. The information is useful to maintenance personnel for isolating port problems and repair verification.

To open the **Link Incident Log**, select **Link Incident Log** from the **Logs** menu on the navigation control panel.



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

Figure 3–5: Link Incident Log

The log contains the following columns:

- **Date/Time -** the date and time the link incident occurred.
- **Port -** the port number that reported the link incident (0 through 23).
- **Link Incident** - a brief description of the link incident. Problem descriptions include:
  - — Implicit incident.
  - — Bit-error threshold exceeded.
  - — Link failure - loss of signal or loss of synchronization.
  - — Link failure - not-operational primitive sequence received.
  - — Link failure - primitive sequence timeout.
  - — Link failure - invalid primitive sequence received for current link state.

Refer to MAP 0600: Port Failure and Link Incident Analysis on page 2–64 for corrective actions in response to these link incident messages.

Refresh the Link Incident Log

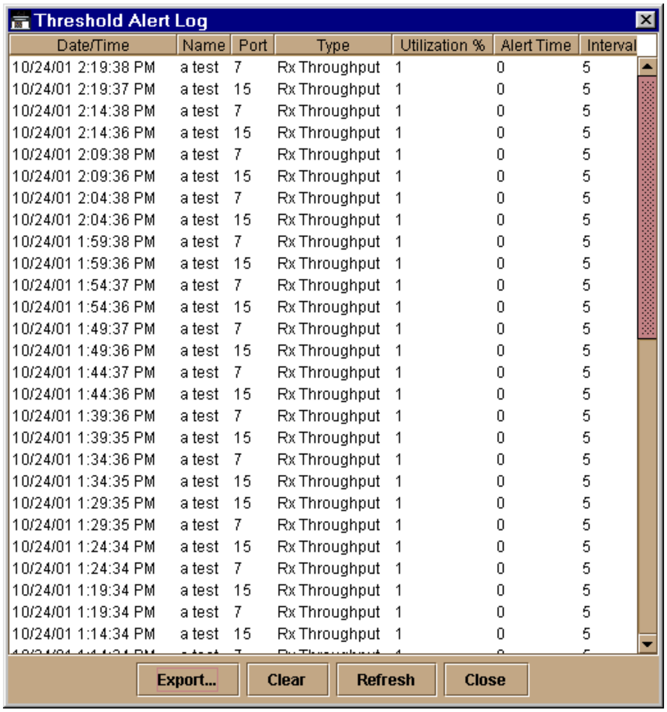
To ensure recently-created link incidents appear in the **Link Incident Log**, periodically refresh the log display. To refresh the log, click **Refresh** at the bottom of the log window.

Clear the Link Incident Log

To ensure the **Link Incident Log** is up-to-date and not filled with archived incidents, periodically clear the log display. To clear the log, click **Clear** at the bottom of the log window.

Threshold Alert Log

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



Threshold Alert Log

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

Figure 3–6: Threshold Alert Log

- **Date/Time**

  Date and time stamp for when the alert occurred.

- **Name**

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

- **Port**

  Port number where the alert occurred.

- **Type**

  The type of alert: transmit (TX) or receive (RX).

- **Utilization %**

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

- **Alert Time**

  The time that the utilization % must exist before an alert is generated. This is set through the **Configure Threshold Alerts** dialog box.

- **Interval**

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

Performing Port Diagnostics

Fibre channel port diagnostics are performed at the switch and Product Manager application. These diagnostics include:

- Inspecting port LEDs at the switch front panel or emulated port LEDs at the HAFM **Hardware View**.
- Inspecting parameters at the HAFM server (Edge Switch 2/24 Product Manager application).
- Inspecting parameters at the EWS interface (refer to the *hp StorageWorks embedded web server user guide* for more information)

Port LEDs

To obtain port operational information, inspect port LEDs at the switch front panel or emulated port LEDs at the HAFM **Hardware View**. Amber and blue/green LEDs adjacent to each port indicate operational status as described in Table 3–2:

Table 3–2: Port Operational States

Port State	Blue/Green LED	Amber LED	Alert Symbol	Description
Online	On or Blinking	Off	None	An attached device is connected to the switch and ready to communicate, or is communicating through the switch with other attached devices. If the port remains online at 1.0625 Gbps, the blue/green LED illuminates green. If the port remains online at 2.125 Gbps, the blue/green LED illuminates blue. At the switch, the blue/green LED blinks green when there is Fibre Channel traffic through the port at 1.0625 Gbps. At the switch, the blue/green LED blinks blue when there is Fibre Channel traffic through the port at 12.125 Gbps.

Table 3–2: Port Operational States (Continued)

Port State	Blue/Green LED	Amber LED	Alert Symbol	Description
Offline	Off Off	Off Off	None Yellow Triangle	The port is blocked and transmitting the offline sequence (OLS) to the attached device. The port is unblocked and receiving the OLS, indicating the attached device is offline.
Beaconing	Off, On, or Blinking	Blinking	Yellow Triangle	The port is beaconing. The amber port LED blinks once every two seconds to enable users to locate the port.
Invalid Attachment	On	Off	Yellow Triangle	The port has an invalid attachment. The reason appears in the **Reason** field at the **Port Properties** dialog box.
Link Incident	Off	Off	Yellow Triangle	A link incident occurred. The alert symbol appears at the **Hardware View** and **Port List View**.
Link Reset	Off	Off	Yellow Triangle	The switch and attached device are performing a link reset operation to recover the link connection. This is a transient state that should not persist.
No Light	Off	Off	None	No signal (light) is received at the switch port. This is a normal condition when there is no cable attached to the port or when the attached device is powered off.
Inactive	On	Off	Yellow Triangle	The port is inactive. The reason appears in the **Reason** field at the **Port Properties** dialog box.
Not Installed	Off	Off	None	An optical transceiver is not installed in the switch port.

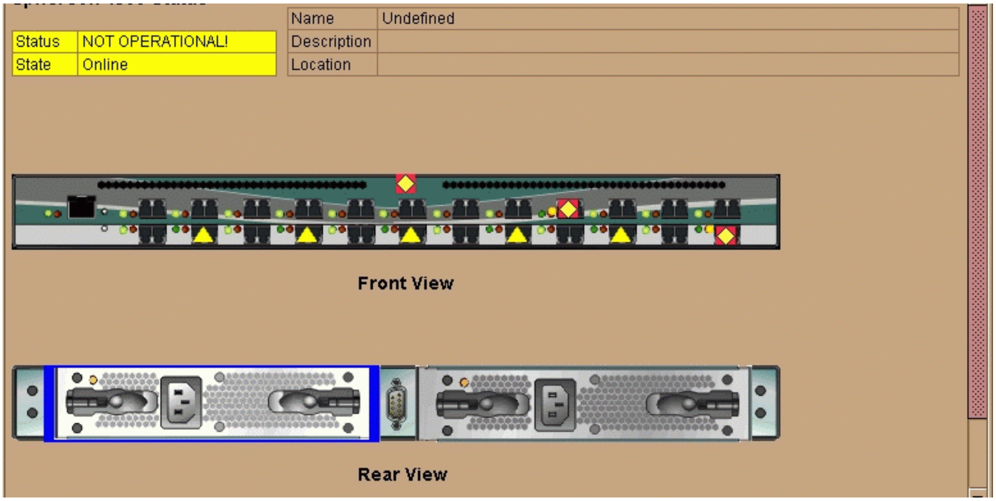
Table 3–2: Port Operational States (Continued)

Port State	Blue/Green LED	Amber LED	Alert Symbol	Description
Not Operational	Off	Off	Yellow Triangle	The port is receiving the not operational sequence (NOS) from an attached device.
Port Failure	Off	On	Red and Yellow Blinking Diamond	The port failed and requires service.
Segmented E_Port	On	Off	Yellow Triangle	The E_Port is segmented, preventing two connected switches from joining and forming a multiswitch fabric.The reason appears in the **Reason** field of the **Port Properties** dialog box.
Testing	Off	Blinking	Yellow Triangle	The port is performing an internal loopback test.
	On	Blinking	Yellow Triangle	The port is performing an external loopback test.

Hardware View

The **Hardware View** (Figure 3–7) displays a representation of and associated information about a specified switch. This information is useful to maintenance personnel for port-specific fault isolation and repair verification, link incidents, and port segmentation problems.

- Port operational state information from the **Port Properties** dialog box (Figure 3–8).
- Port LED behavior that emulates the operational status of the corresponding real switch. Refer to the *hp StorageWorks edge switch 2/24 installation guide* for explanation of LED behavior.
- Colored alert symbols (yellow triangle or red diamond with yellow background) that indicate port status. Refer to the *hp StorageWorks edge switch 2/24 product manager user guide* for an explanation of alert symbol indications.

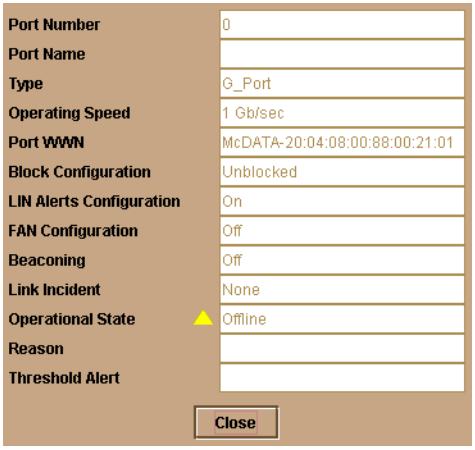


Status	NOT OPERATIONAL!
State	Online

Name	Undefined
Description	
Location	

Figure 3–7: Hardware View

Click the port connector (leftmost port) to open the **Port Properties** dialog box (Figure 3–8).



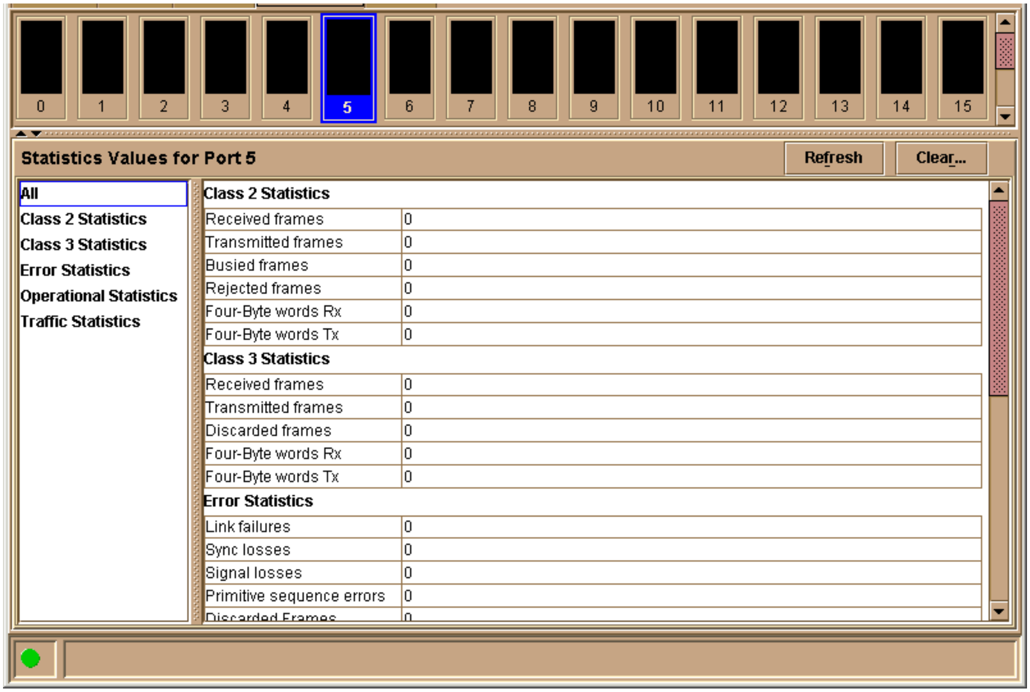
Port Number	0
Port Name	
Type	G_Port
Operating Speed	1 Gb/sec
Port WWN	McDATA-20:04:08:00:88:00:21:01
Block Configuration	Unblocked
LIN Alerts Configuration	On
FAN Configuration	Off
Beaconing	Off
Link Incident	None
Operational State ⚠	Offline
Reason	
Threshold Alert	

Figure 3–8: Port Properties Dialog Box

Refer to the *hp StorageWorks edge switch 2/24 product manager user guide* for an explanation of the **Hardware View** and **Port Properties dialog** box.

Performance View

The **Performance View** (Figure 3–9) displays statistical information about the performance of the ports. The information is useful for isolating port problems. To open the **Performance View** from the **Hardware View**, select **Performance** from the **View** menu on the navigation control panel.



Statistics Values for Port 5

Class 2 Statistics

Received frames	0
Transmitted frames	0
Busied frames	0
Rejected frames	0
Four-Byte words Rx	0
Four-Byte words Tx	0

Class 3 Statistics

Received frames	0
Transmitted frames	0
Discarded frames	0
Four-Byte words Rx	0
Four-Byte words Tx	0

Error Statistics

Link failures	0
Sync losses	0
Signal losses	0
Primitive sequence errors	0
Discarded Frames	0

Figure 3–9: Performance View

Refer to the *hp StorageWorks edge switch 2/24 product manager user guide* for an explanation of the **Performance View**.

Perform Loopback Tests

This section describes procedures to perform an:

- Internal loopback test - an internal loopback test checks internal port, serializer, and deserializer circuitry and checks for the presence of an optical transceiver, but does not check fiber-optic components of the installed transceiver. Operation of the attached device is disrupted during the test.
- **External loopback test -** an external loopback test checks all port circuitry, including fiber-optic components of the installed optical transceiver. To perform the test, the attached device must be quiesced and disconnected from the port, and a singlemode or multimode loopback plug must be inserted in the port.

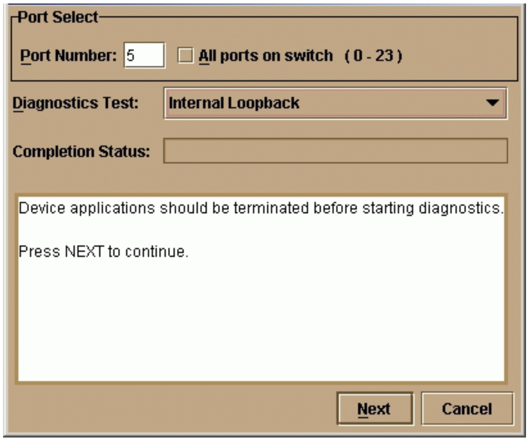
Internal Loopback Test

To perform an internal loopback test for a single port:

1. Notify the customer that a disruptive internal loopback test is to be performed on a port. Ensure the customer’s system administrator quiesces Fibre Channel frame traffic through the port and sets the attached devices offline.

NOTE: An SFP transceiver must be installed in the port during the test. A switch can remain attached during the test.

2. At the HAFM server, open the HAFM application. The **Product View** displays.
3. Select the icon representing the switch to be tested. The **Hardware View** for the selected switch displays.
4. At the **Hardware View**, verify the location of the port to be tested. When the mouse pointer is passed over the graphical port on the front view of the switch, the port highlights with a blue border and an pop-up displays Switch Port.
5. At the navigation control panel, select **Port Diagnostics** from the **Maintenance** menu. The **Port Diagnostics** dialog box displays (Figure 3–10).
6. Type the port number to be tested or select all ports at the **Port Select** area of the dialog box
7. At the **Diagnostics Test** list box, select **Internal Loopback**.



Port Number: 5 □ All ports on switch (0 - 23)

Diagnostics Test: Internal Loopback

Completion Status:

Device applications should be terminated before starting diagnostics.

Press NEXT to continue.

Figure 3–10: Port Diagnostics Dialog Box

8. Click **Next**. The message `Press START TEST to begin diagnostics` appears, and the **Next** button changes to a **Start Test** button.

9. Click **Start Test**. The test begins and:

   — The **Start Test** button changes to a **Stop Test** button

   — The message `Port xx: TEST RUNNING` appears.

   — A red progress bar (indicating percent completion) travels from left to right across the **Completion Status** field.

NOTE: Click **Stop Test** at any time to abort the loopback test.

10. When the test completes, results appear as `Port xx: Passed!` or `Port xx: Failed!` in the message area of the dialog box.

11. When finished, click **Cancel** to close the **Port Diagnostics** dialog box and return to the **Hardware View**.

12. Reset the port:

    a. At the **Hardware View**, right-click the port graphic. A pop-up menu appears.

    b. Select the **Reset Port** option. A message box displays, indicating a link reset operation will occur.

    c. Click **OK**. The port resets.

13. Notify the customer the test is complete and the attached device can be set online.

External Loopback Test

To perform an external loopback test for a single port:

1. Notify the customer that a disruptive external loopback test will be performed on a port and the fiber-optic cable or cables will be disconnected. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the port and sets attached devices offline.

NOTE: At the start of the loopback test, the port can be online, offline, blocked, or unblocked.

2. At the HAFM server, open the HAFM application. The **Product View** displays.
3. Select the icon representing the switch for which the loopback test is to be performed. The **Hardware View** for the selected switch displays.
4. At the **Hardware View**, verify the location of the port to be tested. When the mouse pointer is passed over the graphical port on the front view of the switch, the port highlights with a blue border and an pop-up displays Switch Port.
5. Disconnect the fiber-optic jumper cable from the port.
6. Depending on the port technology, insert a singlemode or multimode loopback plug into the port receptacle.
7. Select the **Port Diagnostics** option from the **Maintenance** menu. The **Port Diagnostics** dialog box displays (Figure 3–10).
8. Type the port number to be tested or select all ports at the **Port Select** area of the dialog box.
9. At the **Diagnostics Test** list box, select the **External Loopback** option.
10. Click **Next**. At the **Port Diagnostics** dialog box, the message `Loopback plug(s) must be installed on ports being diagnosed` appears.
11. Verify a loopback plug is installed and click **Next**. The message `Press START TEST to begin diagnostics` appears, and the **Next** button changes to a **Start Test** button.

12. Click **Start Test**. The test begins and:

    — The **Start Test** button changes to a **Stop Test** button

    — The message `Port xx: TEST RUNNING` appears.

    — A red progress bar (indicating percent completion) travels from left to right across the **Completion Status** field.

NOTE: Click **Stop Test** at any time to abort the loopback test.

13. When the test completes, results appear as `Port xx: Passed!` or `Port xx: Failed!` in the message area of the dialog box.
14. When finished, click **Cancel** to close the **Port Diagnostics** dialog box and return to the **Hardware View**.
15. Remove the loopback plug and reconnect the fiber-optic jumper cable from the device to the port.
16. Reset the port:

    a. At the **Hardware View**, right-click the port graphic. A pop-up menu appears.

    b. Select the **Reset Port** option. A message box displays, indicating a link reset operation will occur.

    c. Click **OK**. The port resets.

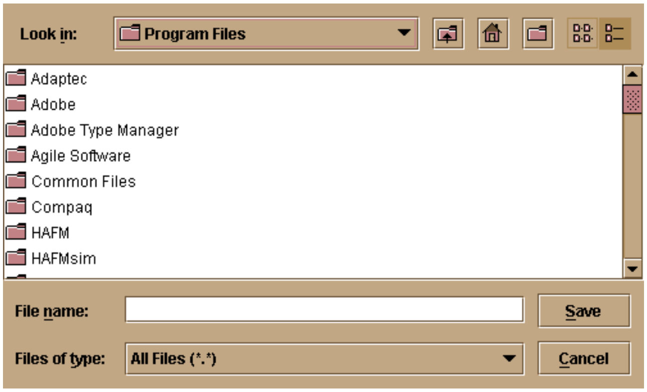
17. Notify the customer the test is complete and the device can be reconnected to the switch and set online.

Collecting Maintenance Data

When the switch operational firmware detects a critical error, the switch automatically copies the contents of dynamic random access memory (DRAM) to a dump area in FLASH memory on the CTP card, then transfers (through the Ethernet connection) the captured dump file from FLASH memory to the HAFM server hard drive.

Perform the maintenance data collection procedure after a firmware fault is corrected or a failed FRU is replaced to capture the data for analysis by third-level support personnel. Maintenance data includes the dump file, hardware log, audit log, and an engineering log viewable only by support personnel. To collect maintenance data:

1. At the HAFM server, open the HAFM application. The **Product View** displays.
2. Select the icon representing the switch for which the data collection procedure is to be performed. The **Hardware View** for the selected switch displays.
3. At the navigation control panel, select **Data Collection** from the **Maintenance** icon. The **Save Data Collection** dialog box (Figure 3–11) displays.



Look in: Program Files

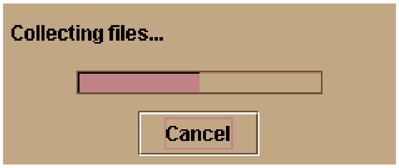
File name:

Files of type: All Files (*.*)

Figure 3–11: Save Data Collection Dialog Box

4. Remove the backup disk from the HAFM server Zip drive and insert a blank Zip disk.
5. At the **Save Data Collection** dialog box, select the zip drive (D:\) from the **Look in** drop-down menu, then type a descriptive name for the collected maintenance data in the **File name** field. Click **Save**.

6. A dialog box (Figure 3–12) displays with a progress bar that shows percent completion of the data collection process. When the process reaches 100%, the **Cancel** button changes to a **Close** button.



Collecting files...

Figure 3–12: Data Collection Status dialog box

7. Click **Close** to close the dialog box.

8. Remove the Zip disk with the newly-collected maintenance data from the HAFM server Zip drive. Return the Zip disk to Hewlett-Packard for failure analysis.

9. To ensure the QuikSync backup application operates normally, replace the original backup disk in the HAFM server Zip drive.

Set the Switch Online or Offline

This section describes procedures to set the switch online or offline. These 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 switch ports are set offline. The switch transmits the offline sequence (OLS) to attached devices, and the devices cannot log in to the switch.

NOTE: When the switch is set offline, the operation of attached Fibre Channel devices is disrupted. Do not set the switch offline unless directed to do so by a procedural step or the next level of support.

Set Online State

To set the switch online:

1. At the HAFM server, open the HAFM application. The **Product View** displays.
2. Select the icon representing the switch to be set online. The **Hardware View** for the selected switch displays.

3. At the navigation control panel, select **Set Online State** from the **Maintenance** menu. If the switch is offline, the **Set Online State** dialog box displays, indicating the state is OFFLINE.

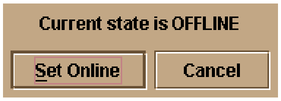

Current state is OFFLINE

Figure 3–13: Set Online Warning dialog box

4. Click **Set Online**. A **Warning** dialog box displays, indicating the switch is to be set online.
5. Click **OK**. As the switch comes online, inspect the Product Manager application. The **State** field of the **Status** table displays Online.

Set Offline State

To set the switch offline:

1. Notify the customer the switch is to be set offline. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the switch and sets attached devices offline.
2. At the HAFM server, open the HAFM application. The **Product View** displays.
3. Select the icon representing the switch to be set offline. The **Hardware View** for the selected switch displays.
4. At the navigation control panel, select **Set Online State** from the **Maintenance** menu. If the switch is online, the **Set Online State** dialog box displays, indicating the state is ONLINE.

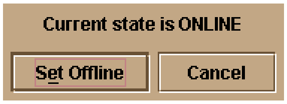

Current state is ONLINE

Figure 3–14: Set Offline Warning dialog box

5. Click **Set Offline**. A **Warning** dialog box displays, indicating the switch is to be set offline.
6. Click **OK**. As the switch goes offline, inspect the Product Manager application. The **State** field of the **Status** table displays OFFLINE.

Block and Unblock Ports

This section describes procedures to block or unblock the switch Fibre Channel ports. Blocking a port prevents the attached device or fabric switch from communicating. A blocked port continuously transmits the offline sequence (OLS).

NOTE: When a port is blocked, the operation of an attached Fibre Channel device is disrupted. Do not block a port unless directed to do so by a procedural step or the next level of support.

Block a Port

To block a port:

1. Notify the customer the port is to be blocked. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the port.
2. At the HAFM server, open the HAFM application. The **Product View** displays.
3. Select the icon representing the switch with the port to be blocked. The **Hardware View** for the selected switch displays.
4. Move the pointer over the port and right-click the mouse to open a list of menus.
5. Select **Block Port**. The **Block Port *n*** dialog box displays (*n* is the port number).

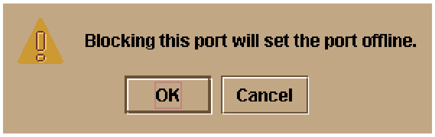

Blocking this port will set the port offline.

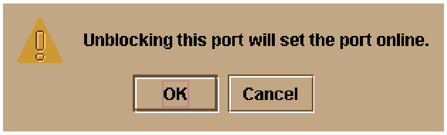
Figure 3–15: Block Port dialog box

6. Click **OK**. The following occur to indicate the port is blocked (and offline):
   - — The emulated green LED associated with the port extinguishes at the **Hardware View**.
   - — The green LED associated with the port extinguishes at the switch.
   - — A check mark displays in the check box adjacent to the **Block Port** menu option.

Unblock a Port

To unblock a port:

1. At the HAFM server, open the HAFM application. The **Product View** displays.
2. Select the icon representing the switch with the port to be unblocked. The **Hardware View** for the selected switch displays.
3. Move the pointer over the port and right-click the mouse to open a list of menus options.
4. Select **Block Port**. Note the check mark in the box adjacent to the menu item, indicating the port is blocked. The **Unblock Port *n*** dialog box displays (*n* is the port number).



Unblocking this port will set the port online.

Figure 3–16: Unblock Port dialog box

5. Click **OK**. The following occur to indicate the port is unblocked (and online):

   — The emulated green LED associated with the port illuminates at the **Hardware View**.

   — The green LED associated with the port illuminates at the switch.

   — The check box adjacent to the **Block Port** menu option becomes blank.

Clean Fiber-Optic Components

Perform this procedure as directed in this publication and when connecting or disconnecting fiber-optic cables from port optical transceivers (if necessary). To clean fiber-optic components:

1. Obtain the appropriate tools (portable can of oil-free compressed air and alcohol pads) from the fiber-optic cleaning kit.
2. Disconnect the fiber-optic cable from the transceiver. Use compressed air to blow any contaminants from the connector as shown in part A of Figure 3–17.

   — Keep the air nozzle approximately 50 millimeters (two inches) from the end of the connector and hold the can upright.

   — Blow compressed air on the surfaces and end of the connector continuously for approximately five seconds.

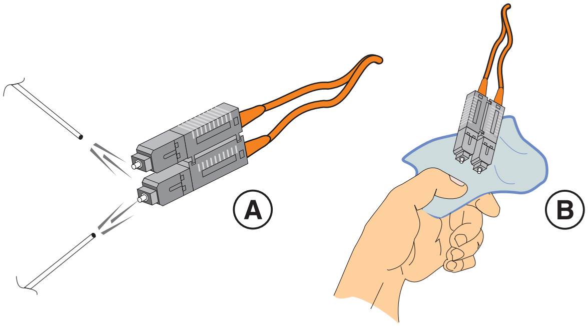


Figure 3–17: Clean Fiber-Optic Components

3. Gently wipe the end-face and other surfaces of the connector with an alcohol pad as shown in part B of Figure 3–17. Ensure the pad makes full contact with the surface to be cleaned. Wait approximately five seconds for surfaces to dry.
4. Repeat step 2 and step 3 of this procedure (second cleaning).
5. Repeat step 2 and step 3 of this procedure again (third cleaning), then reconnect the fiber-optic cable to the port.

Power-On Procedure

To power-on the switch:

1. One alternating current (AC) power cord is required for each power supply. Ensure power cord(s) are available to connect the switch to facility power.

WARNING: A Hewlett-Packard-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 cord(s), and ensure the facility power receptacle is the correct type, supplies the required voltage, and is properly grounded.

2. Plug the power cord(s) into facility power sources and power supply AC connectors at the rear of the switch. When the first power cord is connected, the switch powers on and performs power-on self-tests (POSTs).

3. During POSTs:

   - The green power (**PWR**) LED on the switch front panel illuminates.
   - The amber system error (**ERR**) LED on the switch front panel blinks momentarily while the switch is tested.
   - The green LEDs associated with the Ethernet port blink momentarily while the port is tested.
   - The blue/green and amber LEDs associated with the ports blink momentarily while the ports are tested.

1. After successful POST completion, the green power (PWR) LED remains illuminated and all amber LEDs extinguish.

2. If a POST error or other malfunction occurs, go to MAP 0000: Start MAP on page 2–6 to isolate the problem.

Power-Off Procedure

To power-off the switch:

1. Notify the customer the switch is to be powered off. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the switch and sets attached devices offline.
2. Set the switch offline (Set Offline State on page 3–24).
3. Disconnect power cord(s) from the power supply AC connectors at the rear of the switch.

IML, IPL or Reset the Switch

This section describes procedures to IML, IPL, or reset the Edge Switch 2/24. An IML or reset is performed at the switch front panel using the **IML/RESET** button. An IPL is performed from the HAFM server (Product Manager application). The EWS interface does not provide an IML, IPL, or switch reset function.

An IML and IPL are functionally equivalent. The operations do not cause power-on diagnostics to execute and are not disruptive to Fibre Channel traffic. Both operations:

- Reload switch firmware from FLASH memory.
- Reset the Ethernet LAN interface, causing the connection to the HAFM server to drop momentarily until the connection automatically recovers.

A switch reset is more 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.

△ **CAUTION:** A reset should only be performed if a CTP card failure is indicated. Do not reset the switch unless directed to do so by a procedural step or the next level of support.

Switch IML

To IML the switch from the front panel:

1. Press and hold the **IML/RESET** button until the amber **ERR** LED blinks at twice the unit beaoning rate (approximately three seconds).
2. Release the button to IML the switch. During the IML, the switch-to-HAFM server Ethernet link drops momentarily and the following occur at the **Hardware View**:
   - As the network connection drops, the status table turns yellow, the **Status** field displays `No Link`, and the **State** field displays `Link Timeout`.
   - The status bar at the bottom of the window displays a grey square, indicating switch status is unknown.
   - Illustrated FRUs disappear, and appear again as the connection is re-established.

Switch IPL

To IPL the switch from the HAFM server (Edge Switch 2/24 Product Manager application):

1. At the HAFM server, open the HAFM application. The **Products View** displays.
2. Select (double-click) the icon representing the switch requiring an IPL. The **Hardware View** for the selected switch displays.
3. Select the **IPL** option from the **Maintenance** menu. An **Information** dialog box displays.
4. Click **Yes** to IPL the switch. During the IPL, the switch-to-HAFM server Ethernet link drops momentarily and the following occur at the **Hardware View**:
   - As the network connection drops, the status table turns yellow, the **Status** field displays `No Link`, and the **State** field displays `Link Timeout`.
   - The status bar at the bottom of the window displays a grey square, indicating switch status is unknown.
   - Illustrated FRUs disappear, and appear again as the connection is re-established.

Switch Reset

To reset the switch from the front panel:

1. Press and hold the **IML/RESET** button for approximately ten seconds.
   - After holding the button for three seconds, the amber **ERR** LED blinks at twice the unit beaoning rate.
   - After holding the button for ten seconds, the **ERR** LED stops blinking, and all front panel LEDs illuminate.
2. Release the button to reset the switch. During the reset:
   - The green power (**PWR**) LED on the switch front panel illuminates.
   - The amber system error (**ERR**) LED on the switch front panel blinks momentarily while the switch is tested.
   - The green LEDs associated with the Ethernet port blink momentarily while the port is tested.
   - The blue/green and amber LEDs associated with the ports blink momentarily while the ports are tested.
   - The switch-to-HAFM server Ethernet link drops momentarily and the following occur at the **Hardware View**:
     - As the network connection drops, the status table turns yellow, the **Status** field displays `No Link`, and the **State** field displays `Link Timeout`.
     - The status bar at the bottom of the window displays a grey square, indicating switch status is unknown.
     - Illustrated FRUs disappear, and appear again as the connection is re-established.

Manage Firmware Versions

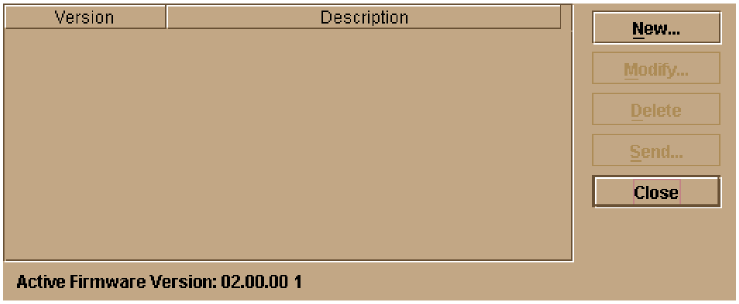
Firmware is the internal operating code stored in FLASH memory on the the switch's CTP card. Up to eight versions can be stored on the HAFM server hard drive and made available for download to a switch. Service personnel can perform the following firmware management tasks:

- Determine the firmware version active on a switch.
- Add to and maintain a library of up to eight firmware versions on the HAFM server hard drive.
- Download a firmware version to a selected switch.

Determine a Switch Firmware Version

To determine a switch firmware version:

1. At the HAFM server, open the HAFM application. The **Product View** displays.
2. Select the icon representing the switch to be inspected for firmware version. The **Hardware View** for the selected switch displays.
3. At the navigation control panel, select **Firmware Library** from the **Maintenance** menu. The **Firmware Library** dialog box displays.



Active Firmware Version: 02.00.00 1

Figure 3–18: Firmware Library dialog box

4. The firmware version displays at the lower left corner of the dialog box in XX.YY.ZZ format, where XX is the version level, YY is the release level, and ZZ is the patch level.
5. Click **Close** to return to the **Hardware View**.

Add a Firmware Version

The firmware version shipped with the switch is provided on the Edge Switch 2/24 documentation kit CD. Subsequent firmware versions for upgrading the switch are provided to customers through the HP website.

NOTE: When adding a firmware version, follow all the instructions in the release notes that accompany the firmware version. This information supplements information in this general procedure.

To add a switch firmware version to the library stored on the HAFM server hard drive:

1. Obtain the new firmware version from the HP website:

NOTE: The following path is subject to change.

   a. At the HAFM server or other personal computer (PC) with Internet access, open the HP website. The uniform resource locator (URL) is:

      http://thenew.hp.com/country/us/eng/support.html

   b. Follow links to the Edge Switch 2/24 firmware.

   c. Click the Edge Switch 2/24 Firmware Version XX.YY.ZZ entry, where XX.YY.ZZ is the desired version. The **Windows Save As** dialog box appears.

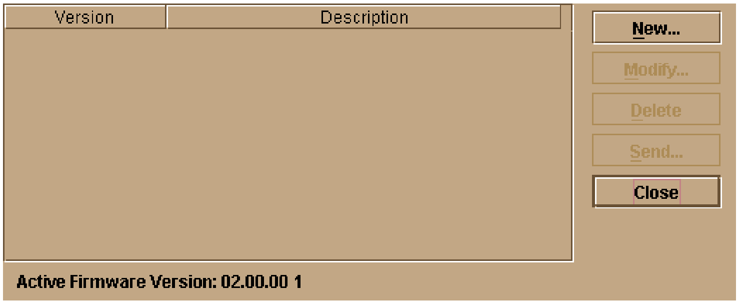
   d. Ensure the correct directory path is specified at the **Save** in field and the correct file is specified in the **File name** field. Click **Save**. The new firmware version is downloaded and saved to the HAFM server or PC hard drive.

   e. If the new firmware version was downloaded to a PC (not the HAFM server), transfer the firmware version file to the HAFM server by CD-ROM or other electronic means.

2. At the HAFM server, open the HAFM application. The **Product View** displays.

3. Select the icon representing the switch for which a firmware version is to be added. The **Hardware View** for the selected switch displays.

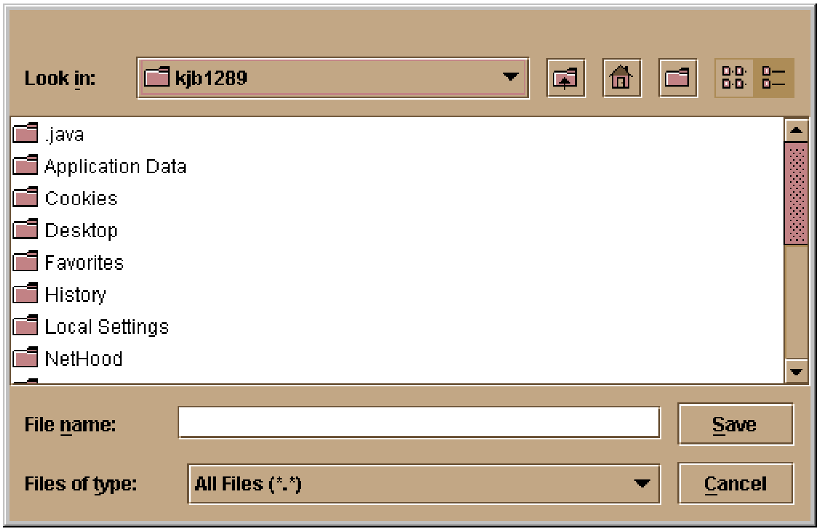
4. At the navigation control panel, select **Firmware Library** from the **Maintenance** menu. The **Firmware Library** dialog box displays.



Active Firmware Version: 02.00.00 1

Figure 3–19: Firmware Library dialog box

5. Click **New**. The **New Firmware Version** dialog box displays.



Look in: kjb1289

File name:

Files of type: All Files (*.*)

Figure 3–20: New Firmware Version dialog box

6. Select the desired firmware version file (downloaded in step 1) from the HAFM server CD-ROM or hard drive. Ensure the correct directory path and filename appear in the **File name** field and click **Save**.

The **New Firmware Description** dialog box displays.

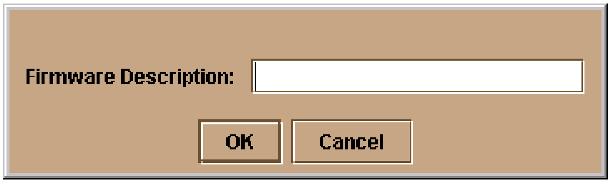


Figure 3–21: Firmware Description dialog box

7. Enter a description (up to 24 characters) for the new firmware version and click **OK**. The description should include the installation date and text that uniquely identify the firmware version.
8. A **Transfer Complete** message box appears indicating the new firmware version is stored on the HAFM server hard drive. Click **Close** to close the message box.
9. The new firmware version and associated description appear in the **Firmware Library** dialog box. Click **Close** to close the dialog box and return to the Product Manager application.
10. To send the firmware version to a switch, refer to Download a Firmware Version to a Switch on page 3–35.

Download a Firmware Version to a Switch

This procedure downloads a selected firmware version from the HAFM server library to a switch managed by the open instance of the Product Manager application.

NOTE: When downloading a firmware version, follow all procedural information in the release notes or EC instructions that accompany the firmware version. This information supplements information in this general procedure.

To download a firmware version to a switch:

1. Notify the customer that a firmware version is to be downloaded to the switch. The switch resets during the firmware download, causing Fibre Channel links to momentarily drop and attached devices to log out and log back in. Data frames lost during switch reset must be retransmitted.
2. At the HAFM server, open the HAFM application. The **Product View** displays.

3. Before downloading firmware version XX.YY.ZZ to a switch, ensure version XX.YY.ZZ or higher of the HAFM application is running on the HAFM server.

   a. Select **About** from the **Help** menu. The **About** dialog box displays the HAFM application version. Click **OK** to close the dialog box.

   b. If required, install the correct version of the HAFM application (Install or Upgrade Software on page 3–42).

4. Select the icon representing the switch for which a firmware version is to be downloaded. The **Hardware View** for the selected switch displays.

5. As a precaution to preserve switch configuration information, perform the data collection procedure (Collecting Maintenance Data on page 3–22).

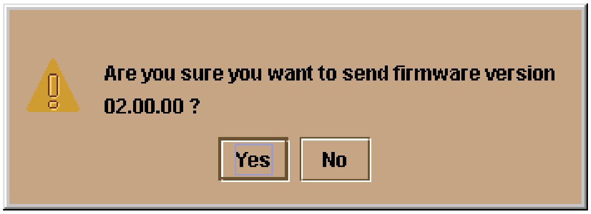
6. At the navigation control panel, select **Firmware Library** from the **Maintenance** menu. The **Firmware Library** dialog box displays.

7. Select the firmware version to be downloaded and click **Send**. The send function verifies existence of certain switch conditions before the download begins. If an error occurs, a message displays indicating the problem must be fixed before the firmware download. Conditions that terminate the process include:

   — The firmware version is being installed to the switch by another user.

   — The switch-to-HAFM server link fails or times out.

   If a problem occurs and a corresponding message displays, go to MAP 0000: Start MAP on page 2–6 to isolate the problem. If no error occurs, the **Send Firmware** confirmation box displays.



Are you sure you want to send firmware version 02.00.00 ?

Figure 3–22: Send Firmware confirmation dialog box

8. Click **Yes**. The **Send Firmware** dialog box displays.

As the download begins, a `Sending Files` message displays at the top of the dialog box. This message remains for a few moments as a progress bar travels across the dialog box to show percent completion of the download. As the download progresses, a `Writing data to FLASH` message displays. This message remains as the progress bar continues to travel across the dialog box. The bar progresses to 100% when the last file is transmitted to the CTP card. The switch then performs an IPL, during which the switch-to-HAFM server link drops momentarily and the following occur at the Product Manager application:

- — As the network connection drops, the **Status** table turns yellow, the **Status** field displays `No Link`, and the **State** field displays a reason message.
- — The alert panel at the bottom of the navigation control panel displays a grey square, indicating switch status is unknown.
- — Illustrated FRUs in the **Hardware View** disappear, and appear again as the connection is re-established.

After the IPL, a `Send firmware complete` message displays as shown below.

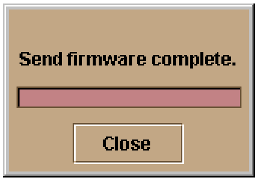

Send firmware complete.

Figure 3–23: Send Firmware Complete message

9. Click **Close** to close the dialog box.
10. Click **Close** to close the **Firmware Library** dialog box and return to the **Hardware View.**

Manage Configuration Data

The Product Manager application provides maintenance options to back up, restore, or reset the configuration file stored in nonvolatile random-access memory (NV-RAM) on the switch CTP card. Configuration data in the file include:

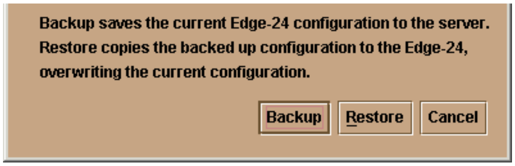
- Switch identification data.
- Port configuration data.
- Switch and fabric operating parameters.
- Simple network management protocol (SNMP) configuration information.
- Zoning configuration information.

Back Up the Configuration

NOTE: The ability to back up configuration data may not exist if the user has a customer-supplied server platform for the HAFM application. The server platform must have Iomega® QuikSync and a Zip drive.

To back up the switch configuration file to the HAFM server (c:\HafmData):

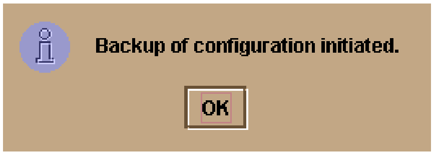
1. At the HAFM server, open the HAFM application. The **Product View** displays.
2. Select the icon representing the switch for which a configuration file is to be backed up. The **Hardware View** for the selected switch displays.
3. At the navigation control panel, select **Backup & Restore Configuration** from the **Maintenance** menu. The **Backup and Restore Configuration** dialog box displays.



Backup saves the current Edge-24 configuration to the server. Restore copies the backed up configuration to the Edge-24, overwriting the current configuration.

Figure 3–24: Backup and Restore Configuration dialog box

4. Click **Backup**. When the backup process finishes, the **Backup Complete** message displays.



Backup of configuration initiated.

Figure 3–25: Backup Complete message

5. Click **OK** to close the dialog box and return to the **Hardware View**.

Restore the Configuration

To restore the switch configuration file from the HAFM server:

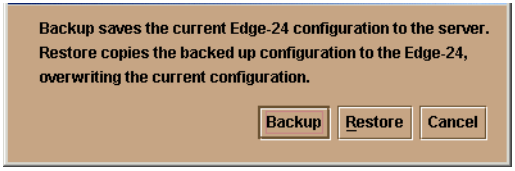
1. Notify the customer that the switch is to be set offline. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the switch and sets attached devices offline.

2. Set the switch offline (Set Offline State on page 3–24).

3. At the HAFM server, open the HAFM application. The **Product View** displays.

4. Select the icon representing the switch for which a configuration file is to be restored. The **Hardware View** for the selected switch displays.

5. At the navigation control panel, select **Backup & Restore Configuration** from the **Maintenance** menu. The **Backup and Restore Configuration** dialog box displays.

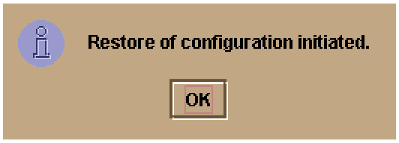


Backup saves the current Edge-24 configuration to the server. Restore copies the backed up configuration to the Edge-24, overwriting the current configuration.

Figure 3–26: Backup and Restore Configuration dialog box

6. Click **Restore**. A **Warning** message box displays.

7. Click **Yes**. When the restore process finishes, the **Restore Complete** message displays.



Restore of configuration initiated.

Figure 3–27: Restore Complete message

8. Click **OK** to close the dialog box and return to the **Hardware View**.

Reset Configuration Data

NOTE: This procedure resets the switch IP address to the default of 10.1.1.10 and may disrupt server-to-switch communication. All optional features are disabled.

To reset the switch data to the factory default settings:

1. Notify the customer the switch is to be set offline. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the switch and sets attached devices offline.

2. Set the switch offline (Set Offline State on page 3–24).

3. At the HAFM server, open the HAFM application. The **Product View** displays.

4. Select the icon representing the switch for which a configuration file is to be reset to factory default settings. The **Hardware View** for the selected switch displays.

5. At the navigation control panel, select **Reset Configuration** from the **Maintenance** menu. The **Reset Configuration** dialog box displays.

6. Click **Reset**. When the reset process finishes, the dialog box closes and the application returns to the **Hardware View**.

7. The switch IP address resets to the default address of `10.1.1.10`.

   — If the configured IP address (prior to reset) was the same as the default address, the switch-to-HAFM server Ethernet link is not affected and the procedure is complete.

   — If the configured IP address (prior to reset) was not the same as the default address, the switch-to-HAFM server Ethernet link drops and HAFM server communication is lost. Continue to the next step.

8. To change the switch IP address and restart the HAFM server session, go to step 10.
9. To restart an HAFM server session using the default IP address of **10.1.1.10**:

    a. Close the Edge Switch 2/24 Product Manager application and return to the **Products View**.

    b. The icon representing the reset switch displays a grey square in the background, indicating switch is not communicating with the HAFM server. Right-click the icon. A pop-up menu appears.

    c. Select the **Modify** option. The **Modify Network Address** dialog box displays.

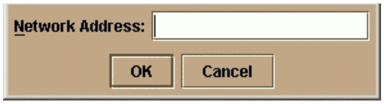


Figure 3–28: Modify Network Address dialog box

    d. Type `10.1.1.10` in the **Network Address** field and click **OK**. Switch-to-HAFM server communication is restored and the procedure is complete.

10. Change the switch IP address and restart the HAFM server session as follows:

    a. Delete the icon representing the reset switch. The icon displays a grey square in the background, indicating switch is not communicating with the HAFM server. Right-click the icon. A pop-up menu appears.

    b. Select the **Delete** option. An **Product Delete Confirmation** message displays, confirming deletion of the product.

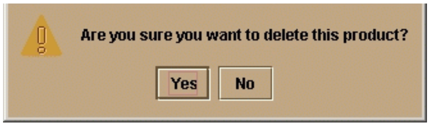

Are you sure you want to delete this product?

Figure 3–29: Product Delete Confirmation message

    c. Click **Yes** to delete the icon representing the reset switch.

    d. Change a switch’s IP address through the maintenance port at the rear of the switch. Refer to the *hp StorageWorks edge switch 2/24 installation guide* for information on configuring switch network information.

e. Identify the switch to the HAFM application. Refer to the *hp StorageWorks edge switch 2/24 installation guide* for information on identifying the switch to the HAFM application

f. Switch-to-HAFM server communication is restored and the procedure is complete.

Install or Upgrade Software

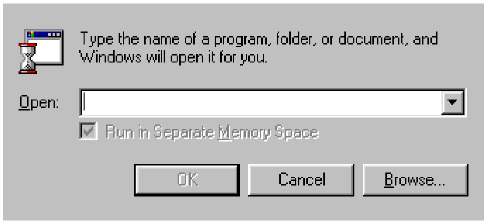
This section describes the procedure to install or upgrade the HAFM application to the HAFM server. The HAFM application includes the switch Product Manager and HAFM services applications.

The HAFM application shipped with the switch is provided on the HAFM Applications CD-ROM. Subsequent software versions for upgrading the switch are provided to customers through the HAFM Applications CD-ROM or through Hewlett-Packard's home page.

NOTE: When installing or upgrading a software version, follow all procedural information in the release notes or instructions that accompany the software version. This information supplements information in this general procedure.

To install or upgrade the HAFM application and associated applications to the HAFM server:

1. Log out of all HAFM application sessions (local and remote) and exit the HAFM application.
2. Insert the HAFM Applications CD-ROM into the CD-ROM drive of the HAFM server.
3. At the HAFM server, click **Start** at the Windows task bar. The **Windows Workstation** menu displays.
4. At the **Windows Workstation** menu, select **Run**. The **Run** dialog box appears.



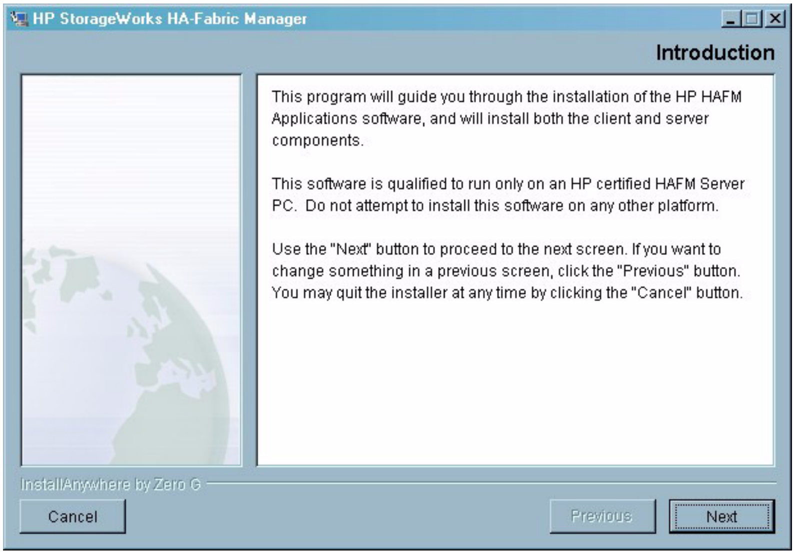
Type the name of a program, folder, or document, and Windows will open it for you.

Open:

☑ Run in Separate Memory Space

Figure 3–30: Windows Run dialog box

5. At the **Run** dialog box, select directory path (hard drive or CD-ROM drive) and filename of the executable file (`HAFM_ServerInstall.exe`) using the **Browse** button. The directory path and filename display in the **Open** field.
6. Click **OK**. A series of message boxes appear as the InstallAnywhere third-party application prepares to install the HAFM application software, followed by the **HAFM** dialog box.



This program will guide you through the installation of the HP HAFM Applications software, and will install both the client and server components.

This software is qualified to run only on an HP certified HAFM Server PC. Do not attempt to install this software on any other platform.

Use the "Next" button to proceed to the next screen. If you want to change something in a previous screen, click the "Previous" button. You may quit the installer at any time by clicking the "Cancel" button.

Figure 3–31: HAFM Install dialog box

7. Follow the online instructions for the InstallAnywhere program. Click **Next**, **Install**, or **Done** as appropriate.
8. Power off and reboot the HAFM server PC.
   a. Simultaneously press **Ctrl**, **Alt**, and **Delete** to display the **Windows Logon Information** dialog box.
   b. Type a user name and password and click **OK**. The Windows desktop displays.

NOTE: If required, obtain the user name and password from the customer or next level of support.

9. The HAFM application automatically opens. At the HAFM splash screen, enter a user name, password, and HAFM server name (all are case sensitive), and click **Login**. The application opens and the **Product View** displays.

NOTE: If required, obtain the user name, password, and HAFM server name from the customer or next level of support.

4

FRU Removal and Replacement

This chapter describes the removal and replacement procedures (RRPs) for the HP StorageWorks Edge Switch 2/24 field-replaceable units (FRUs). Do not remove a FRU until a failure is isolated to that FRU. If fault isolation was not performed, see MAP 0000: Start MAP on page 2–6.

Procedural Notes

Note the following:

1. Read the removal and replacement procedures (RRPs) for that FRU before removing the FRU.
2. Follow all **WARNING** and **CAUTION** statements and statements in the preface of this manual.
3. After completing a FRU replacement, clear the event code reporting the failure and the event code reporting the recovery from the switch **Event Log** (at the HAFM server). Extinguish the amber system error (**ERR**) light-emitting diode (LED) at the switch front panel.

Remove and Replace FRUs

This section describes procedures to remove and replace concurrent switch FRUs, along with tools required to perform each procedure. Concurrent FRUs are removed and replaced while the switch is powered on and operational.

Table 4–1 lists concurrent FRUs that are removed and replaced while the switch is powered on and operational. The table also lists ESD precautions (yes or no) for each FRU, and references the page number of the removal and replacement procedure.

Table 4–1: Concurrent FRUs

Concurrent FRU Name	ESD Precaution Requirement	Page
Small form factor pluggable (SFP) optical transceiver	No	4-2
Redundant power supply (with internal cooling fans)	No	4-5

RRP 1: SFP Optical Transceiver

Use the following procedures to remove or replace an SFP optical transceiver from the front of the switch chassis. A list of tools required is provided.

Tools Required

The following tools are required to perform these procedures.

- Protective cap (provided with the fiber-optic jumper cable).
- Loopback plug (provided with the switch).
- Fiber-optic cleaning kit.

Removal

To remove an SFP optical transceiver:

1. Notify the customer that the port with the defective transceiver will be blocked. Ensure the customer's system administrator sets the attached device offline.
2. Identify the defective port transceiver from:
   — The illuminated amber LED adjacent to the port.

   — At the EWS interface, failure information associated with the port at the **Port Properties** page of the **View** panel.

   — At the HAFM server, failure information associated with the port at the **Hardware View**, **Port List View**, or **Port Properties** dialog box.
3. Block communication to the port (Block and Unblock Ports on page 3–25).

4. Disconnect the fiber-optic jumper cable from the port:
    a. Pull the keyed LC connector free from the port's optical transceiver.
    b. Place a protective cap over the jumper cable connector.
5. The optical transceiver has a wire locking bale to secure the transceiver in the port receptacle and to assist in removal. The locking bale rotates up or down, depending on the transceiver manufacturer and port location (top row, odd-numbered ports **1** through **23**, or bottom row even-numbered ports **0** through **22**).
    a. Disengage the locking mechanism by rotating the wire locking bale up or down 90 degrees.
    b. Grasp the wire locking bale and pull the transceiver from the port receptacle.
6. Perform one of the following to inspect the **Event Log**:
    — If at a web browser connected to the EWS interface, click the **Log** tab at the **Monitor** panel. The **Event Log** displays. An event code **513** (SFP optics hot-removal completed) appears in the log.
    — If at the HAFM server, open the **Hardware View**, click **Logs**, and select **Event Log**. The **Event Log** displays. An event code **513** (SFP optics hot-removal completed) appears in the log.

Replacement

To replace an SFP optical transceiver:

1. Remove the replacement transceiver from its packaging.
2. Insert the transceiver into the port receptacle, then engage the locking mechanism by rotating the wire locking bale up or down 90 degrees.
3. Perform an external loopback test on the port. Refer to Perform Loopback Tests on page 3–18 for instructions. If the test fails, go to MAP 0000: Start MAP on page 2–6 to isolate the problem.
4. Reconnect the fiber-optic jumper cable:
    a. Remove the protective cap from the cable connector and the protective plug from the port's optical transceiver. Store the cap and plug in a suitable location for safekeeping.

b. Clean the jumper cable and transceiver connectors. Refer to Clean Fiber-Optic Components on page 3–27 for instructions.

c. Insert the keyed LC cable connector into the port's optical transceiver.

5. Ensure the amber LED adjacent to the port transceiver is extinguished. If the amber LEDs is illuminated, go to MAP 0000: Start MAP on page 2–6 to isolate the problem.

6. Perform one of the following to inspect the **Event Log**:

— If at a web browser connected to the EWS interface, click the **Log** tab at the **Monitor** panel. The **Event Log** displays. Ensure an event code **510** (SFP optics hot-insertion initiated) appears. If the event code does not appear in the log, go to MAP 0000: Start MAP on page 2–6 to isolate the problem.

— If at the HAFM server, open the **Hardware View**, click **Logs**, and select **Event Log**. The **Event Log** displays. Ensure an event code **510** (SFP optics hot-insertion initiated) appears. If the event code does not appear in the log, go to MAP 0000: Start MAP on page 2–6 to isolate the problem.

7. Perform one of the following to verify port operation:

If at a web browser connected to the EWS interface, open the **Switch** tab at the **View** panel and:

a. Ensure no amber LEDs illuminate that indicate a port failure.

b. Click the graphic representing the port with the replacement transceiver to open the **Port Properties** tab. Verify port and port technology information is correct.

c. If a problem is indicated, go to MAP 0000: Start MAP on page 2–6 to isolate the problem.

If at the HAFM server, open the **Hardware View** and:

a. Ensure no alert symbols appear that indicate a port failure (yellow triangle or red diamond).

b. Double-click the graphic representing the port with the replacement transceiver to open the **Port Properties** dialog box. Verify port information is correct.

c. Right-click the graphic representing the port with the replacement transceiver and select **Port Technology** from the menu. The **Port Technology** dialog box displays. Verify port technology information is correct.

d. If a problem is indicated, go to MAP 0000: Start MAP on page 2–6 to isolate the problem.

8. Restore communication to the port with the replacement transceiver as directed by the customer. Refer to Block and Unblock Ports on page 3–25 for instructions. Inform the customer the port is available.

9. Perform one of the following to clear the system error (**ERR**) LED on the switch front bezel:

— If at a web browser connected to the EWS interface, click the **Log** tab at the **Monitor** panel. The **Event Log** displays. Click **Clear System Error Light**.

— If at the HAFM server, open the **Hardware View**, right-click the front panel bezel graphic (away from a FRU) to open a menu. Click the **Clear System Error Light** menu selection.

RRP 2: Redundant Power Supply

Use the following procedures to remove or replace a redundant power supply (with internal cooling fans) from the rear of the switch chassis.

Removal

To remove a redundant power supply:

1. Identify the defective power supply from:

— The illuminated amber LED on the FRU.

— At the EWS interface, failure information associated with the power supply at the **FRU Properties** page of the **View** panel.

— At the HAFM server, failure information associated with the power supply at the **Hardware View** or **FRU List View**.

2. Disconnect the AC power cord from the power supply.

3. Disengage and remove the power supply as follows:

a. Disengage the locking mechanism by rotating both finger handles outward by 90 degrees as shown in part (A) of Figure 4–1.

b. Use the finger handles to pull the power supply out of the switch chassis as shown in part (B) of Figure 4–1. Support the power supply as it is pulled from the chassis.

⚠ **WARNING: To prevent electric shock, do not reach into nonvisible areas of a Edge Switch 2/24 connected to primary facility power.**

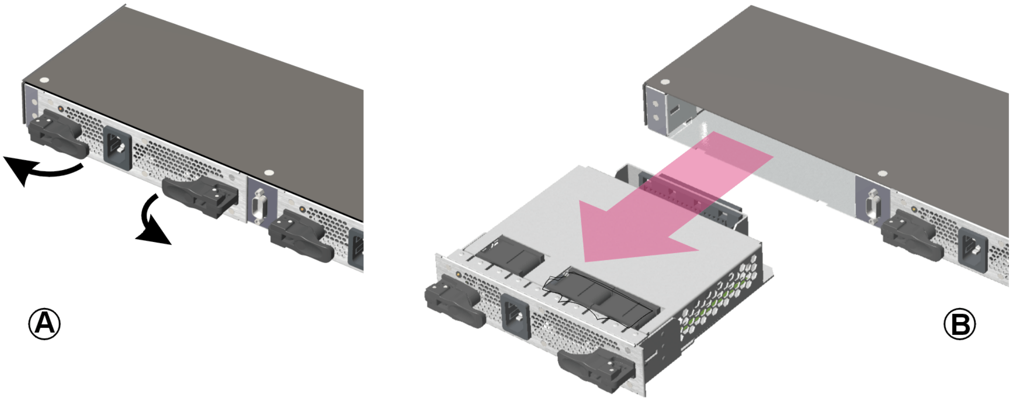


Figure 4–1: Redundant power supply removal and replacement

4. Perform one of the following to inspect the **Event Log**. Note that multiple events appear because the power supply contains three internal cooling fans.

   If at a web browser connected to the EWS interface, click the **Log** tab at the **Monitor** panel. The **Event Log** displays. The following event codes appear:

   — **200 -** Power supply AC voltage failure (recorded when AC power is disconnected).

   — **300 -** A cooling fan propeller has failed (first fan).

   — **301 -** A cooling fan propeller has failed (second fan).

   — **302 -** A cooling fan propeller has failed (third fan).

   — **206 -** Power supply removed.

If at the HAFM server, open the **Hardware View**, click **Logs**, and select **Event Log**. The **Event Log** displays. The **Event Log** displays. The following event codes appear:

- **200 -** Power supply AC voltage failure (recorded when AC power is disconnected).
- **300 -** A cooling fan propeller has failed (first fan).
- **301 -** A cooling fan propeller has failed (second fan).
- **302 -** A cooling fan propeller has failed (third fan).
- **206 -** Power supply removed.

Replacement

To replace a redundant power supply:

1. Remove the replacement power supply from its shipping container.
2. Inspect the rear of the power supply for bent or broken connector pins that may have been damaged during shipping. If any pins are damaged, obtain a new power supply.
3. Position the power supply in the rear of the switch chassis as shown in part (B) of Figure 4–1. Ensure the finger handles are disengaged and rotated 90 degrees outward.
   a. While supporting the power supply with one hand, insert it into the switch chassis.
   b. Firmly push the power supply into the chassis. Rotate the finger handles 90 degrees inward to seat the power supply and engage the connector pins. Ensure the faceplate is flush with the chassis cutout.
4. Connect the AC power cord to the power supply and to a facility power source.
5. Wait several seconds, then inspect the power supply to ensure the amber LED is extinguished. If the LED is illuminated, go to MAP 0000: Start MAP on page 2–6 to isolate the problem.
6. Perform one of the following to inspect the **Event Log**:

If at a web browser connected to the EWS interface, click the **Log** tab at the **Monitor** panel. The **Event Log** displays. Ensure the following event codes appear. If the event codes do not appear, go to MAP 0000: Start MAP on page 2–6 to isolate the problem.

— **207 -** Power supply installed.

— **313 -** A cooling fan propeller has recovered (first fan).

— **314 -** A cooling fan propeller has recovered (second fan).

— **315 -** A cooling fan propeller has recovered (third fan).

— **203 -** Power supply AC voltage recovery.

If at the HAFM server, open the **Hardware View**, click **Logs**, and select **Event Log**. The **Event Log** displays. Ensure the following event codes appear. If the event codes do not appear, go to MAP 0000: Start MAP on page 2–6 to isolate the problem.

— **207 -** Power supply installed.

— **313 -** A cooling fan propeller has recovered (first fan).

— **314 -** A cooling fan propeller has recovered (second fan).

— **315 -** A cooling fan propeller has recovered (third fan).

— **203 -** Power supply AC voltage recovery.

7. Perform one of the following to verify power supply operation:

   — If at a web browser connected to the EWS interface, open the **Switch** tab at the **View** panel and ensure no amber LEDs illuminate that indicate a power supply failure. If a problem is indicated, go to MAP 0000: Start MAP on page 2–6 to isolate the problem.

   — If at the HAFM server, open the **Hardware View** and observe the power supply graphic to ensure no alert symbols appear that indicate a failure (yellow triangle or red diamond). If a problem is indicated, go to MAP 0000: Start MAP on page 2–6 to isolate the problem.

8. Perform the data collection procedure. Refer to Collecting Maintenance Data on page 3–22 for instructions.

9. Perform one of the following to clear the system error (**ERR**) LED on the switch front bezel:

   — If at a web browser connected to the EWS interface, click the **Log** tab at the **Monitor** panel. The **Event Log** displays. Click **Clear System Error Light**.

   — If at the HAFM server, open the **Hardware View** and right-click the front panel bezel graphic (away from a FRU) to open a menu. Click the **Clear System Error Light** menu selection.

A
Messages

This appendix lists information and error messages that appear in pop-up message boxes at the HP StorageWorks HA-Fabric Manager (HAFM) application and HP StorageWorks Edge Switch 2/24 Product Manager applications.

The first section of the appendix lists HAFM application messages. The second section lists Product Manager messages. The text of each message is followed by a description and recommended course of action.

HAFM Application Messages

This section lists HAFM application information and error messages in alphabetical order.

Message	Description	Action
A zone must have at least one zone member.	When creating a new zone, one or more zone members must be added.	Add one or more zone members to the new zone.
A zone set must have at least one zone.	When creating a new zone set, one or more zones must be added.	Add one or more zones to the new zone set.
All zone and zone set names must be unique.	When creating a new zone or zone set, the name must be unique.	Choose a unique name for the new zone or zone set.

Message	Description	Action
All zone members are logged.	An attempt was made to display all zone members not logged-in using the **Zone Set** tab, but all members are logged in.	Information message - no action required.
Are you sure you want to delete this network address?	The currently-selected network address will be deleted.	Click **Yes** to delete or **No** to cancel.
Are you sure you want to delete this nickname?	The selected nickname will be deleted from the list of nickname definitions.	Click **Yes** to delete the nickname or **No** to cancel the operation.
Are you sure you want to delete this product?	The selected product will be deleted from the list of product definitions.	Click **Yes** to delete the product or **No** to cancel the operation.
Are you sure you want to delete this user?	The selected user will be deleted from the list of user definitions.	Click **Yes** to delete the user or **No** to cancel the operation.
Are you sure you want to delete this zone?	The selected zone will be deleted from the zone library.	Click **Yes** to delete the zone or **No** to cancel the operation.
Are you sure you want to overwrite this zone set?	The selected zone set will be overwritten in the zoning library.	Click **Yes** to overwrite or **No** to cancel.
Are you sure you want to remove all members from this zone?	All members will be deleted from the selected zone.	Click **Yes** to delete the members or **No** to cancel the operation.

Message	Description	Action
Cannot add a switch to a zone.	The device that you are attempting to add to the zone is a switch, which cannot be added to a zone.	Specify the port number or corresponding world wide name (WWN) for the device you want to add to the zone.
Cannot connect to HAFM server.	The HAFM application at a remote workstation could not connect to the HAFM server.	Verify the HAFM server internet protocol (IP) address is valid.
Cannot delete product.	The selected product cannot be deleted.	Verify the HAFM server-to-product link is up. • If the link is up, the HAFM server may be busy. • Another Product Manager instance may be open. • The user may not have permission to delete the product.
Cannot disable Fabric Binding while Enterprise Fabric Mode is active.	The user attempted to disable fabric binding through the **Fabric Binding** dialog box, but Enterprise Fabric Mode was enabled.	Disable Enterprise Fabric Mode through the **Enterprise Fabric Mode** dialog box before disabling fabric binding.
Cannot display route on a one switch fabric.	The user cannot show routes between end devices in a fabric when configuring **Show Route** from the **Fabrics** menu.	This error displays when attempting to show routes on a fabric with only one switch. Configure the Show Route option only for a multiswitch fabric.

Message	Description	Action
Cannot display route. Device is not a member of a zone in the active zone set.	The user cannot show the route for a device that is not a member of a zone in the active zone set.	Enable the default zone or activate the zone for the device before attempting to show the route.
Cannot display route. Error 9.	An internal error occurred while trying to show routes.	Retry the operation. If the condition persists, contact support personnel and report the problem.
Cannot display route. No active zone enabled.	You cannot show the route through a fabric with no active zone.	Enable the default zone or activate a zone set before attempting to show the route.
Cannot display route. All switches in route must be managed by the same server.	You cannot show the route through a fabric that has switches or directors that are managed by a different HAFM server.	This route cannot be shown unless all Edge Switches and Directors in the route are managed by this HAFM server.
Cannot display route. All switches in route must support routing.	You cannot show the route through a fabric that has switches or directors which do not support routing.	The route must contain only Directors or Edge Switches
Cannot have spaces in field.	Spaces are not allowed as part of the entry for this field.	Delete spaces from the field entry.
Cannot modify a zone set with an invalid name. Rename zone set and try again.	A zone set must have a valid name to be modified.	Assign a valid name to the zone set, then click **Modify**.
Cannot modify a zone with an invalid name. Rename zone and try again.	A zone must have a valid name to be modified.	Assign a valid name to the zone, then click **Modify**.

Message	Description	Action
Cannot modify product.	The selected product cannot be modified.	Verify the HAFM server-to-product link is up. • If the link is up, the HAFM server may be busy. • Another Product Manager instance may be open. • The user may not have permission to modify the product.
Cannot perform operation. Fabric is unknown.	This message appears if no switches in the fabric are connected to the HAFM server.	Ensure at least one fabric-attached switch or director has an Ethernet connection to the HAFM server and retry the operation.
Cannot perform operation. The list of attached nodes is unavailable.	This message appears when attached nodes are unavailable and the user attempts to modify a zone or create a new zone.	Verify an attached node is available and retry the operation.
Cannot retrieve current SNMP configuration.	The current SNMP configuration could not be retrieved.	Try again. If the problem persists, contact the next level of support.
Cannot save current SNMP configuration.	The current SNMP configuration could not be saved.	Try again. If the problem persists, contact the next level of support.
Cannot set write authorization without defining a community name.	An SNMP community name is not configured.	Enter a valid community name in the **Configure SNMP** dialog box.

Message	Description	Action
Cannot show zoning library. No fabric exists.	The user cannot show the zoning library if no fabric exists. A Director or Edge Switch must be identified to the HAFM application for a fabric to exist.	Identify a Director or Edge Switch to the HAFM application from the **New Product** dialog box.
Click **OK** to remove all contents from log.	This action deletes all contents from the selected log.	Click **OK** to delete the log contents or **Cancel** to cancel the operation.
Connection to HAFM server lost.	The connection to the remote HAFM server was lost.	Log in to the HAFM server again through the **HAFM Login** dialog box.
Connection to HAFM server lost. Click **OK** to exit application.	The HAFM application at a remote workstation lost the network connection to the HAFM server.	Start the HAFM application to connect to the HAFM server.
Could not export log to file.	A log file input/output (I/O) error occurred and the file could not be saved to the specified destination. The disk may be full or write protected.	If the disk is full, use another disk. If the disk is write protected, change the write-protect properties or use another disk.
Default zoning is not supported in Open Fabric Mode.	A default zone cannot be enabled when the switches in a fabric are set to Open Fabric mode.	Change the setting from Open Fabric mode to Homogeneous mode and retry the default zoning operation.

Message	Description	Action
Device is not a member of a zone in the active zone set.	The selected device is not a member of a zone in the active zone set and cannot communicate with the other device in the route.	Enable the default zone or activate a zone set containing the member before attempting to show the route.
Download complete. Click **OK** and start the HAFM.	Download of the HAFM and Product Manager applications is complete.	Start the HAFM application to continue.
Duplicate community names require identical write authorizations.	If configuring two communities with identical names, they must also have identical write authorizations.	Verify that both communities with the same name have the same write authorizations.
Duplicate Fabric Name.	The specified fabric name already exists.	Choose another name for the fabric.
Duplicate name in zoning configuration. All zone and zone set names must be unique.	Every name in the zoning library must be unique.	Modify (to make it unique) or delete the duplicate name.
Duplicate nickname in nickname configuration.	Duplicate nicknames cannot be configured.	Modify the selected nickname to make it unique.
Duplicate World-Wide Name in nickname configuration.	A world-wide name can be associated with only one nickname.	Modify (to make it unique) or delete the selected world-wide name.
Duplicate zone in zone set configuration.	More than one instance of a zone is defined in a zone set.	Delete one of the duplicate zones from the zone set.

Message	Description	Action
Duplicate zone member in zone configuration.	More than one instance of a zone member is defined in a zone.	Delete one of the duplicate zone members from the zone.
Enabling this zone set will replace the currently active zone set. Do you want to continue?	Only one zone set can be active. By enabling the selected zone set, the active zone set will be replaced.	Click **OK** to continue or **Cancel** to end the operation.
Error creating zone.	The HAFM application encountered an internal error.	Try the operation again. If the problem persists, contact the next level of support.
Error creating zone set.	The HAFM application encountered an internal error.	Try the operation again. If the problem persists, contact the next level of support.
Error deleting zone.	The HAFM application encountered an internal error.	Try the operation again. If the problem persists, contact the next level of support.
Error deleting zone set.	The HAFM application encountered an internal error.	Try the operation again. If the problem persists, contact the next level of support.
Error reading log file.	The HAFM application encountered an error while trying to read the log.	Try the operation again. If the problem persists, contact the next level of support.
Error removing zone or zone member.	The HAFM application encountered an internal error.	Try the operation again. If the problem persists, contact the next level of support.

Message	Description	Action
Error transferring files < message >.	An error occurred while transferring files from the PC hard drive to the HAFM application. The message varies, depending on the problem.	Try the file transfer operation again. If the problem persists, contact the next level of support.
Fabric Log will be lost once the fabric unpersists. Do you want to continue?	When you unpersist a fabric, the corresponding Fabric Log is deleted.	Click Yes to unpersist the fabric or No to cancel the operation.
Fabric not persisted.	The user attempted to refresh or clear the Fabric Log after a fabric was unpersisted. When you unpersist a fabric, the corresponding Fabric Log is deleted.	Click **OK** to continue. Ensure the fabric is persisted before attempting to refresh or clear the Fabric Log.
Field cannot be blank.	The data field requires an entry and cannot be left blank.	Enter appropriate information in the data field.
Field has exceeded maximum number of characters.	The maximum number of data entry characters allowed in the field was exceeded.	Enter the information using the proscribed number of characters.
File transfer aborted.	The user aborted the file transfer process.	Verify the file transfer is to be aborted, then click **OK** to continue.
HAFM management session is already active from this workstation.	An HAFM management session is open and active at this workstation.	A workstation can have only one active HAFM management session.

Message	Description	Action
HAFM error <error number 1 through 8 >.	The HAFM application encountered an internal error (**1** through **8** inclusive) and cannot continue operation.	Contact the next level of support to report the problem.
HAFM server is shutting down. Connection will be terminated.	The HAFM application is closing and terminating communication with the attached product.	Reboot the HAFM server. If the problem persists, contact the next level of support.
HAFM server could not log you on. Verify your username and password.	The incorrect username and password (both case sensitive) were used while attempting to login to the HAFM application.	Verify the user name and password with the customer's network administrator and retry the operation.
Enterprise Fabrics feature not installed. Please contact your sales representative.	A user selected **Fabric Binding** or **Enterprise Fabric Mode** from the **Fabrics** menu. These selections are not enabled because the optional SANtegrity feature is not installed.	Install the optional SANtegrity feature to use fabric binding or enable Enterprise Fabric Mode.
Invalid character in field.	An invalid character was entered in the data field.	Remove invalid characters from the entry.

Message	Description	Action
Invalid name.	One of the following invalid names was used: CON, AUX, COM1, COM2, COM3, COM4, COM5, COM6, COM7, COM8, COM9, LPT1, LPT2, LPT3, LPT4, LPT5, LPT6, LPT7, LPT8, LPT9, NUL, or PRN.	Select a valid name and retry the operation.
Invalid network address.	The IP address specified for the product is unknown to the domain name server (invalid).	Verify and enter a valid product IP address.
Invalid port number. Valid ports are (0-< nn >).	You have specified an invalid port number.	Specify a valid port number, in the range 0 to the maximum number of ports on the product minus one. For example, for a switch with 24 ports, the valid port range is 0 to 23.
Invalid product selection.	At the **New Product** dialog box, an invalid product was selected.	Select a valid product and retry the operation.

Message	Description	Action
Invalid request.	Three conditions result in this message: • The user tried to add or modify a product from product view and the network (IP) address is already in use. Network addresses must be unique. • The user tried to create a new user with a user name that already exists. User names must be unique. • The user tried to delete default Administrator user. The default Administrator user cannot be deleted.	Select the action that is appropriate to the activity that caused the error: • Network address: Specify a unique network (IP) address for the product. • User name: Specify a unique user name for the new user ID. • Do not delete the default Administrator user.
Invalid HAFM server address.	The IP address specified for the HAFM server is unknown to the domain name server (invalid).	Verify and enter a valid HAFM server IP address.

Message	Description	Action
Invalid UDP port number.	The specified user datagram protocol (UDP) port number is invalid. The number must be an integer from 1 through 65535 inclusive.	Verify and enter a valid UDP port number.
Invalid World-Wide Name or nickname.	The specified world-wide name format is invalid. The valid format is eight two-digit hexadecimal numbers separated by colons (xx:xx:xx:xx:xx:xx:xx:xx).	Enter a world-wide name using the correct format.
Invalid World-Wide Name. Valid WWN format is xx:xx:xx:xx:xx:xx:xx:xx.	The specified world-wide name format is invalid. The valid format is eight two-digit hexadecimal numbers separated by colons (xx:xx:xx:xx:xx:xx:xx:xx).	Enter a world-wide name using the correct format.
Invalid zone in zone set.	The defined zone no longer exists and is invalid.	Delete the invalid zone from the zone set.
Limit exceeded.	You cannot add a new product or user to the HAFM application if the maximum number of that resource exists on the system.	Delete products or users from the system before attempting to add new ones.

Message	Description	Action
No address selected.	You cannot complete the operation because an address has not been selected.	Select an address and retry the operation.
No attached nodes selected.	An operation was attempted without an attached node selected.	Select an attached node and try the operation again.
No nickname selected.	No nickname was selected when the command was attempted.	Select a nickname and try again.
No Product Managers installed.	No Director or Edge Switch Product Manager application is installed on this workstation.	Install the appropriate Product Manager to this workstation.
No routing information available.	No information is available for the route selected.	Select a different route and try the operation again.
No HAFM server specified.	An HAFM server is not defined to the HAFM application.	At the **HAFM Login** screen, type a server name in the **HAFM server** field and click **Login**.
No user selected.	A user was not selected when the command was attempted.	Select a user and try again.
No zone member selected.	A zoning operation was attempted without a zone member selected.	Select a zone member and try the operation again.
No zone selected.	A zoning operation was attempted without a zone selected.	Select a zone and try the operation again.

Message	Description	Action
No zone selected or zone no longer exists.	A zoning operation was attempted without a zone selected, or the zone selected no longer exists in the fabric.	Select a zone and try the operation again.
No zone set active.	A zone set cannot be deactivated if there are no active zones.	Informational message only-no action is required.
No zone set selected.	A zoning operation was attempted without a zone set selected.	Select a zone set and try the operation again.
No zone set selected or zone set no longer exists.	A zoning operation was attempted without a zone set selected, or the zone set you selected no longer exists in the fabric.	Select a zone set and try the operation again.
Only attached nodes can be displayed in this mode.	Users cannot display unused ports when adding ports by world-wide name.	Change the add criteria to **Add by Port**.
Password and confirmation don't match.	Entries in the password field and confirmation password field do not match. The entries are case sensitive and must be the same.	Enter the password and confirmation password again.
Product manager instance is currently open.	A product cannot be deleted while an instance of the Product Manager application is open.	Close the Product Manager application, then delete the product.

Message	Description	Action
Remote session support has been disabled.	The connection between the specified remote workstation and the HAFM server was disallowed.	Consult with the customer's network administrator to determine if the workstation entry should be modified at the **Session Options** dialog box.
Remote sessions are not allowed from this network address.	Only IP addresses of remote workstations specified at the **Session Options** dialog box are allowed to connect to the HAFM server.	Consult with the customer's network administrator to determine if the IP address is to be configured for remote sessions.
Resource is unavailable.	The specified operation cannot be performed because the product is unavailable.	Verify the HAFM server-to-product link is up. If the link is up, the HAFM server may be busy. Try the operation again later.
Selection is not a World-Wide Name.	The selection made is not a world-wide name.	Select a valid world-wide name before performing this operation.
Server shutting down.	The HAFM application is closing and terminating communication with the attached product.	Reboot the HAFM server. If the problem persists, contact the next level of support.
SNMP trap address not defined.	If an SNMP community name is defined, a corresponding SNMP trap recipient address must also be defined.	Enter a corresponding SNMP trap recipient address.
The Administrator user cannot be deleted.	The administrator user is permanent and cannot be deleted from the **Configure Users** dialog box.	Informational message only-no action is required.

Message	Description	Action
The Domain ID was not accepted. The World Wide Name and Domain ID must be unique in the Fabric Membership List.	A user attempted to add a Director or Edge Switch to the fabric membership list through the Fabric Binding option (SANtegrity feature), but a product already exists in the fabric with the same domain ID.	Enter a unique domain ID for the switch in the **Add Detached Switch** dialog box.
The HAFM server is busy processing a request from another Product Manager.	The HAFM server PC is processing a request from another instance of a Product Manager application, and cannot perform the requested operation.	Wait until the process completes, then retry the operation.
The link to the managed product is not available.	The Ethernet connection between the HAFM server and managed product is down or unavailable.	Establish and verify the network connection.
The maximum number of members has already been configured.	The maximum number of zone members that can be defined to the application was reached.	Delete an existing zone member before adding a new zone member.
The maximum number of nicknames has already been configured.	The maximum number of nicknames that can be defined to the HAFM application was reached.	Delete an existing nickname before adding a new nickname.

Message	Description	Action
The maximum number of open products has already been reached.	The maximum number of open products allowed was reached.	Close a Product Manager session (existing open product) before opening a new session.
The maximum number of products has already been configured.	The number of managed HA Fabric Directors and Edge Switches (48) that can be defined to the HAFM application was reached.	Delete an existing product before adding a new product.
The maximum number of products of this type has already been configured.	The number of HA Fabric Directors and Edge Switches of this type (48) that can be defined to the HAFM application was reached.	Delete an existing product of this type before adding a new product.
The maximum number of remote network addresses has already been configured.	A maximum of four IP addresses for remote workstations can be configured at the **Session Options** dialog box. That number was reached.	Delete an existing IP address before adding a new IP address.
The maximum number of HAFM application sessions has been reached.	A maximum of eight concurrent remote management sessions can be configured at the **Session Options** dialog box. The specified number was reached.	Increase the number of remote sessions allowed (if less than four), or terminate a session before attempting to initiate a new session.

Message	Description	Action
The maximum number of HAFM server network addresses has already been configured.	The number of HAFM server IP addresses that can be defined to the HAFM application was reached.	Delete an existing IP address before adding a new address.
The maximum number of users has already been configured.	The number of users (16) that can be defined to the HAFM application was reached.	Delete an existing user before adding a new user.
The maximum number of zones allowed has already been configured.	The maximum number of zones that can be defined was reached.	Delete an existing zone before adding a new zone.
The maximum number of zone sets has already been configured.	The maximum number of zone sets that can be defined was reached.	Delete an existing zone set before adding a new zone set.
The maximum number of zones per zone set has already been configured.	The maximum number of zones that can be defined in a zone set was reached.	Delete an existing zone before adding a new zone to the zone set.
The nickname does not exist.	The entered nickname does not exist in the fabric.	Configure the nickname to the appropriate product or select an existing nickname.
The nickname is already assigned. Either use a different name or do not save the name as a nickname.	The entered nickname already exists in the fabric. Each nickname must be unique.	Define a different nickname.

Message	Description	Action
The software version on this HAFM server is not compatible with the version on the remote HAFM server.	A second HAFM server PC (client) connecting to the HAFM server must be running the same software version to log in.	Upgrade the software version on the downlevel HAFM server PC.
The zoning library conversion must be completed before continuing.	The zoning library conversion is incomplete and the requested operation cannot continue.	Complete the zoning library conversion, then retry the operation.
This fabric log is no longer valid because the fabric has been unpersisted.	The selected Fabric Log is no longer available because the fabric was unpersisted.	To start a new log for the fabric, persist the fabric through the **Persist Fabric** dialog box.
This network address has already been assigned.	The specified IP address was assigned and configured. A unique address must be assigned.	Consult with the customer's network administrator to determine a new IP address to be assigned and configured.
This product is not managed by this HAFM server.	The product selected is not managed by this HAFM server.	Select a product managed by this HAFM server or go to the HAFM server that manages the affected product.
This switch is currently part of this fabric and cannot be removed from the Fabric Membership List. Isolate the switch from the fabric prior to removing it from the Fabric Membership List.	A user attempted to remove a Director or Edge Switch from the fabric membership list using the Fabric Binding option, but the Director or Edge Switch is still part of the fabric.	Remove the director switch from the fabric by setting the product offline or blocking the E_Port connection.

Message	Description	Action
This user name has already been assigned.	The specified user name is already assigned and configured.	Modify (to make it unique) or delete the duplicate name.
This Worldwide Name was not accepted. The World Wide Name and Domain ID must be unique in the Fabric Membership List.	A user attempted to add a product to the fabric membership list through the Fabric Binding option (SANtegrity feature), but an entry already exists in the with the same WWN.	Enter a unique WWN for the Director or Edge Switch at the **Add Detached Switch** dialog box.
Too many members defined.	The maximum number of zone members that can be defined was reached.	Delete an existing zone member before adding a new zone member.
You do not have a compatible version of the HAFM server software. In order for the HAFM application to function properly, a compatible version must be installed on the client machine. Click **OK** to install a compatible version.	The HAFM application version running on the HAFM server differs from the version running on the remote workstation (client). A compatible version must be downloaded from the HAFM server.	Download a compatible version of the HAFM application to the remote workstation (client) using the web install procedure.
You do not have rights to perform this action.	Configured user rights do not allow this operation to be performed.	Verify user rights with the customer’s network administrator and change as required.
You must define an SMTP server address.	A simple mail transfer protocol (SMTP) server address must be defined and configured for e-mail to be activated.	Define the SMTP server address at the **Configure E-Mail** dialog box.

Message	Description	Action
You must define at least one E-mail address.	At least one e-mail address must be defined and configured for e-mail to be activated.	Define an e-mail address at the **Configure E-Mail** dialog box.
You must define at least one remote network address.	At least one IP address for a remote workstation must be configured for a remote session to be activated.	Define an IP address for at least one remote workstation at the **Session Options** dialog box.
You must download the HAFM client via the web install.	An attempt was made to download the HAFM application to a remote workstation (client) using an improper procedure.	Download a compatible version of the HAFM application to the remote workstation (client) using the web install procedure.
Zones configured with port numbers are ignored in Open Fabric Mode.	While in Open Fabric mode, zones configured using port numbers are enforced through world-wide names.	Informational message only - no action is required.
Zones must be defined before creating a zone set.	You cannot create a zone set without any zones defined for the HAFM.	Define zones using the **New Zone** dialog box.
Zoning by port number is not supported in Open Fabric Mode.	You cannot specify an item for zoning by port number if the HAFM application is set to Open Fabric Mode.	Either define zones by device WWN or change to Homogeneous Fabric 1.0 mode in the **Configure Operation Mode** dialog box of Product Manager application.
Zoning name already exists.	Duplicate zone names are not allowed in the zoning library.	Modify (to make it unique) or delete the duplicate zone name.

Edge Switch 2/24 Product Manager Messages

This section lists switch Product Manager information and error messages in alphabetical order.

Message	Description	Action
Activating this configuration will overwrite the current configuration.	Confirmation message to activate a new address configuration.	Click Yes to confirm activating the new address configuration or No to cancel the operation.
All configuration names must be unique.	All address configurations must be saved with unique names.	Save the configuration with a different name that is unique to all saved configurations.
All port names must be unique.	A duplicate Fibre Channel port name was configured. All port names must be unique.	Reconfigure the Fibre Channel port with a unique name.
Another Product Manager is currently performing a firmware install.	Only one instance of the Product Manager application can install a firmware version to the switch or director at a time.	Wait for the firmware installation process to complete and try the operation again.
Are you sure you want to delete firmware version?	This message requests confirmation to delete a firmware version from the HAFM server's firmware library.	Click **Yes** to delete the firmware version or **No** to abort the operation.
Are you sure you want to delete this address configuration?	Confirmation to delete the selected address configuration.	Click Yes to confirm the deletion of the address configuration or No to cancel the operation.

Message	Description	Action
Are you sure you want to send firmware version?	This message requests confirmation to send a firmware version from the HAFM server's firmware library to the switch or director.	Click **Yes** to send the firmware version or **No** to abort the operation.
Cannot disable Switch Binding while Enterprise Fabric Mode is active and the switch is Online.	A user attempted to disable switch binding through the **Switch Binding Change State** dialog box, but Enterprise Fabric Mode is enabled.	Either disable Enterprise Fabric Mode using the **Enterprise Fabric Mode** dialog box at the HAFM application, or set the switch offline to disable switch binding.
Cannot disable Insistent Domain ID while Fabric Binding is active.	A user attempted to disable the Insistent Domain ID parameter through the **Configure Switch Parameters** dialog box, but fabric binding is enabled.	Disable fabric binding through the **Fabric Binding** dialog box before disabling the parameter.
Cannot enable beaconing on a failed FRU.	Message occurs when selecting Enable Beaconing for a failed FRU.	Replace the FRU and enable beaconing or enable beaconing on an operating FRU.
Cannot enable beaconing while the system error light is on.	Beaconing cannot be enabled while the system error LED is illuminated.	Select **Clear System Error Light** from the **Product** menu to clear the error light, then enable beaconing.
Cannot have spaces in field.	Spaces are not allowed as part of the entry for this field.	Delete spaces from the field entry.
Cannot install firmware to a switch with a failed CTP card.	Firmware cannot be installed on a switch with a failed CTP card.	The CTP card failed and is not a FRU. Replace the switch.

Message	Description	Action
Cannot perform this operation while the switch is offline.	This operation cannot be performed while the switch is offline.	Set the switch offline through the **Set Online State** dialog box and retry the operation.
Cannot retrieve current SNMP configuration.	The switch or director SNMP configuration cannot be retrieved by the Product Manager application because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot retrieve diagnostics results.	Switch or director diagnostic results cannot be retrieved by the Product Manager application because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot retrieve switch date and time.	The switch or director date and time cannot be retrieved by the Product Manager application because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot retrieve switch state.	The switch or director state cannot be retrieved by the Product Manager application because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot retrieve port configuration.	The port configuration cannot be retrieved by the Product Manager application because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.

Message	Description	Action
Cannot retrieve port information.	Port information cannot be retrieved by the Product Manager application because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot retrieve port statistics.	Port statistics cannot be retrieved by the Product Manager application because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot run diagnostics on a port that is failed.	Port diagnostics (loopback tests) cannot be performed on a port that has failed any previous diagnostic (power-on diagnostic, online diagnostic, or loopback test). The amber LED associated with the port illuminates to indicate the failed state.	Reset the port and perform diagnostics again.
Cannot run diagnostics on an active E_Port.	Port diagnostics cannot be performed on a configured and active expansion port (E_Port).	Run diagnostics only on an inactive E-port.
Cannot run diagnostics. The port is not installed.	Port diagnostics cannot be performed if the port transceiver is not installed.	Install an optical transceiver or run diagnostics only on a port with an installed transceiver.

Message	Description	Action
Cannot run diagnostics while a device is logged-in to the port.	Port diagnostics (internal loopback test) cannot be performed on a port while an attached Fibre Channel device is logged in.	Ensure the device is logged out and perform diagnostics again.
Cannot save port configuration.	The port configuration cannot be saved at the Product Manager application because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot save SNMP configuration.	The switch or director SNMP configuration cannot be saved at the Product Manager application because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot set switch date and time.	The switch or director date and time cannot be set at the Product Manager application because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot set switch state.	The switch or director state cannot be set at the Product Manager application because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.

Message	Description	Action
Cannot set fibre channel parameters.	Fibre Channel parameters for the switch or director cannot be set at the Product Manager application because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot set write authorization without defining a community name.	A community name was not defined in the **Configure SNMP** dialog box for the write authorization selected.	Enter a community name in the name field where write authorization is checked.
Cannot start data collection.	The data collection procedure cannot be started by the Product Manager application because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot start port diagnostics.	Port diagnostics cannot be started at the Product Manager application because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Click **OK** to remove all contents from log.	This action deletes all contents from the selected log.	Click **OK** to delete the log contents or **Cancel** to cancel the operation.
Continuing may overwrite host programming. Continue?	Configurations sent from the host may be overwritten by the HAFM application.	Continuing activates the current configuration and overwrites the host configuration.

Message	Description	Action
Could not export log to file.	A log file I/O error occurred and the file could not be saved to the specified destination. The disk may be full or write protected.	If the disk is full, use another disk. If the disk is write protected, change the write-protect properties or use another disk.
Could not find firmware file.	A firmware version could not be found because the data directory structure for the HAFM server is corrupt.	Reinstall the HAFM and Product Manager applications. If the condition persists, contact the next level of support.
Could not remove dump files from server.	Dump files could not be deleted from the HAFM server because the notebook PC or Product Manager application is busy.	Retry the operation later. If the condition persists, contact the next level of support.
Could not stop port diagnostics.	Port diagnostics could not be stopped by the Product Manager application because the Ethernet link is down or busy, or because the switch or director is busy.	Retry the operation later. If the condition persists, contact the next level of support.
Could not write firmware to flash.	A firmware version could not be written from the HAFM server to FLASH memory on the switch's CTP2 card.	Retry the operation again. If the condition persists, contact the next level of support.

Message	Description	Action
Date entered is invalid.	The date is entered incorrectly at the **Configure Date and Time** dialog box. Individual field entries may be correct, but the overall date is invalid (for example, a day entry of **31** for a 30-day month).	Verify each entry is valid and consistent.
Device applications should be terminated before starting diagnostics. Press NEXT to continue.	Port diagnostics (loopback tests) cannot be performed on a port while an attached device application is running.	Terminate the device application and perform diagnostics again.
[device WWN] cannot be removed from the Switch Membership List while participating in Switch Binding. The device must be isolated from the switch, or Switch Binding deactivated before it can be removed.	A user attempted to remove a device WWN from the switch membership list (SANtegrity feature) with switch binding enabled.	Disconnect the device by blocking the switch port and setting the switch offline, or disable switch binding through the **Switch Binding Change State** dialog box before removing devices from the switch membership list.
Disabling Insistent Domain ID will disable Fabric Binding. Do you want to continue?	Fabric binding is enabled through the HAFM application and a user attempted to disable the Insistent Domain ID parameter at the **Configure Switch Parameters** dialog box.	Click Yes to continue and disable fabric binding.

Message	Description	Action
Disabling Switch Binding will disable Enterprise Fabric Mode. Do you want to continue?	A user attempting to disable switch binding through the **Switch Binding State Change** dialog box, but Enterprise Fabric Mode is enabled.	Disable Enterprise Fabric Mode at the **Enterprise Fabric Mode** dialog box before disabling switch binding.
Do you want to continue with IPL?	This message requests confirmation to initial program load (IPL) the switch or director.	Click **OK** to IPL the switch or director or **No** to cancel the operation.
Duplicate Community names require identical write authorizations.	Duplicate community names are entered at the **Configure SNMP** dialog box, and have different write authorizations.	Delete the duplicate community name or make the write authorizations consistent.
Duplicate port names detected.	Ports cannot have the same name.	Rename ports using the **Configure Ports** option in the **Configure** menu.
Enterprise Fabric Mode will be disabled if any of the following parameters are disabled: Insistent Domain ID, Rerouting Delay, Domain RSCN's. Do you want to continue?	A user attempted to disable one or more of these parameters at the **Configure Switch Parameters** dialog box with the switch online and Enterprise Fabric Mode (SANtegrity feature) enabled.	Click Yes to continue and disable Enterprise Fabric Mode.

Message	Description	Action
Error retrieving port information.	An error occurred at the Product Manager application while retrieving port information because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Error retrieving port statistics.	An error occurred at the Product Manager application while retrieving port statistics because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Error stopping port diagnostics.	An error occurred at the Product Manager application while attempting to stop port diagnostics from running because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Error transferring files < message >.	An error occurred while transferring files from the PC hard drive to the Product Manager application. The message varies, depending on the problem.	Try the file transfer operation again. If the problem persists, contact the next level of support.
Field cannot be blank.	The data field requires an entry and cannot be left blank.	Enter appropriate information in the data field.
File transfer aborted.	The user aborted the file transfer process.	Verify the file transfer is to be aborted, then click **OK** to continue.

Message	Description	Action
File transfer is in progress.	A firmware file is being transferred from the HAFM server hard drive, or a data collection file is being transferred to a diskette.	Informational message only-no action is required.
Firmware download timed out.	A firmware download operation timed out and aborted.	Retry the operation. If the problem persists, contact the next level of support.
Firmware file I/O error.	A firmware download operation aborted because a file I/O error occurred.	Retry the operation. If the problem persists, contact the next level of support.
Firmware file not found.	The firmware version is not installed (or was deleted) from the firmware library at the HAFM server.	Add the firmware version to the library and retry the operation.
Enterprise Fabrics feature not installed. Please contact your sales representative.	A user selected Switch Binding from the **Configure** menu. This selection is not supported because the SANtegrity feature is not installed.	Install the optional SANtegrity feature key through the **Configure Feature Key** dialog box before enabling switch binding.
Incorrect product type.	When configuring a new product through the **New Product** dialog box, an incorrect product was selected for the network address.	Select the correct product type for the product with the network address.
Internal file transfer error received from switch.	The switch or director detected an internal file transfer error.	Retry the operation. If the problem persists, contact the next level of support.

Message	Description	Action
Installing this feature key, while online, will cause an IPL operation on the switch and a momentary loss of LAN connection. This operation is non-disruptive to the Fibre Channel traffic. Do you wish to continue installing this feature key?	If the switch is online, installing a feature key causes a switch IPL. The LAN connection to the HAFM server is lost momentarily, but Fibre Channel traffic is not affected.	Click Yes to install the feature key or No to discontinue the operation.
Invalid character in field.	An invalid character was entered in the data field.	Remove invalid characters from the entry.
Invalid configuration name.	A user attempted to save an invalid address configuration name.	Enter a configuration name of up to 24 alphanumeric characters, including spaces, hyphens and underscores.
Invalid feature key.	The entered feature key was not recognized.	Enter the feature key again. The key is case sensitive and includes dashes.
Invalid firmware file.	The file selected for firmware download is not a firmware version file.	Select the correct firmware version file and retry the operation.
Invalid network address.	The IP address specified for the product is unknown to the domain name server (invalid).	Verify and enter a valid product IP address.
Invalid port number.	The Fibre Channel number entered is invalid. The port number must be an integer from 0 through 63 inclusive.	Verify and enter a valid port number.

Message	Description	Action
Invalid response received from switch.	An error occurred at the switch or director during a firmware download operation.	Retry the firmware download operation. If the problem persists, contact the next level of support.
Invalid serial number for this feature key.	The switch serial number and entered feature key do not match.	Ensure the entered feature key corresponds to the switch serial number.
Invalid UDP port number.	The specified user datagram protocol (UDP) port number is invalid. The number must be an integer from 1 through 65535 inclusive.	Verify and enter a valid UDP port number.
Invalid value for day (1 - 31).	At the **Configure Date and Time** dialog box, the DD value (day) must be an integer from 1 through 31 inclusive.	Verify and enter a valid date.
Invalid value for E_D_TOV.	At the **Configure Operating Parameters** dialog box, the error detect time-out value (E_D_TOV) must be an integer from 2 through 600 inclusive.	Verify and enter a valid number.
Invalid value for hour (0 - 23).	At the **Configure Date and Time** dialog box, the HH value (hour) must be an integer from 0 through 23 inclusive.	Verify and enter a valid time.

Message	Description	Action
Invalid value for minute (0 - 59).	At the **Configure Date and Time** dialog box, the MM value (minute) must be an integer from 0 through 59 inclusive.	Verify and enter a valid time.
Invalid value for month (1 - 12).	At the **Configure Date and Time** dialog box, the MM value (month) must be an integer from 1 through 12 inclusive.	Verify and enter a valid date.
Invalid value for R_A_TOV.	At the **Configure Operating Parameters** dialog box, the resource allocation time-out value (R_A_TOV) must be an integer from 10 through 1200 inclusive.	Verify and enter a valid number.
Invalid value for second (0 - 59).	At the **Configure Date and Time** dialog box, the SS value (second) must be an integer from 0 through 59 inclusive.	Verify and enter a valid time.
Invalid value for year.	At the **Configure Date and Time** dialog box, the YYYY value (year) must be a four-digit value.	Verify and enter a four-digit value for the year.

Message	Description	Action
Invalid World-Wide Name.	The specified world-wide name format is invalid. The valid format is eight two-digit hexadecimal numbers separated by colons (xx:xx:xx:xx:xx:xx:xx:xx).	Enter a world-wide name using the correct format.
Link dropped.	The HAFM server-to-switch or director Ethernet link was dropped.	Retry the operation. If the condition persists, contact the next level of support.
Log is currently in use.	Access to the log is denied because the log was opened by another instance of the Product Manager application.	Retry the operation later. If the condition persists, contact the next level of support.
Maximum number of versions already installed.	The number of firmware versions that can be defined to the HAFM application's firmware library was reached.	Delete an existing firmware version before adding a new version.
Nickname already exists. Please use a different nickname.	The entered nickname already exists.	Specify a unique nickname.
No backup configuration available to restore.	A backup of the configuration is not on the HAFM server hard drive. A configuration restore cannot be completed.	Select **Backup and Restore Configuration** from the **Maintenance** menu and select **Backup** to create a backup configuration file.
No file was selected.	Action requires the selection of a file.	Select a file.

Message	Description	Action
No firmware versions to delete.	There are no firmware versions in the firmware library to delete, therefore the operation cannot be performed.	Informational message only-no action is required.
No firmware version was selected.	A file was not selected in the **Firmware Library** dialog box before an action, such as modify or send, was performed.	Click on a firmware version in the dialog box to select it, then perform the action again.
Non-redundant switch must be offline to install firmware.	Because the switch has only a single CTP card, it must be offline to initiate a firmware installation.	Set switch offline and try the firmware installation again.
Not all of the optical transceivers are installed for this range of ports.	One or more ports in the specified port range do not have optical transceivers installed.	Specify a port range valid for ports installed.
Performing this action will overwrite the date/time on the switch.	Warning that occurs when configuring the date and time through the **Configure Date and Time** dialog box, that the new time or date will overwrite the existing time or date set for the switch or director.	Verify that you want to overwrite the current date or time.
Performing this operation will change the current state to Offline.	This message requests confirmation to set the switch or director offline.	Click **OK** to set the switch or director offline or **Cancel** to cancel the operation.

Message	Description	Action
Performing this operation will change the current state to Online.	This message requests confirmation to set the switch or director online.	Click **OK** to set the switch or director online or **Cancel** to cancel the operation.
Periodic Date/Time synchronization must be cleared before enabling switch clock alert.	Action cannot be performed because **Periodic Date/Time Synchronization** option is active.	Click **Periodic Date/Time Synchronization** check box in **Configure Date and Time** dialog box (**Configure** menu) to clear check mark and disable periodic date/time synchronization.
Port binding was removed from attached devices that are also participating in Switch Binding.	A user disabled port binding for attached devices, but one or more of the devices is controlled by fabric binding.	Review the switch binding membership list to determine if devices should or should not be included.
Port diagnostics cannot be performed on an inactive port.	This message displays when port diagnostics are performed on an inactive port.	Perform diagnostics on an active port.
Product manager error <error number>.	The product manager application encountered an internal error and cannot continue.	Contact support personnel and report the problem.
Product manager instance is currently open.	A Product Manager window is open.	Informational message only.
R_A_TOV must be greater than E_D_TOV.	The R_A_TOV value must be greater than the E_D_TOV value.	Change a value so R_A_TOV exceeds E_D_TOV.
Resource is unavailable.	The specified operation cannot be performed because the switch is unavailable.	Verify the switch-to-HAFM server link is operational. If the link is up, the HAFM server may be busy. Try the operation later.

Message	Description	Action
Send firmware failed.	A firmware download operation failed.	Retry the firmware download operation. If the problem persists, contact the next level of support.
SNMP trap address not defined.	If an SNMP community name is defined, a corresponding SNMP trap recipient address must also be defined.	Enter a corresponding SNMP trap recipient address.
Stop diagnostics failed. The test is already running.	Diagnostics for the port was not running and the **Stop** was selected on the **Port Diagnostics** dialog box. Diagnostics quit for the port, but **Stop** button remains enabled.	Verify port operation. Retry diagnostics for port and select **Stop** from the dialog box. If problem persists, contact your service representative.
Stop diagnostics failed. The test was not running.	The action to stop diagnostics failed because the test was not running.	Information message - no action required.
Switch Binding was removed from attached devices that are also participating in Port Binding. Please review the Port Binding Configuration.	Device WWNs were removed from the switch membership list (SANtegrity feature), but one or more of the devices still has security controlled by port binding.	Verify the security level for each device is specified as required by reviewing the Bound WWN list at the **Configure Ports** dialog box.
Switch must be offline to configure.	The switch or director must be set offline prior to configuring Fibre Channel operating parameters.	Set the switch or director offline, reconfigure parameters at the **Configure Operating Parameters** dialog box, and retry the operation.

Message	Description	Action
System diagnostics cannot run. The Operational Status is invalid.	System diagnostics cannot run on switch or Director or Edge Switch with failed ports.	Replace failed ports.
The add firmware process has been aborted.	The user aborted the process to add a firmware version to the HAFM server's firmware library.	Verify the firmware addition is to be aborted, then click **OK** to continue.
The data collection process failed.	An error occurred while performing the data collection procedure.	Try the data collection procedure again. If the problem persists, contact the next level of support.
The data collection process has been aborted.	The user aborted the data collection procedure.	Verify the data collection procedure is to be aborted, then click **OK** to continue.
The following parameters cannot be disabled while Enterprise Fabric Mode is active: Insistent Domain ID, Rerouting Delay, Domain RSCN's.	A user attempted to disable one or more of these parameters at the **Configure Switch Parameters** dialog box with the switch online and Enterprise Fabric Mode (SANtegrity feature) enabled.	Click Yes to continue and disable Enterprise Fabric Mode.
The maximum number of address configurations has been reached.	The maximum number of address configurations that can be saved to the HAFM server was reached.	Delete configurations no longer needed to allow one or more new address configurations to be saved.
The optical transceiver is not installed.	Information is not available for a port without an optical transceiver installed.	Install an SFP optical transceiver in the port.

Message	Description	Action
The switch did not accept the request.	The switch or director cannot perform the requested action.	Retry the operation. If the condition persists, contact the next level of support.
The switch did not respond in the time allowed.	While waiting to perform a requested action, the switch or director timed out.	Retry the operation. If the condition persists, contact the next level of support.
The switch is busy saving maintenance information.	The switch or director cannot perform the requested action because it is busy saving maintenance information.	Retry the operation later. If the condition persists, contact the next level of support.
The switch must be offline to configure.	This configuration task requires the switch or director to be offline.	Take the switch or director offline and retry the action.
The firmware file is corrupted.	A firmware version file is corrupt.	Contact the next level of support to report the problem.
The firmware version already exists.	This firmware version already exists in HAFM server's firmware library.	Informational message only-no action is required.
The link to the switch is not available.	The Ethernet connection between the HAFM server and the switch or director is down or unavailable.	Establish and verify the network connection.
The HAFM server is busy processing a request from another Product Manager.	The HAFM server PC is processing a request from another instance of a Product Manager application, and cannot perform the requested operation.	Wait until the process is completes, then perform the operation again.

Message	Description	Action
This feature has not been installed. Please contact your sales representative.	A user selected an option that is unavailable because a necessary feature is not installed.	Contact your sales representative to obtain and install the desired optional feature.
This feature key does not include all of the features currently installed and cannot be activated while the switch is online.	The installed feature set contains features not being installed with the new feature key. To activate the new feature key, you must set the switch offline. Activating the new feature set removes features not in the new feature set.	Set the switch offline through the **Set Online State** dialog box. Activate the new feature key using the **Configure Feature Key** dialog box.
This feature key does not include all of the features currently installed. Do you want to continue with feature key activation?	The installed feature set contains features not being installed with the new feature key.	Click Yes to activate the feature key and remove current features not in the new feature set or No to cancel the operation.
Threshold alerts are not supported on firmware earlier than 01.03.00.	Threshold alerts are not supported in firmware releases before 1.03.00.	Informational message.
Unable to change incompatible firmware release.	The firmware you are trying to download cannot be used for this Product Manager application release.	Download compatible firmware for this Product Manager application release.

Message	Description	Action
Unable to save data collection file to destination.	The HAFM server could not save the data collection file to the specified location (PC hard drive, diskette, or network).	Retry the operation. If the condition persists, contact the next level of support.
You do not have rights to perform this action.	Configured user rights do not allow this operation to be performed.	Verify user rights with the customer's network administrator and change as required.

B

Event Codes

This appendix lists all three-digit HP StorageWorks Edge Switch 2/24 event codes and provides detailed information about each code. Event codes are listed in numerical order and in tabular format.

An event is an occurrence (state change, problem detection, or problem correction) that requires user attention or that should be reported to a system administrator or service representative. An event usually indicates a switch operational state transition, but may also indicate an impending state change (threshold violation). An event may also provide information only, and not indicate an operational state change. Event codes are grouped as follows:

- **000** through **199** - system events.
- **200** through **299** - power supply events.
- **300** through **399** - fan events.
- **400** through **499** - CTP card events.
- **500** through **599** - port module events.
- **800** through **899** - Thermal

Events can be recorded in the switch **Event Logs** at the HAFM server, at a remote workstation if E-mail and call-home features are enabled, or at a simple network management protocol (SNMP) workstation. An event may also illuminate the system error (**ERR**) light-emitting diode (LED) on the front panel.

In addition to numerical event codes, the tables in this appendix also provide a:

- **Message -** a brief text string that describes the event.
- **Severity -** a severity level that indicates event criticality as follows:
  - **0 -** informational.
  - **2 -** minor.
  - **3 -** major.
  - **4 -** severe (not operational).
- **Explanation -** a complete explanation of what caused the event.
- **Action -** the recommended course of action (if any) to resolve the problem.
- **Event Data -** supplementary event data (if any) that appears in the event log in hexadecimal format.
- **Distribution -** check marks in associated fields indicate where the event code is reported (front panel, HAFM server, or host).

System Events (000 through 199)

Event Code: 001							
Message:	System power-down.						
Severity:	Informational.						
Explanation:	The switch was powered off or disconnected from the facility AC power source. The event code is distributed the next time the switch powers on, but the date and time of the code reflect the power-off time.						
Action:	No action required.						
Event Data:	No supplementary data included with the event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Event Code: 011							
Message:	Login Server database invalid.						
Severity:	Minor.						
Explanation:	Following an initial machine load (IML) or firmware download, the Login Server database failed its cyclic redundancy check (CRC) validation. All Fabric Services databases are initialized to an empty state, resulting in an implicit Fabric logout of all attached devices.						
Action:	Perform the data collection procedure and return the Zip disk to Hewlett-Packard support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔		

Event Code: 021							
Message:	Name Server database invalid.						
Severity:	Minor.						
Explanation:	Following an IML or firmware download, the Name Server database failed its CRC validation. All Fabric Services databases are initialized to an empty, state resulting in an implicit Fabric logout of all attached devices.						
Action:	Perform the data collection procedure and return the Zip disk to Hewlett-Packard support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔		

Event Code: 031							
Message:	SNMP request received from unauthorized community.						
Severity:	Informational.						
Explanation:	An SNMP request containing an unauthorized community name was received and rejected with an error. Only requests containing authorized SNMP community names as configured through the switch Product Manager application are allowed.						
Action:	Add the community name to the SNMP configuration using the switch Product Manager application.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Event Code: 051							
Message:	Management Server database invalid.						
Severity:	Minor.						
Explanation:	Following an IML, or firmware download, the Management Server database failed its CRC validation. All Management Services databases are initialized to an empty state, resulting in an implicit logout of all devices logged in to the Management Server.						
Action:	Perform the data collection procedure and return the Zip disk to Hewlett-Packard support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔		

Event Code: 052							
Message:	Management Server internal error, asynchronous status report activation, or mode register update occurred.						
Severity:	Informational.						
Explanation:	An internal operating error was detected by the Management Server subsystem, an asynchronous status was reported to an attached host, or a mode register update occurred.						
Action:	Management Server internal error: Perform the data collection procedure and return the Zip disk to Hewlett-Packard support personnel. Asynchronous status report activation: No action required. Mode register update: No action required.						
Event Data:	Supplementary data consists of reporting tasks of type **eMST_SB2**, with component_id **eMSCID_SB2_CHPGM**. For each type of error or indication, the subcomponent_id is: Management Server internal error: subcomponent_id is **eMS_ELR_SB2_DEVICE_PROTOCOL_ERROR** or **eMS_ELR_SB2_MSG_PROCESSING_ERROR**. Asynchronous status report activation: subcomponent_id is **eSB2_CP_RER_ASYNCH_STATUS_REPORTING**. Mode register update: subcomponent_id is **eMS_ELR_MODE_REGISTER_UPDATE**.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓			✓	

Event Code: 061							
Message:	Fabric Controller database invalid.						
Severity:	Minor.						
Explanation:	Following an IML, or firmware download, the Fabric Controller database failed its CRC validation. All Fabric Controller databases are initialized to an empty state, resulting in a momentary loss of interswitch communication capability.						
Action:	Perform the data collection procedure and return the Zip disk to Hewlett-Packard support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔		

Event Code: 062							
Message:	Maximum interswitch hop count exceeded.						
Severity:	Informational.						
Explanation:	The fabric controller software detected that a path to another fabric element (Director or Edge Switch) traverses more than seven interswitch links (ISLs or hops). This may result in Fibre Channel frames persisting in the fabric longer than standard timeout values allow.						
Action:	If possible, reconfigure the fabric so the path between any two Director or Edge Switch traverses no more than seven ISLs.						
Event Data:	Byte **0** = domain ID of the fabric element (director or switch) more than seven hops away. Bytes **1** - **3** = reserved.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Event Code: 063							
Message:	Remote switch has too many ISLs.						
Severity:	Major.						
Explanation:	The fabric element (director or switch) whose domain ID is indicated in the event data has too many ISLs attached, and that element is unreachable from this switch. HAFM application Version 3.2 and earlier supports up to 32 ISLs. HAFM application Version 3.3 and later supports up to 128 ISLs.						
Action:	Reduce the ISLs on the indicated fabric element to a number within the limits specified.						
Event Data:	Byte **0** = domain ID of the fabric element (director or switch) with too many ISLs. Bytes **1** - **3** = reserved.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Event Code: 070	
Message:	E_Port is segmented.
Severity:	Informational.
Explanation:	A switch E_Port recognized an incompatibility with an attached fabric element (Director or Edge Switch), preventing the switch from participating in the fabric. A segmented port does not transmit Class 2 or Class 3 traffic (data from attached devices), but transmits Class F traffic (management and control data from the attached Director or Edge Switch). Refer to the event data for the segmentation reason.
Action:	Action depends on the segmentation reason specified in the event data.

Event Data:	The first byte of event data (byte **0**) specifies the E_Port number. The fifth byte (byte **4**) specifies the segmentation reason as follows: **1 = Incompatible operating parameters.** Ether the resource allocation time out value (R_A_TOV) or error detect time out value (E_D_TOV) is inconsistent between the switch and another fabric element (Director or Edge Switch). Modify the R_A_TOV and E_D_TOV to make the values consistent for all fabric Directors and Edge Switches. **2 = Duplicate domain ID.** The switch has the same preferred domain ID as another fabric element (Director or Edge Switch). Modify the switch Domain ID to make it unique. **3 = Incompatible zoning configurations.** The same name is applied to a zone for the switch and another fabric element (Director or Edge Switch), but the zones contain different zone members. Modify the zone name to make it unique, or ensure zones with the same name contain identical zone members. **4 = Build fabric protocol error.** A protocol error was detected during incorporation of the switch into the fabric. Disconnect the E_Port link, reconnect the link, and initial program load (IPL) the switch. If the condition persists, perform the data collection procedure and return the Zip disk to Hewlett-Packard support personnel. **5 = No principal switch.** No Director or Edge Switch in the fabric can become the principal switch. Modify the switch priority to any value other than 255. **6 = No response from attached switch (hello timeout).** The switch periodically verifies operation of attached fabric elements (Director or Edge Switch). The switch E_Port (at the operational switch) times out and segments if the attached device does not respond. Check the status of the attached Director or Edge Switch. If the condition persists, perform the data collection procedure (at the attached device) and return the Zip disk to Hewlett-Packard support personnel. **7 = ELP retransmission failure timeout.** A switch that exhibits a hardware or link failure attempted to join a fabric and transmitted multiple exchange link protocol (ELP) frames to a fabric element (Director or Edge Switch). However, because of the problem, the switch did not receive responses to the ELP frames, and did not receive a fabric login (FLOGI) frame. After five ELP transmission attempts, the switch E_Port (failed switch) times out and segments. Refer to MAP 0000: Start MAP to perform hardware fault isolation at the failed switch. **7 = ELP retransmission failure timeout.** A switch that exhibits a hardware or link failure attempted to join a fabric and transmitted multiple exchange link protocol (ELP) frames to a fabric element (Director or Edge Switch). However, because of the problem, the switch did not receive responses to the ELP frames, and did not receive a fabric login (FLOGI) frame. After five ELP transmission attempts, the switch E_Port (failed switch) times out and segments. Refer to MAP 0000: Start MAP to perform hardware fault isolation at the failed switch.

Event Code: 070 (continued)							
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Event Code: 071	
Message:	Switch is isolated.
Severity:	Informational.
Explanation:	The switch is isolated from other fabric elements (Director or Edge Switch). This event code is accompanied by one or more **070** event codes. Refer to the event data for the segmentation reason.
Action:	Action depends on the segmentation reason specified in the event data.
Event Data:	The first byte of event data (byte **0**) specifies the E_Port number. The fifth byte (byte **4**) specifies the segmentation reason as follows: **1 = Incompatible operating parameters.** Ether the resource allocation time out value (R_A_TOV) or error detect time out value (E_D_TOV) is inconsistent between the switch and another fabric element (Director or Edge Switch). Modify the R_A_TOV and E_D_TOV to make the values consistent for all fabric Directors and Edge Switches. **2 = Duplicate domain ID.** The switch has the same preferred domain ID as another fabric element (Director or Edge Switch). Modify the switch's Domain ID to make it unique. **3 = Incompatible zoning configurations.** The same name is applied to a zone for the switch and another fabric element (Director or Edge Switch), but the zones contain different zone members. Modify the zone name to make it unique, or ensure zones with the same name contain identical zone members.

Event Code: 071 (continued)							
Event Data (continued):	**4 = Build fabric protocol error.** A protocol error was detected during incorporation of the switch into the fabric. Disconnect the E_Port link, reconnect the link, and IPL the switch. If the condition persists, perform the data collection procedure and return the Zip disk to Hewlett-Packard support personnel. **5 = No principal switch.** No Director or Edge Switch in the fabric can become the principal switch. Modify the switch priority to any value other than 255. **6 = No response from attached switch (hello timeout).** The switch periodically verifies operation of attached fabric elements (Director or Edge Switch). The switch E_Port (at the operational switch) times out and segments if the attached device does not respond. Check the status of the attached Director or Edge Switch. If the condition persists, perform the data collection procedure (at the attached device) and return the Zip disk to Hewlett-Packard support personnel. **7 = ELP retransmission failure timeout.** A switch that exhibits a hardware or link failure attempted to join a fabric and transmitted multiple ELP frames to a fabric element (Director or Edge Switch). However, because of the problem, the switch did not receive responses to the ELP frames, and did not receive an FLOGI frame. After five ELP transmission attempts, the switch E_Port (failed switch) times out and segments. Refer to MAP 0000: Start MAP to perform hardware fault isolation at the failed switch.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Event Code: 072							
Message:	E_Port connected to unsupported switch.						
Severity:	Informational.						
Explanation:	The switch is attached (through an ISL) to an incompatible fabric element (Director or Edge Switch).						
Action:	Disconnect the ISL.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Event Code: 073							
Message:	Fabric initialization error.						
Severity:	Informational.						
Explanation:	An error was detected during the fabric initialization sequence, most likely caused by frame delivery errors. Event data is intended for engineering evaluation.						
Action:	Perform the data collection procedure and return the Zip disk to Hewlett-Packard support personnel.						
Event Data:	Byte **0** = error reason code for engineering evaluation. Byte **1** = reserved. Bytes **4** - **9** = port numbers for which problems were detected.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Event Code: 074							
Message:	ILS frame delivery error threshold exceeded.						
Severity:	Informational.						
Explanation:	Fabric controller frame delivery errors exceeded an E_Port threshold and caused fabric initialization problems (**073** event code). Most fabric initialization problems are caused by control frame delivery errors, as indicated by this code. Event data is intended for engineering evaluation.						
Action:	Perform the data collection procedure and return the Zip disk to Hewlett-Packard support personnel.						
Event Data:	Byte **0** = E_Port number reporting the problem. Byte **1** = reserved.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Event Code: 080							
Message:	Unauthorized world-wide name.						
Severity:	Informational.						
Explanation:	The world-wide name of the device or switch plugged in the indicated port is not authorized for that port.						
Action:	Change the port binding definition or plug the correct device or switch into this port.						
Event Data:	Byte **0** = Port number reporting the unauthorized connection. Bytes **1** - **3** = reserved. Bytes **4** - **11** = WWN of the unauthorized device or fabric element.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔	✔		✔	

Event Code: 081	
Message:	Invalid attachment.
Severity:	Informational.
Explanation:	A switch port recognized an incompatibility with the attached fabric element or device and isolated the port. An isolated port does not transmit Class 2, Class 3, or Class F traffic. Refer to the event data for the reason.
Action:	Action depends on the reason specified in the event data.
Event Data:	The first byte of event data (byte **0**) specifies the port number. The fifth byte (byte **4**) specifies the isolation reason as follows: **1 = Unknown -** Isolation reason is unknown, but probably caused by failure of a device attached to the switch through an E_Port connection. Fault isolate the failed device or contact support personnel to report the problem. **2 = ISL connection not allowed -** The port connection conflicts with the configured port type. Change the port type to **F_Port** if the port is cabled to a device, or **E_Port** if the port is cabled to a fabric element to form an ISL. **3 = Incompatible switch -** The switch returned a *Process ELP Reject - Unable to Process* reason code because the attached fabric element is not compatible. Set the switch operating mode to **Homogeneous Fabric 1.0** if connected to a HP product. Set the switch operating mode to **Open Fabric 1.0** if connected to an open-fabric compliant product manufactured by a different vendor. **4 = Incompatible switch -** The switch returned a *Process ELP Reject - Invalid Revision Level* reason code because the attached fabric element is not compatible. Set the switch operating mode to **Homogeneous Fabric 1.0** if connected to a HP product. Set the switch operating mode to **Open Fabric 1.0** if connected to an open-fabric compliant product manufactured by a different vendor. **5 = Loopback plug connected -** A loopback plug is connected to the port with no diagnostic test running. Remove the loopback plug. **6 = N_Port connection not allowed -** The switch is connected to a fabric element through a port configured as an F_Port. Change the port type to **E_Port**. **7 = Non-HP switch at other end** - The attached fabric element is not a HP product. Set the switch operating mode to **Open Fabric 1.0** if connected to an open-fabric compliant product manufactured by a different vendor. **A = Unauthorized port binding WWN -** The device WWN or nickname used to configure port binding for this port is not valid. Reconfigure the port with the WWN or nickname authorized for the attached device.

	B = Unresponsive node - The attached node did not respond, resulting in a G_Port ELP timeout. Check the status of the attached device and clean the link's fiber-optic components (cable and connectors). If the problem persists, contact support personnel to report the problem. **C = ESA security mismatch -** Processing of the Exchange Security Attribute (ESA) frame detected a security feature mismatch. The fabric binding and switch binding parameters for this switch and the attached fabric element must agree. Ensure the parameters for both fabric elements are compatible or disable the fabric and switch binding features. **D = Fabric binding mismatch -** Fabric binding is enabled and an attached fabric element has an incompatible fabric membership list. Update the fabric membership list for both fabric elements to ensure compatibility or disable the fabric binding feature. **E = Authorization failure reject -** The fabric element connected to the switch through an ISL detected a security violation. As a result, the switch received a generic reason code and set the port to an invalid attachment state. Check the port status of the attached fabric element and clean the link's fiber-optic components (cable and connectors). If the problem persists, contact support personnel to report the problem. **F = Unauthorized switch binding WWN -** Switch binding is enabled and an attached device or fabric element has an incompatible switch membership list. Update the switch membership list for the switch and the attached device or fabric element to ensure compatibility or disable the switch binding feature.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

<table>
<tr><th colspan="8">Event Code: 120</th></tr>
<tr><td>Message:</td><td colspan="7">Error detected while processing system management command.</td></tr>
<tr><td>Severity:</td><td colspan="7">Informational.</td></tr>
<tr><td>Explanation:</td><td colspan="7">This event occurs when the switch receives an HAFM command that violates specified boundary conditions, typically as a result of a network error. The switch rejects the command, drops the switch-to-HAFM server Ethernet link, and forces error recovery processing. When the link recovers, the command can be retried.</td></tr>
<tr><td>Action:</td><td colspan="7">No action is required for an isolated event. If this event persists, perform a data collection for this switch using the HAFM application. Perform the data collection procedure and return the Zip disk to Hewlett-Packard support personnel.</td></tr>
<tr><td>Event Data:</td><td colspan="7">No supplementary data included with the event.</td></tr>
<tr><td rowspan="3">Distribution:</td><td colspan="2">Switch</td><td colspan="3">HAFM Server</td><td colspan="2">Host</td></tr>
<tr><td>EWS Event Log</td><td>System Error LED</td><td>Event Log</td><td>E-Mail</td><td>Call Home</td><td>Sense Info</td><td>Link Incident</td></tr>
<tr><td>✔</td><td></td><td>✔</td><td></td><td></td><td></td><td></td></tr>
</table>

<table>
<tr><th colspan="8">Event Code: 121</th></tr>
<tr><td>Message:</td><td colspan="7">Zone set activation failed - zone set too large.</td></tr>
<tr><td>Severity:</td><td colspan="7">Informational.</td></tr>
<tr><td>Explanation:</td><td colspan="7">This event occurs when the switch receives a zone set activation command that exceeds the size supported by the switch. The switch rejects the command, drops the switch-to-HAFM server Ethernet link, and forces error recovery processing. When the link recovers, the command can be modified and retried.</td></tr>
<tr><td>Action:</td><td colspan="7">Reduce the size of the zone set to conform to the limit specified, then retry the activation command.</td></tr>
<tr><td>Event Data:</td><td colspan="7">No supplementary data included with the event.</td></tr>
<tr><td rowspan="3">Distribution:</td><td colspan="2">Switch</td><td colspan="3">HAFM Server</td><td colspan="2">Host</td></tr>
<tr><td>EWS Event Log</td><td>System Error LED</td><td>Event Log</td><td>E-Mail</td><td>Call Home</td><td>Sense Info</td><td>Link Incident</td></tr>
<tr><td>✔</td><td></td><td>✔</td><td></td><td></td><td></td><td></td></tr>
</table>

Power Supply Events (200 through 299)

Event Code: 200							
Message:	Power supply AC voltage failure.						
Severity:	Major.						
Explanation:	Alternating current (AC) input to the indicated power supply is disconnected or AC circuitry in the power supply failed. The second power supply assumes the full operating load for the switch.						
Action:	Ensure the power supply is connected to facility AC power, and verify operation of the facility power source. If the AC voltage does not recover (indicated by event code **203**), replace the failed power supply. Perform the data collection procedure and return the Zip disk and failed power supply to Hewlett-Packard support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Event Code: 201							
Message:	Power supply DC voltage failure.						
Severity:	Major.						
Explanation:	Direct current (DC) circuitry in the power supply failed. The second power supply assumes the full operating load for the switch.						
Action:	Replace the failed power supply. Perform the data collection procedure and return the Zip disk and failed power supply to Hewlett-Packard support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Event Code: 203							
Message:	Power supply AC voltage recovery.						
Severity:	Informational.						
Explanation:	AC voltage recovered for the power supply. Both power supplies adjust to share operating load for the switch.						
Action:	No action required.						
Event Data:	No supplementary data included with the event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Event Code: 204							
Message:	Power supply DC voltage recovery.						
Severity:	Informational.						
Explanation:	DC voltage recovered for the power supply. Both power supplies adjust to share operating load for the switch.						
Action:	No action required.						
Event Data:	No supplementary data included with the event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Event Code: 206							
Message:	Power supply removed.						
Severity:	Informational.						
Explanation:	A power supply was removed while the Switch was powered on and operational. The second power supply assumes the full operating load for the switch.						
Action:	No action required or install an operational power supply.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Event Code: 207							
Message:	Power supply installed.						
Severity:	Informational.						
Explanation:	A redundant power supply was installed with the switch powered on and operational. Both power supplies adjust to share operating load for the switch.						
Action:	No action required.						
Event Data:	No supplementary data included with the event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Fan Module Events (300 through 399)

Event Code: 300							
Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	One cooling fan (out of six) failed or is rotating at insufficient angular velocity. The remaining fans are operational. The amber LED illuminates at the rear of the power supply assembly associated with the failed fan.						
Action:	Replace the power supply assembly containing the indicated fan module.						
Event Data:	The first byte of event data (byte **0**) specifies the failed fan number (**0** through **5** inclusive).						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Event Code: 301							
Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	Two cooling fans (out of six) failed or are rotating at insufficient angular velocity. The remaining fans are operational. The amber LED illuminates at the rear of the power supply assembly (or assemblies) associated with the failed fans.						
Action:	Replace the power supply assembly (or assemblies) containing the indicated fan modules.						
Event Data:	The first byte of event data (byte **0**) specifies the failed fan numbers (**0** through **5** inclusive).						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Event Code: 302							
Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	Three cooling fans (out of six) failed or are rotating at insufficient angular velocity. The remaining fans are operational. The amber LED illuminates at the rear of the power supply assembly (or assemblies) associated with the failed fans.						
Action:	Replace the power supply assembly (or assemblies) containing the indicated fan modules.						
Event Data:	The first byte of event data (byte **0**) specifies the failed fan numbers (**0** through **5** inclusive).						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Event Code: 303							
Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	Four cooling fans (out of six) failed or are rotating at insufficient angular velocity. The remaining fans are operational. The amber LED illuminates at the rear of both power supply assemblies.						
Action:	Replace both power supply assemblies.						
Event Data:	The first byte of event data (byte **0**) specifies the failed fan numbers (**0** through **5** inclusive).						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Event Code: 304							
Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	Five cooling fans (out of six) failed or are rotating at insufficient angular velocity. The remaining fan is operational. The amber LED illuminates at the rear of both power supply assemblies.						
Action:	Replace both power supply assemblies.						
Event Data:	The first byte of event data (byte **0**) specifies the failed fan numbers (**0** through **5** inclusive).						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Event Code: 305							
Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	All six cooling fans failed or are rotating at insufficient angular velocity. The amber LED illuminates at the rear of both power supply assemblies.						
Action:	Replace both power supply assemblies.						
Event Data:	The first byte of event data (byte **0**) specifies the failed fan numbers (**0** through **5** inclusive).						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

<table>
<tr><th colspan="8">Event Code: 310</th></tr>
<tr><td>Message:</td><td colspan="7">Cooling fan propeller recovered.</td></tr>
<tr><td>Severity:</td><td colspan="7">Informational.</td></tr>
<tr><td>Explanation:</td><td colspan="7">One cooling fan (out of six) recovered or the associated power supply assembly was replaced. All fans are operational.</td></tr>
<tr><td>Action:</td><td colspan="7">No action required.</td></tr>
<tr><td>Event Data:</td><td colspan="7">The first byte of event data (byte <b>0</b>) specifies the recovered fan number (<b>0</b> through <b>5</b> inclusive).</td></tr>
<tr><td rowspan="3">Distribution:</td><td colspan="2">Switch</td><td colspan="3">HAFM Server</td><td colspan="2">Host</td></tr>
<tr><td>EWS Event Log</td><td>System Error LED</td><td>Event Log</td><td>E-Mail</td><td>Call Home</td><td>Sense Info</td><td>Link Incident</td></tr>
<tr><td>✓</td><td></td><td>✓</td><td></td><td></td><td></td><td></td></tr>
</table>

<table>
<tr><th colspan="8">Event Code: 311</th></tr>
<tr><td>Message:</td><td colspan="7">Cooling fan propeller recovered.</td></tr>
<tr><td>Severity:</td><td colspan="7">Informational.</td></tr>
<tr><td>Explanation:</td><td colspan="7">Two cooling fans (out of six) recovered or the associated power supply assembly (or assemblies) were replaced. All fans are operational.</td></tr>
<tr><td>Action:</td><td colspan="7">No action required.</td></tr>
<tr><td>Event Data:</td><td colspan="7">The first byte of event data (byte <b>0</b>) specifies the recovered fan numbers (<b>0</b> through <b>5</b> inclusive).</td></tr>
<tr><td rowspan="3">Distribution:</td><td colspan="2">Switch</td><td colspan="3">HAFM Server</td><td colspan="2">Host</td></tr>
<tr><td>EWS Event Log</td><td>System Error Indicator</td><td>Event Log</td><td>E-Mail</td><td>Call Home</td><td>Sense Info</td><td>Link Incident</td></tr>
<tr><td>✓</td><td></td><td>✓</td><td></td><td></td><td></td><td></td></tr>
</table>

Event Code: 312							
Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	Three cooling fans (out of six) recovered or the associated power supply assembly (or assemblies) were replaced. All fans are operational.						
Action:	No action required.						
Event Data:	The first byte of event data (byte **0**) specifies the recovered fan numbers (**0** through **5** inclusive).						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Event Code: 313							
Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	Four cooling fans (out of six) recovered or both power supply assemblies were replaced. All fans are operational.						
Action:	No action required.						
Event Data:	The first byte of event data (byte **0**) specifies the recovered fan numbers (**0** through **5** inclusive).						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Event Code: 314							
Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	Five cooling fans (out of six) recovered or both power supply assemblies were replaced. All fans are operational.						
Action:	No action required.						
Event Data:	The first byte of event data (byte **0**) specifies the recovered fan numbers (**0** through **5** inclusive).						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Event Code: 315							
Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	All six cooling fans recovered or both power supply assemblies were replaced. All fans are operational.						
Action:	No action required.						
Event Data:	The first byte of event data (byte **0**) specifies the recovered fan numbers (**0** through **5** inclusive).						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

CTP Card Events (400 through 499)

Event Code: 400							
Message:	Power-up diagnostics failure.						
Severity:	Major.						
Explanation:	Power-on self tests (POSTs) detected a faulty field-replaceable unit (FRU) as indicated by the event data.						
Action:	If a CTP card failure is indicated, replace the switch. If a fan or power supply failure is indicated, replace the power supply assembly. Perform the data collection procedure and return the Zip disk to Hewlett-Packard support personnel.						
Event Data:	Byte **0** = FRU code as follows: **02** = CTP card, **05** = cooling fan, **06** = power supply assembly. Byte **1** = FRU slot number.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Event Code: 410							
Message:	Switch reset.						
Severity:	Informational.						
Explanation:	The switch reset due to system power-up, IML, or manual reset. A software reset can occur automatically after a firmware fault (event code **411**), or be user-initiated. Event data indicates the type of reset.						
Action:	No action required.						
Event Data:	Byte **0** = reset type as follows: **00** = power-on, **02** = IML, **04** = reset.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

<table>
<tr><th colspan="8">Event Code: 411</th></tr>
<tr><td>Message:</td><td colspan="7">Firmware fault.</td></tr>
<tr><td>Severity:</td><td colspan="7">Major.</td></tr>
<tr><td>Explanation:</td><td colspan="7">Switch firmware encountered an unexpected condition and dumped operating state information to FLASH memory for retrieval and analysis. The dump file automatically transfers from the switch to the HAFM server, where it is stored for later retrieval through the data collection procedure.
The switch performs a software reset, during which all attached Fibre Channel devices are momentarily disrupted, log out, and log back in.</td></tr>
<tr><td>Action:</td><td colspan="7">Perform the data collection procedure and return the Zip disk to Hewlett-Packard support personnel.</td></tr>
<tr><td>Event Data:</td><td colspan="7">Bytes 0 through 3 = fault identifier, least significant byte first.</td></tr>
<tr><td rowspan="3">Distribution:</td><td colspan="2">Switch</td><td colspan="3">HAFM Server</td><td colspan="2">Host</td></tr>
<tr><td>EWS Event Log</td><td>System Error LED</td><td>Event Log</td><td>E-Mail</td><td>Call Home</td><td>Sense Info</td><td>Link Incident</td></tr>
<tr><td>✔</td><td>✔</td><td>✔</td><td>✔</td><td>✔</td><td>✔</td><td></td></tr>
</table>

Event Code: 421							
Message:	Firmware download complete.						
Severity:	Informational.						
Explanation:	A switch firmware version was downloaded from the HAFM Server or embedded web server. The event data indicates the firmware version in hexadecimal format ***xx.yy.zz bbbb***, where *xx* is the release level, ***yy*** is the maintenance level, ***zz*** is the interim release level, and ***bbbb*** is the build ID.						
Action:	No action required.						
Event Data:	Bytes **0** and **1** = release level (**xx**). Byte **2** = always a period. Bytes **3** and **4** = maintenance level (**yy**). Byte **5** = always a period. Bytes **6** and **7** = interim release level (**zz**). Byte **8** = always a space. Bytes **9** through **12** = build ID (**bbbb**).						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Event Code: 423							
Message:	CTP firmware download initiated.						
Severity:	Informational.						
Explanation:	The HAFM server initiated download of a new firmware version to the switch.						
Action:	No action required.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Event Code: 433							
Message:	Non-recoverable Ethernet fault.						
Severity:	Major.						
Explanation:	A non-recoverable Ethernet interface failure was detected and the LAN connection to the HAFM server or Internet was terminated. No failure information or event codes are reported outside the switch. Although Fibre Channel port functionality is not affected, the switch cannot be monitored or configured.						
Action:	Replace the switch.						
Event Data:	Byte **0** = LAN error type as follows: **01** = hard failure, **04** = registered fault. Byte **1** = LAN error subtype (internally defined). Byte **2** = LAN fault identifier (internally defined).						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Event Code: 440							
Message:	Embedded port hardware failed.						
Severity:	Major.						
Explanation:	The embedded port hardware detected a fatal CTP error.						
Action:	Replace the switch.						
Event Data:	Byte **0** = CTP slot position (**00**). Byte **1** = engineering reason code Bytes **4** through **7** = elapsed millisecond tick count.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Event Code: 442							
Message:	Embedded port anomaly detected.						
Severity:	Informational.						
Explanation:	The switch detected a deviation in the normal operating mode or status of the embedded port.						
Action:	No action required. An additional event code is generated if this incident exceeds an error threshold or results in a port failure.						
Event Data:	Byte **0** = port number. Byte **1** = engineering reason code.port. Bytes **4** through **7** = elapsed millisecond tick count. Bytes **8** and **9** = high-availability error callout #1. Bytes **10** and **11** = high-availability error callout #2. Byte **12** = detecting port. Byte **13** = connected port. Bytes **16** and **17** = high-availability error callout #3. Bytes **18** and **19** = high-availability error callout #4.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Event Code: 445							
Message:	ASIC detected a system anomaly.						
Severity:	Informational.						
Explanation:	The application-specific integrated chip (ASIC) detected a deviation in the normal operating mode or operating status of the switch.						
Action:	No action required. An additional event code is generated if this incident exceeds an error threshold that results in a system event.						
Event Data:	Byte **0** = port number. Byte **1** = engineering reason code.port. Bytes **4** through **7** = elapsed millisecond tick count. Bytes **8** and **9** = high-availability error callout #1. Bytes **10** and **11** = high-availability error callout #2. Byte **12** = detecting port. Byte **13** = connected port. Bytes **16** and **17** = high-availability error callout #3. Bytes **18** and **19** = high-availability error callout #4.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

<table>
<tr><th colspan="8">Event Code: 453</th></tr>
<tr><td>Message:</td><td colspan="7">New feature key installed.</td></tr>
<tr><td>Severity:</td><td colspan="7">Informational.</td></tr>
<tr><td>Explanation:</td><td colspan="7">This event occurs when a new feature key is installed from the HAFM server or EWS interface. The switch performs an IPL when the feature key is enabled. Event data indicates which feature or features are installed.</td></tr>
<tr><td>Action:</td><td colspan="7">No action required.</td></tr>
<tr><td>Event Data:</td><td colspan="7">Byte <b>0</b> = feature description as follows: <b>00</b> through <b>04</b> = Flexport, <b>06</b> = open-system management server.
Byte <b>1</b> = feature description as follows: <b>06</b> = SANtegrity.</td></tr>
<tr><td rowspan="3">Distribution:</td><td colspan="2">Switch</td><td colspan="3">HAFM Server</td><td colspan="2">Host</td></tr>
<tr><td>EWS Event Log</td><td>System Error LED</td><td>Event Log</td><td>E-Mail</td><td>Call Home</td><td>Sense Info</td><td>Link Incident</td></tr>
<tr><td>✔</td><td></td><td>✔</td><td></td><td></td><td></td><td></td></tr>
</table>

Port Events (500 through 599)

Event Code: 506							
Message:	Fibre Channel port failure.						
Severity:	Major.						
Explanation:	A Fibre channel port failed. The amber LED corresponding to the port illuminates to indicate the failure. Other ports remain operational if their LEDs are extinguished.						
Action:	Perform the data collection procedure and return the Zip disk to Hewlett-Packard support personnel. Perform a switch reset. If the problem persists, replace the switch.						
Event Data:	Byte **0** = port number (**00** through **23**). Byte **1** = engineering reason code. Bytes **4** through **7** = elapsed millisecond tick count. Bytes **8** through **11** = reason code specific. Byte **16** = connector type. Bytes **17** and **18** = transmitter technology. Byte **19** = distance capabilities. Byte **20** = supported transmission media. Byte **21** and **22** = speed capability and configuration.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Event Code: 507							
Message:	Loopback diagnostics port failure.						
Severity:	Informational.						
Explanation:	A loopback diagnostic test detected a Fibre Channel port failure.						
Action:	No action required. An event code **506** is generated if this diagnostic failure results in a hard port failure.						
Event Data:	Byte **0** = port number (**00** through **23**). Byte **1** = engineering reason code. Bytes **4** through **7** = elapsed millisecond tick count. Bytes **8** through **11** = reason code specific. Byte **12** = test type.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Event Code: 508							
Message:	Fibre Channel port anomaly detected.						
Severity:	Informational.						
Explanation:	The CTP detected a deviation in the normal operating mode or status of the indicated Fibre Channel port.						
Action:	No action required. An event code **506** is generated if this anomaly results in a hard port failure.						
Event Data:	Byte **0** = port number (**00** through **23**). Byte **1** = anomaly reason code. Bytes **4** through **7** = elapsed millisecond tick count. Bytes **8** and **9** = high-availability error callout #1. Bytes **10** and **11** = high-availability error callout #2. Byte **12** = detecting port. Byte **13** = connected port. Bytes **16** and **17** = high-availability error callout #3. Bytes **18** and **19** = high-availability error callout #4.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Event Code: 510							
Message:	SFP optical transceiver hot-insertion initiated.						
Severity:	Informational.						
Explanation:	Installation of a small form factor pluggable (SFP) optical transceiver was initiated with the switch powered on and operational. The event indicates that operational firmware detected the presence of the transceiver.						
Action:	No action required.						
Event Data:	Byte **0** = port number (**00** through **23**). Bytes **4** through **7** = elapsed millisecond tick count.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Event Code: 512							
Message:	SFP optical transceiver nonfatal error.						
Severity:	Minor.						
Explanation:	Switch firmware detected an SFP optical transceiver non-fatal error.						
Action:	Replace the failed transceiver with a functional transceiver of the same type.						
Event Data:	Byte **0** = port number (**00** through **23**). Byte **1** = engineering reason code. Bytes **4** through **7** = elapsed millisecond tick count.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

<table>
<tr><th colspan="8">Event Code: 513</th></tr>
<tr><td>Message:</td><td colspan="7">SFP optical transceiver hot-removal completed.</td></tr>
<tr><td>Severity:</td><td colspan="7">Informational.</td></tr>
<tr><td>Explanation:</td><td colspan="7">A SFP optical transceiver was removed while the switch was powered on and operational.</td></tr>
<tr><td>Action:</td><td colspan="7">No action required.</td></tr>
<tr><td>Event Data:</td><td colspan="7">Byte <b>0</b> = port number (<b>00</b> through <b>23</b>).
Bytes <b>4</b> through <b>7</b> = elapsed millisecond tick count.</td></tr>
<tr><td rowspan="3">Distribution:</td><td colspan="2">Switch</td><td colspan="3">HAFM Server</td><td colspan="2">Host</td></tr>
<tr><td>EWS Event Log</td><td>System Error LED</td><td>Event Log</td><td>E-Mail</td><td>Call Home</td><td>Sense Info</td><td>Link Incident</td></tr>
<tr><td>✔</td><td></td><td>✔</td><td></td><td></td><td></td><td></td></tr>
</table>

<table>
<tr><th colspan="8">Event Code: 514</th></tr>
<tr><td>Message:</td><td colspan="7">SFP optical transceiver failure.</td></tr>
<tr><td>Severity:</td><td colspan="7">Major.</td></tr>
<tr><td>Explanation:</td><td colspan="7">A SFP optical transceiver failed. The amber LED corresponding to the port illuminates to indicate the failure. Other ports remain operational if their LEDs are extinguished.</td></tr>
<tr><td>Action:</td><td colspan="7">Replace the failed transceiver with a functional transceiver of the same type.</td></tr>
<tr><td>Event Data:</td><td colspan="7">Byte <b>0</b> = port number (<b>00</b> through <b>23</b>).
Byte <b>1</b> = engineering reason code.
Bytes <b>4</b> through <b>7</b> = elapsed millisecond tick count.</td></tr>
<tr><td rowspan="3">Distribution:</td><td colspan="2">Switch</td><td colspan="3">HAFM Server</td><td colspan="2">Host</td></tr>
<tr><td>EWS Event Log</td><td>System Error LED</td><td>Event Log</td><td>E-Mail</td><td>Call Home</td><td>Sense Info</td><td>Link Incident</td></tr>
<tr><td>✔</td><td>✔</td><td>✔</td><td>✔</td><td>✔</td><td>✔</td><td></td></tr>
</table>

Event Code: 523							
Message:	FL_Port open request failed.						
Severity:	Informational.						
Explanation:	When the indicated FL_Port attempted to open a loop device, the port open (OPN) sequence was returned.						
Action:	No action required.						
Event Data:	Byte **0** = port number (**00** through **23**). Byte **1** = arbitrated loop physical address (AL_PA) of the device transmitting the OPN sequence.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Event Code: 524							
Message:	No AL_PA acquired.						
Severity:	Informational.						
Explanation:	Switch cannot allocate an AL_PA of **0** (loop master) for an FC-AL device during loop initialization. The device cannot participate in loop operation.						
Action:	Disconnect the FC-AL device that is loop master.						
Event Data:	Byte **0** = port number (**00** through **23**).						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Event Code: 525							
Message:	FL_Port arbitration timeout.						
Severity:	Informational.						
Explanation:	A switch port could not win loop arbitration within the specified loop protocol time out value (LP_TOV).						
Action:	Switch firmware reinitializes the arbitrated loop. No user action required.						
Event Data:	Byte **0** = port number (**00** through **23**).						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Event Code: 581							
Message:	Implicit incident.						
Severity:	Major.						
Explanation:	An attached open systems interconnection (OSI) server recognized a condition caused by an event that occurred at the server. The event caused an implicit Fibre Channel link incident.						
Action:	A link incident record (LIR) is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to MAP 0000: Start MAP on page 2–6 to perform fault isolation.						
Event Data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
			✔				✔

Event Code: 582							
Message:	Bit error threshold exceeded.						
Severity:	Major.						
Explanation:	An attached OSI server determined the number of code violation errors recognized exceeded the bit error threshold.						
Action:	A LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to MAP 0000: Start MAP on page 2–6 to perform fault isolation.						
Event Data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
			✔				✔

Event Code: 583							
Message:	Loss of signal or loss of synchronization.						
Severity:	Major.						
Explanation:	An attached OSI server recognized a loss-of-signal condition or a loss-of-synchronization condition that persisted for more than the specified receiver-transmitter timeout value (R_T_TOV).						
Action:	A LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to MAP 0000: Start MAP on page 2–6 to perform fault isolation.						
Event Data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
			✔				✔

Event Code: 584							
Message:	Not operational primitive sequence received.						
Severity:	Major.						
Explanation:	An attached OSI server received a not-operational primitive sequence (NOS).						
Action:	A LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to MAP 0000: Start MAP on page 2–6 to perform fault isolation.						
Event Data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
			✔				✔

Event Code: 585							
Message:	Primitive sequence timeout.						
Severity:	Major.						
Explanation:	An attached OSI server recognized either a link reset (LR) protocol timeout or a timeout while waiting for the appropriate response (while in a NOS receive state and after NOS was not longer recognized).						
Action:	A LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to MAP 0000: Start MAP on page 2–6 to perform fault isolation.						
Event Data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
			✔				✔

Event Code: 586							
Message:	Invalid primitive sequence received for current link state.						
Severity:	Major.						
Explanation:	An attached OSI server recognized either a link reset (LR) or a link-reset response (LRR) sequence while in the wait-for-online sequence (OLS) state.						
Action:	A LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to MAP 0000: Start MAP on page 2–6 to perform fault isolation.						
Event Data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
			✔				✔

Thermal Events (800 through 899)

Event Code: 810							
Message:	High temperature warning (CTP card thermal sensor).						
Severity:	Major.						
Explanation:	The thermal sensor associated with a CTP card indicates the warm temperature threshold was reached or exceeded.						
Action:	Replace the failed switch. Perform the data collection procedure and return the Zip disk and faulty switch to Hewlett-Packard support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error Indicator	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Event Code: 811							
Message:	Critically hot temperature warning (CTP card thermal sensor).						
Severity:	Major.						
Explanation:	The thermal sensor associated with a CTP card indicates the hot temperature threshold was reached or exceeded.						
Action:	Replace the failed switch. Perform the data collection procedure and return the Zip disk and faulty switch to Hewlett-Packard support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Glossary

This glossary defines terms used in this manual or related to this product and is not a comprehensive glossary of computer terms.

NUMERICS

8B/10B
A data encoding scheme developed by IBM, translating byte-wide data to an encoded 10-bit format.

10BaseT
An implementation of the Institute of Electrical and Electronics Engineers (IEEE) Ethernet standard on 24-gauge unshielded twisted-pair wiring, a baseband medium at 10 Mbps.

100BaseT
An implementation of the Institute of Electrical and Electronics Engineers (IEEE) Ethernet standard on 24-gauge unshielded twisted-pair wiring, a baseband medium at 100 Mbps.

A

AC
See alternating current.

access
The ability and means necessary to store data in, to retrieve data from, to transfer data into, to communicate with, or to make use of any resource of a storage device, a system, or area such as random access memory (RAM) or a register.

access control
A list of all devices that can access other devices across the network and the permissions associated with that access. *See also* persistent binding; zoning.

access time
The amount of time, including seek time, latency, and controller time, necessary for a storage device to retrieve information.

active configuration
In S/390 mode, the Director or Edge Switch configuration that is determined by the status of the connectivity attributes.

active field-replaceable unit
Active FRU. A FRU that is currently operating as the active, and not the backup FRU. *See also* backup field-replaceable unit.

active FRU
See active field-replaceable unit.

active port address matrix
In S/390 mode, an active port address matrix is the port address matrix that is currently active or operational on an attached Director or Edge Switch. *See also* connectivity capability.

active zone set
A single zone set that is active in a multiswitch fabric and is created when a specific zone set is enabled. This zone set is compiled by checking for undefined zones or aliases. *See also* zone; zone set.

address
(1) To refer to a device or an item of data by its address *(A, I)*. (2) The location in a computer where data is stored. (3) In data communication, the unique code assigned to each device or workstation connected to a network. (4) The identifier of a location, source, or destination *(D)*.

address name
Synonym for port name.

agent
Software that processes queries on behalf of an application and returns replies.

alarm
(1) A notification of an abnormal condition within a system that provides an indication of the location or nature of the abnormality to either a local or remote alarm indicator. (2) A simple network management protocol (SNMP) message notifying an operator of a network or device problem.

alert panel
This panel, located below the navigation control panel, displays an alert symbol that indicates the current state of the switch.

alias
A nickname representing a world-wide name.

allowed connection

In S/390 mode, in a Director or Edge Switch, the attribute that when set, establishes dynamic connectivity capability. *Contrast with* blocked connection. *See* connectivity attribute. *See also* dynamic connectivity; unblocked connection.

allowed port connection

In S/390 mode, this attribute establishes dynamic connectivity capability.

alternating current

AC. Electric current that reverses direction at regular sinusoidal intervals *(D). Contrast with* direct current.

American National Standard Code for Information Interchange

ASCII. A standard character set consisting of 7-bit coded characters (8-bit including parity check) used for information exchange between systems and equipment *(D).*

American National Standards Institute

ANSI. A national organization consisting of producers, consumers, and general interest groups that establishes procedures by which accredited organizations create and maintain industry standards in the United States *(A).*

ANSI

See American National Standards Institute.

API

See application program interface.

application

(1) The use to which a data processing system is put, for example, a payroll application, an airline reservation application, or a network application. (2) A collection of software components used to perform specific types of work on a computer *(D).*

application client

The source object of the small computer system interface (SCSI) commands and destination for the command responses.

application program

(1) A program that is specific to the solution of an application problem. Synonymous with application software. (2) A program written for or by a user that applies to the user's work, such as a program that does inventory control or payroll. (3) A program used to connect and communicate with stations in a network, enabling users to perform application-oriented activities *(I).*

application program interface

API. A set of programming functions and routines that provides access between protocol layers, such as between an application and network services.

application-specific integrated circuit
ASIC. An asynchronous transfer mode (ATM) local area network/ wide area network (LAN/WAN) circuit using cell relay transport technology. ASICs are designed for a specific application or purpose, such as implementing the lower-layer Fibre Channel protocol (FC-0). They are particularly suited to sending video and audio information, as well as text. ASICs differ from general-purpose devices such as memory chips or microprocessors.

archive
(1) To copy files to a long-term storage medium for backup. (2) Removing data, usually old or inactive files, from a system and permanently storing the data on removable media to reclaim system hard disk space.

area
The second byte of the node port (N_Port) identifier.

ASCII
See American National Standard Code for Information Interchange.

ASIC
See application-specific integrated circuit.

attribute
In S/390 mode, the connection status of the address on a configuration matrix: allowed, blocked, or prohibited.

Audit Log
Log summarizing actions (audit trail) made by the user. There are two types of *Audit Logs*: the Director or Edge Switch *Audit Log*, and the HAFM *Audit Log*.

(1) Director or switch *Audit Log*. Log displayed through the Product Manager application that provides a history of all configuration changes made to an individual Director or Edge Switch from the respective Product Manager application, a simple network management protocol (SNMP) management workstation, a Fibre Connection (FICON) or open systems host, or the maintenance port. This information is useful for administrators and users. *Contrast with* HAFM Audit Log. *See also* Event Log; Hardware Log; Link Incident Log; Threshold Alert Log.

(2) *See* HAFM Audit Log.

availability
The accessibility of a computer system or network resource.

B

b
See bit.

B
See byte.

backbone
Cable on which two or more stations or networks may be attached, typically used to link computer networks at one site with those at another. Smaller branch networks are sometimes called ribs.

backplane
The backplane provides direct current (DC) power distribution and connections for all logic cards.

backup field-replaceable unit
Backup FRU. When an active FRU fails, an identical backup FRU takes over operation automatically (failover) to maintain Director or Edge Switch and Fibre Channel link operation. *See also* active field-replaceable unit.

backup FRU
See backup field-replaceable unit.

bandwidth
(1) The amount of data that can be sent over a given circuit. (2) A measure of how fast a network can move information, usually measured in Hertz (Hz).

baud
The unit of signaling speed, expressed as the maximum number of times per second the signal can change the state of the transmission line or other medium. The units of baud are seconds to the negative 1 power. Note: With Fibre Channel scheme, a signal event represents a single transmission bit.

BB_Credit
See buffer-to-buffer credit.

beaconing
Use of light-emitting diodes (LEDs) on ports, port cards, field-replaceable units (FRUs), and switches to aid in the fault-isolation process. When enabled, active beaconing will cause LEDs to flash in order for the user to locate field-replaceable units (FRU's), switches, or directors in cabinets or computer rooms.

ber
See bit error rate.

bezel
A removable panel that covers empty drive bays and port cards.

bidirectional
In Fibre Channel protocol, the capability to simultaneously communicate at maximum speeds in both directions over a link.

bit
Abbreviated as b. (1) Binary digit, the smallest unit of data in computing, with a value of zero or one *(D)*. (2) A bit is the basic data unit of all digital computers. It is usually part of a data byte or data word; however, a single bit can be used to control or read logic ON/OFF functions. (3) A bit is a single digit in a binary number. Bits are the basic unit of information capacity on a computer storage device. Eight bits equals one byte.

bit density
Expressed as bits per inch (bpi), the number of bits that can be written on one inch of track on a disk surface.

bit error rate
Abbreviated as ber. Ratio of received bits that contain errors to total of all bits transmitted.

bits per inch
Abbreviated as bpi. Indicates the density of information on a hard drive.

blocked connection
In S/390 mode, in a Director or Edge Switch, the attribute that, when set, removes the communication capability of a specific port. A blocked address is disabled so that no other address can be connected to it. A blocked attribute supersedes a dedicated or prohibited attribute on the same address. *Contrast with* allowed connection; unblocked connection. *See* connectivity attribute. *See also* dynamic connection; dynamic connectivity.

blocked port
In a Director or Edge Switch, the attribute that when set, removes the communication capability of a specific port. A blocked port continuously transmits the offline sequence.

boot
(1) To start or restart a computer. (2) Loading the operating system.

bpi
See bits per inch.

B_Port
See bridge port.

bps
Bits per second.

Bps

Bytes per second.

bridge

(1) An attaching device that connects two local area network (LAN) segments to allow the transfer of information from one LAN segment to the other. A bridge can connect the LAN segments directly by network adapters and software in a single device, or can connect network adapters in two devices through software and use of a telecommunication link between the two adapters. (2) A functional unit that connects two LANs that use the same logical link control protocol, but may use different media access control protocols *(T)*. *Contrast with* router. (3) A device that connects and passes packets between two network segments that use the same communications protocol.

bridge port

B_Port. (1) In Fibre Channel protocol, a fabric inter-element port used to connect bridge devices with E_Ports on a switch. B_Ports provide a subset of E_Port functionality. (2) A term for a physical interface between the fabric (switch) and a bridge device. The interface is identical to an expansion port (E_Port), but it does not participate in full expansion port protocols. As such, it does not assign domain IDs or participate in routing protocol. *See also* expansion port; fabric port; generic port; node port; segmented expansion port.

British thermal unit

Btu. The quantity of heat required to raise the temperature of one pound of water by one degree Fahrenheit *(D)*.

broadband

Large bandwidth communications channel capable of multiple, parallel high-speed transmissions.

broadcast

In Fibre Channel protocol, to send a transmission to all node ports (N_Ports) on a fabric. *See also* broadcast frame.

broadcast frame

In Fibre Channel protocol, a frame whose destination address specifies all node ports (N_Ports) in the fabric. *See also* broadcast.

Btu

See British thermal unit.

buffer

Storage area for data in transit. Buffers compensate for differences in processing speeds between devices. *See* buffer-to-buffer credit.

buffer-to-buffer credit

BB_Credit. (1) The maximum number of receive buffers allocated to a transmitting node port (N_Port) or fabric port (F_Port). Credit represents the maximum number of outstanding frames that can be transmitted by that N_Port or F_Port without causing a buffer overrun condition at the receiver. (2) The maximum number of frames a port can transmit without receiving a receive ready signal from the receiving device. BB_Credit can be adjustable to provide different levels of compensation.

bypassed port

If a port is bypassed, all serial channel signals route past the port. A device attached to the port cannot communicate with other devices in the loop.

byte

Abbreviated as B. A byte generally equals eight bits, although a byte can equal from four to ten bits. A byte can also be called an octet *See also* octet.

C

call-home

Product feature which enables the HAFM server to automatically contact 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.

cascade

Linking two or more Fibre Channel switches to form a larger switch or fabric. The switched link through fiber cables attached between one or more expansion ports (E_Ports). *See also* expansion port.

CBY

Channel operations running in byte mode. This occurs when a channel is attached to a converter and specifies the I/O operation mode for the channel path under the I/O configuration program (IOCP) channel path identifier (CHPID) statement ‘Type’ parameter. *Contrast with* CVC.

cell

In S/390 mode, in a port address matrix, a cell is the intersection point between a horizontal port address and a vertical port address. A selected cell is indicated by the cell cursor.

chained

Two Director or Edge Switch that are physically attached.

channel

(1) A system element that controls one channel path, and whose mode of operation depends on the type of hardware attached. Each channel controls an I/O interface between the channel control element and the attached control units *(D)*. (2) Point-to-point link that transports data from one point to the other. (3) A connection or socket on the motherboard to controller card. A motherboard may have only one or two channels (primary and secondary). If a motherboard has only one channel, it may be necessary to add a controller card to create a secondary channel.

channel-attached

(1) Pertaining to direct attachment of devices by data I/O channels to a computer. (2) Pertaining to devices attached to a control unit by cables, not telecommunication lines *(D)*. *Synonymous with* local.

channel wrap test

A diagnostic procedure that checks S/390 host-to-director or host-to-switch connectivity by returning the output of the host as input. The test is host-initiated and transmits Fibre Channel frames to a Director or Edge Switch port. A Director or Edge Switch port enabled for channel wrapping echoes the frame back to the host.

Class 2 Fibre Channel service

Provides a connectionless (not dedicated) service with notification of delivery or nondelivery between two node ports (N_Ports).

Class 3 Fibre Channel service

Provides a connectionless (not dedicated) service without notification of delivery or nondelivery between two node ports (N_Ports). *Synonymous with* datagram.

Class F Fibre Channel service

Used by switches to communicate across interswitch links (ISLs) to configure, control, and coordinate a multiswitch fabric.

Class of Fibre Channel service

Defines the level of connection dedication, acknowledgment, and other characteristics of a connection.

command

(1) A character string from an external source to a system that represents a request for system action. (2) A request from a terminal to perform an operation or execute a program. (3) A value sent through an I/O interface from a channel to a control unit that specifies the operation to be performed *(D)*.

communications tray

The communications tray is a sliding tray located in the middle of the Fabricenter cabinet. The communications tray holds the laptop personal computer (PC), zip drive, and zip drive power supply.

community name (SNMP)
A name that represents an simple network management protocol (SNMP) community that the agent software recognizes as a valid source for SNMP requests. A product recognizes a management station as a valid recipient for trap information when the station's community names are configured.

community profile
Information that specifies which management objects are available to what management domain or simple network management protocol (SNMP) community name.

community (SNMP)
A relationship between an simple network management protocol (SNMP) agent and a set of SNMP managers that defines authentication, access control, and proxy characteristics.

component
(1) Hardware or software that is part of a functional unit. (2) A functional part of an operating system; for example, the scheduler or supervisor *(D)*.

concurrent firmware upgrade
Firmware is upgraded without disrupting switch operation.

concurrent maintenance
Ability to perform maintenance tasks, such as removal or replacement of field-replaceable units (FRUs), while a hardware product is operating.

configuration data
The collection of data that results from configuring product and system operating parameters. For example, configuring operating parameters, simple network management protocol (SNMP) agent, zoning configurations, and port configurations through the Product Manager application, results in a collection of configuration data. Configuration data includes: identification data, port configuration data, operating parameters, simple network management protocol (SNMP) configuration, and zoning configuration. A configuration backup file is required to restore configuration data if the control processor (CTP) card in a nonredundant director 2/64 is removed and replaced.

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 with the dedicated bandwidth that is required in a Class 1 Fibre Channel Service (FC-1) point-to-point link.

connectivity
The ability of devices to link together.

connectivity attribute

In S/390 mode, the characteristic that determines port address status for the Director or Edge Switch. *See* allowed connection; blocked connection; connectivity capability; connectivity control; dynamic connection; dynamic connectivity; unblocked connection.

connectivity capability

(1) The capability that allows attachment of a device to a system without requiring physical reconfiguration of either the device or the interconnections. (2) The Director or Edge Switch capability that allows logical manipulation of link connections to provide physical device attachment *(D)*. *See also* active port address matrix; connectivity attribute; connectivity control.

connectivity control

In S/390 mode, in a Director or Edge Switch, the method used to change port address connectivity attributes and determine the communication capability of the link attached to the port *(D)*. *See also* active port address matrix; connectivity attribute; connectivity capability.

connector

Synonym for optical fiber connector.

console

See personal computer; server.

control processor card

CTP card. Circuit card that contains the Director or Edge Switch microprocessor. The CTP card also initializes hardware components of the system after power-on. The card may contain an RJ-45 twisted pair connector. In the Edge Switch, the CTP card is the main circuit board of the switch and is not replaceable (not a FRU).

credit

See buffer-to-buffer credit.

CTP card

See control processor card.

customer support

Synonym for technical support.

CVC

Channel operations running in block mode. This occurs when a channel is attached to a converter. This specifies the I/O operation mode for the channel path under the I/O configuration program (IOCP) channel path identifier (CHPID) statement Type parameter. *Contrast with* CBY.

D

database
A collection of data with a given structure for accepting, storing, and providing on-demand data for multiple users. *(T)*

data directory
Critical information for all managed products (including Directors and Edge Switches). Information stored here includes:

- All configuration data
- All log files
- Call-home settings
- Firmware library
- Zoning library

datagram
Synonym for Class 3 Fibre Channel service.

dB
See decibel.

dBm
Decibels referenced to one milliwatt. Zero dBm equals one milliwatt, with a logarithmic relationship as the value increases *(D)*.

DC
See direct current.

decibel
Abbreviated as dB. A standard unit used to express gain or loss of optical power, expressed as the ratio of input power to output power on a logarithmic basis *(D)*.

default
Pertaining to an attribute, value, or option that is assumed by a system when none is explicitly specified *(D, I)*.

default zone
A zone that contains all attached devices that are not members of a separate active zone.

destination
A point or location, such as a processor, Director or Edge Switch, or server, to which data is transmitted *(D)*.

device
(1) Mechanical, electrical, or electronic hardware with a specific purpose *(D)*. *See also* managed product.

(2) *See* node.

diagnostics
(1) The process of investigating the cause or nature of a problem in a product or system. (2) Procedures or tests used by computer users and service personnel to diagnose hardware or software problems *(D)*.

dialog box
A pop-up window in the user interface with informational messages or fields to be modified or completed with desired options.

direct current
DC. Electric current that continuously flows in one direction *(D)*. *Contrast with* alternating current.

director
An intelligent, highly-available, Fibre Channel switch 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.

diskette
A thin magnetic disk enclosed in a plastic jacket, which is removable from a computer and is used to store and transport data *(D)*.

diskette drive
The hardware mechanism by which a computer reads data from and writes data to removable diskettes *(D)*.

DNS name
Domain name system or domain name service. Host or node name for a device or managed product that is translated to an Internet protocol (IP) address through a domain name server.

domain
A Fibre Channel term describing the most significant byte in the node port (N_Port) identifier for the Fibre Channel device. It is not used in the Fibre Channel small computer system interface (FC-SCSI) hardware path ID. It is required to be the same for all SCSI targets logically connected to a Fibre Channel adapter.

domain ID

Domain identifier. A number that uniquely identifies a switch in a multiswitch fabric. A distinct domain ID is automatically allocated to each switch in the fabric by the principal switch. The preferred domain ID is the domain ID value that a switch requests from the principal switch. If the value has not been allocated to another switch in the fabric, it will be granted by the principal switch and will become the requesting switch's active domain ID. The active domain ID is the domain ID that has been assigned by the principal switch and that a switch is currently using.

domain name server

In TCP/IP, a server program that supplies name-to-address translation by mapping domain name to internet addresses. *(D)*

DRAM

See dynamic random access memory.

drop-down menu

A menu that appears when a heading in a navigation bar is clicked on with the mouse. The objects that appear in the drop-down menus are organize by their headings in the navigation bar.

duplex

In data communication, pertaining to transmission in which data is sent and received at the same time *(D). Contrast with* half duplex.

duplex connector

An optical fiber component that terminates jumper cable fibers in one housing and provides physical keying for attachment to a duplex receptacle *(D).*

duplex receptacle

A fixed or stationary optical fiber component that provides a keyed attachment method for a duplex connector *(D).*

dynamic connection

A connection between two ports, established or removed by the directors and that, when active, appears as one continuous link. *See* connectivity attribute. *See also* allowed connection; blocked connection; connectivity capability; dynamic connectivity; unblocked connection.

dynamic connectivity

The capability that allows connections to be established and removed at any time.

dynamic random access memory

DRAM. Random access memory that resides in a cell comprised of a capacitor and transistor. DRAM data deteriorates (that is, is dynamic) unless the capacitor is periodically recharged by the controlling microprocessor. DRAM is slow, but relatively inexpensive *(D). Contrast with* static random access memory.

E

EAF

See enhanced availability feature.

EDI

See electronic data interchange.

E_D_TOV

See error-detect time-out value.

EE-PROM

See electronically erasable programmable read-only memory.

EIA

See Electronic Industries Association.

electromagnetic interference

EMI. Undesirable electromagnetic emissions generated by solar activity, lightning, and electronic devices. The emissions interfere with or degrade the performance of another electronic device *(D)*.

electronically erasable programmable read-only memory

A memory chip that can be loaded with data and later erased and loaded with update information.

electronic data interchange

EDI. The electronic transfer of preformatted business documents, such as purchase orders and bills of lading, between trading partners.

Electronic Industries Association

EIA. The governing body that publishes recommended standards for physical devices and associated interfaces. For example, RS-232 is the EIA standard that defines computer serial port connectivity *(D)*. *See also* Telecommunications Industry Association.

electronic mail

E-mail. Any communications service that permits the electronic transmission and storage of messages and attached or enclosed files.

electrostatic discharge

ESD. The undesirable discharge of static electricity that can damage or degrade electronic circuitry *(D)*.

e-mail

See electronic mail.

embedded web server interface
The interface provides a graphical user interface (GUI) similar to the Product Manager application, and supports Director or Edge Switch configuration, statistics monitoring, and basic operations. With Director or Edge Switch firmware installed, administrators or operators with a browser-capable personal computer (PC) and an Internet connection can monitor and manage the Director or Edge Switch through an embedded web server interface.

embedded web server interface timeout
If the embedded web server interface is running but no user activity occurs, (such as viewing different pages, refreshing, or reconfiguring information), the application times out after 30 minutes. The user must log in again. A login dialog box displays if the user attempts to access any pages after the timeout has occurred.

embedded web server interface window
The window for the embedded web server interface. The window is divided into two separate panels: the navigation panel on the left, and the main panel on the right.

EMI
See electromagnetic interference.

enhanced availability feature
EAF. A backup field-replaceable unit (backup FRU) that is ordered and installed to provide redundancy and reduce disruption in case of failure.

enterprise
The entire storage system. The series of computers employed largely in high-volume and multi-user environments such as servers or networking applications; may include single-user workstations required in demanding design, engineering and audio/visual applications.

E_Port
See expansion port.

error-detect time-out value
E_D_TOV. The time the switch waits for an expected response before declaring an error condition.

error log
See Event Log.

error message
Indication that an error has been detected *(D)*.

ESD
See electrostatic discharge.

Ethernet

A widely implemented local area network (LAN) protocol that uses a bus or star topology and serves as the basis for the Institute of Electrical and Electronics Engineers (IEEE) 802.3 standard, which specifies the physical and software layers.

Ethernet hub

A device used to connect the HAFM server and the directors it manages.

event code

A three-digit number that specifies the exact event that occurred. 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 Director or Edge Switch (Director or Edge Switch Event Log) or through the HAFM Services application (HAFM Event Log). There are two *Event Logs*: Director or Edge Switch *Event Log*, and *HAFM Event Log*.

(1) Director or switch *Event Log*. Log displayed through the Product Manager application that provides a history of events for an individual Director or Edge Switch, such as system events, degraded operation, FRU failures, FRU removals and replacements, port problems, Fibre Channel link incidents, and HAFM server-to-product communication problems. All detected software and hardware failures are recorded in the *Event Log*. The information is useful to maintenance personnel for fault isolation and repair verification. *Contrast with* HAFM Event Log. *See also* Audit Log; Hardware Log; Link Incident Log; Threshold Alert Log.

(2) See HAFM Event Log.

exchange

A term that refers to one of the Fibre Channel protocol “building blocks,” composed of one or more nonconcurrent sequences.

expansion port

E_Port. Physical interface on a Fibre Channel switch within a fabric, that attaches to an E_Port on another Fibre Channel switch through an interswitch link (ISL) to form a multiswitch fabric. *See also* bridge port; fabric port; generic port; node port; segmented expansion port.

F

fabric

Entity that interconnects node ports (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. A switch is the smallest entity that can function as a complete switched fabric topology.

fabric element

Any active director, switch, or node in a switched fabric.

fabric login

The process by which node ports (N_Ports) establish their operating parameters. During fabric login, the presence or absence of a fabric is determined, and paths to other N_Ports are mapped. Specific operating characteristics for each port, such as buffer-to-buffer credit (BB_Credit) and data frame size, are also established.

fabric login command

FLOGI. The command that establishes the initial operating parameters and topology for a fabric. The command is accepted by a fabric port (F_Port).

fabric mode

See interoperability mode.

fabric port

F_Port. Physical interface within the fabric that connects to a node port (N_Port) through a point-to-point full duplex connection. *See also* bridge port; expansion port; generic port; node port; segmented expansion port.

fabric services

The services that implement the various Fibre Channel protocol services that are described in the standards. These services include the fabric controller (login server), name server, and management server.

fabric switches

A device which allows the communication between multiple devices using Fibre Channel protocols. A fabric switch enables the sharing bandwidth and end-nodes using basic multiplexing techniques.

failover

Automatic and nondisruptive transition of functions from an active field-replaceable unit (FRU) that has failed to a backup FRU.

FC

See Fibre Channel.

FC-0
The Fibre Channel layer that describes the physical link between two ports, including the transmission media, transmitter and receiver circuitry, and interfaces *(D)*. This consists of a pair of either optical fiber or electrical cables (link media) along with transceiver circuitry which work together to convert a stream of bits at one end of the link to a stream of bits at the other end.

FC-1
Middle layer of the Fibre Channel physical and signaling interface (FC-PH) standard, defining the 8B/10B encoding/decoding and transmission protocol.

FC-2
The Fibre Channel layer that specifies the signaling protocol, rules, and mechanisms required to transfer data blocks. The FC-2 layer is very complex and provides different classes of service, packetization, sequencing, error detection, segmentation, and reassembly of transmitted data *(D)*.

FC-3
The Fibre Channel layer that provides a set of services common across multiple node ports (N_Ports) of a Fibre Channel node. The services are not commonly used and are essentially reserved for Fibre Channel architecture expansion *(D)*.

FC-4
The Fibre Channel layer that provides mapping of Fibre Channel capabilities to upper level protocols (ULP), including Internet protocol (IP) and small computer system interface (SCSI) *(D)*.

FCA
See Fibre Channel Association.

FC adapter
Fibre Channel adapter. *See* host bus adapter.

FCC
Federal Communications Commission.

FCC-IOC
See Fibre Channel I/O controller.

FCFE
See Fibre Channel fabric element.

FCFE-MIB
See Fibre Channel fabric element management information base.

FCIA
See Fibre Channel Industry Association.

FC IP

See Fibre Channel IP address.

FCMGMT

See Fibre Channel management framework integration.

FC-PH

See Fibre Channel physical and signaling interface.

feature key

A unique key to enable additional product features. This key is entered into the Configure Feature Key dialog box in the Product Manager application to activate optional hardware and software features. Upon purchasing a new feature, Hewlett-Packard will provide the feature key to the customer.

fiber

The fiber-optic cable made from thin strands of glass through which data in the form of light pulses is transmitted. It is used for high-speed transmissions over medium (200 m) to long (10 km) distances.

fiber-optic cable

Synonym for optical cable.

fiber optics

The branch of optical technology concerned with the transmission of radiant power through fibers of transparent materials such as glass, fused silica, or plastic *(E)*. Telecommunication applications of fiber optics use optical fibers. A single fiber or a nonspatially aligned fiber bundle is used for each information channel. Such fibers are often called optical fibers to differentiate them from fibers that are used in noncommunication applications *(D)*.

fibre

A generic Fibre Channel term used to cover all transmission media types specified in the Fibre Channel Physical Layer (FC-PH) standard such as optical fiber, copper twisted pair, and copper coaxial cable.

Fibre Channel

FC. Integrated set of standards recognized by American National Standards Institute (ANSI) which defines specific protocols for flexible information transfer. Logically, a point-to-point serial data channel, structured for high performance.

Fibre Channel adapter

FC adapter. *See* host bus adapter.

Fibre Channel address

A 3-byte node port (N_Port) identifier which is unique within the address domain of a fabric. Each port may choose its own identifier, or the identifier may be assigned automatically during fabric login.

Fibre Channel Association
FCA. The FCA is a non-profit corporation consisting of over 150 members throughout the world. Its mission is to nurture and help develop the broadest market for Fibre Channel products through market development, education, standards monitoring, and fostering interoperability among members' products.

Fibre Channel fabric element
FCFE. Any device linked to a fabric.

Fibre Channel fabric element management information base
FCFE-MIB. A table of variables available to network management stations and resident on a switch or director. Through the simple network management protocol (SNMP) these pointers can be manipulates to monitor, control, and configure the switch or director.

Fibre Channel Industry Association
FCIA. A corporation consisting of over 100 computer industry-related companies. Its goal is to provide marketing support, exhibits, and tradeshows for its member companies. The FCIA complements activities of the various standards committees.

Fibre Channel I/O controller
FCC-IOC. In a director, the integrated controller on the control processor (CTP) card dedicated to the task of managing the embedded Fibre Channel port. In a Director or Edge Switch, the FCC-IOC controls the embedded Fibre Channel port and configures the ports' application-specific integrated circuits (ASICs).

Fibre Channel IP address
FC IP. The default FC IP on a new switch is a temporary number divided by the switch's world-wide name (WWN). The system administrator needs to enter a valid IP address.

Fibre Channel management framework integration
FCMGMT. A standard defined by the Fibre Alliance to provide easy management for Fibre Channel-based devices such as switches, hubs, and host-bus adapters.

Fibre Channel physical and signaling interface
FC-PH. The American National Standards Institute (ANSI) document that specifies the FC-0 (physical signaling), FC-1 (data encoding), and FC-2 (frame construct) layers of the Fibre Channel protocol *(D)*.

Fibre Channel standard
American National Standards Institute (ANSI) standard that provides a common, efficient data transport system that supports multiple protocols. The architecture integrates both channel and network technologies, and provides active, intelligent interconnection among devices. All data transmission is isolated from the control protocol, allowing use of point-to-point, arbitrated loop, or switched fabric topologies to meet the needs of an application.

Fibre Connection
FICON. An IBM set of products and services introduced in 1999 that is based on the Fibre Channel Standard. FICON technology uses fiber-optic cables as the data transmission medium, and significantly improves I/O performance (including one Gbps bi-directional data transfer). FICON is designed to coexist with ESCON™ channels, and FICON-to-ESCON control unit connections are supported.

FICON
See Fibre Connection.

FICON Management Server
An optional feature that can be enabled on the Director or Edge Switch or switch through the Product Manager application. When enabled, host control and management of the Director or Edge Switch or switch is provided through an S/390 Parallel Enterprise or 2/Series Server attached to a Director or Edge Switch or switch port.

field-replaceable unit
FRU. Assembly removed and replaced in its entirety when any one of its components fails *(D)*. *See* active field-replaceable unit.

file server
A computer that stores data centrally for network users and manages access to that data.

file transfer protocol
FTP. A transmission control protocol/Internet protocol (TCP/IP) -based client/server protocol used to transfer files to and from a remote host. Does not perform any conversion or translation.

firewall
A networking device that blocks unauthorized access to all or parts of a network.

firewall zoning
Hardware enforced access between F_Ports enforced at the source port. The hardware verifies the destination port against the zone defined for the source port.

firmware
Embedded program code that resides and runs on, for example, directors, switches, and hubs.

FLASH memory
Reusable nonvolatile memory that is organized as segments for writing, and as bytes or words for reading. FLASH memory is faster than read-only memory, but slower than random access memory *(D)*.

FLOGI
See fabric login command.

F_Port
See fabric port.

frame
A variable-length packet of data that is transmitted in frame relay technology.

FRU
See field-replaceable unit.

FTP
See file transfer protocol.

full-duplex
The capability to transmit in two directions simultaneously.

G

gateway address
(1) In transmission control protocol/Internet protocol (TCP/IP), a device that connects two systems that use the same or different protocols. (2) In TCP/IP, the address of a router to which a device sends frames destined for addresses not on the same physical network (for example, not on the same Ethernet) as the sender. The hexadecimal format for the gateway address is XXX.XXX.XXX.XXX.

Gb
See gigabit.

GB
See gigabyte.

Gbps
Acronym for gigabits per second.

generic port
G_Port. Physical interface on a Director or Edge Switch that can function either as a fabric port (F_Port) or an expansion port (E_Port), depending on the port type to which it connects. *See also* bridge port; expansion port; fabric port; node port; segmented expansion port.

GHz
See gigahertz.

gigabit
Gb. A unit of measure for data storage, equal to approximately 134,217,728 bytes. Approximately one eighth of a gigabyte.

gigabyte

GB. A unit of measure for data storage, equal to 1,073,741,824 bytes. Generally approximated as one billion bytes *(D)*.

gigahertz

GHz. One billion cycles per second (Hertz) *(D)*.

G_Port

See generic port.

graphical user interface

GUI. A visually oriented interface where the user interacts with representations of real-world objects displayed on the computer screen. Interactions with such objects produce actions that are intuitive to the user *(D)*.

ground

That portion of a conducting circuit connected to the earth *(D)*.

GSM card

A generic port (G_Port) module card containing shortwave laser ports for multimode fiber-optic cables.

GUI

See graphical user interface.

H

HAFM Audit Log

HAFM *Audit Log*. Log displayed though the HAFM application that provides a history of user actions performed at the HAFM server through the HAFM application. This information is useful for system administrators and users. *See also* Audit Log; HAFM Event Log; HAFM Product Status Log; HAFM Session Log.

HAFM Event Log

HAFM *Event Log*. Log displayed though the HAFM application that provides a record of events or error conditions recorded by the HAFM Services application. Entries reflect the status of the application and managed Directors and Edge Switches. Information associated with a call-home failure is intended for use by maintenance personnel to fault isolate the problem (modem failure, no dial tone, etc.), while information provided in all other entries is generally intended for use by third-level support personnel to fault isolate more significant problems. *See also* HAFM Audit Log; HAFM Product Status Log; HAFM Session Log; Event Log.

HAFM application

HP StorageWorks HA-Fabric Manager (HAFM) application. (1) Software application that is the system management framework providing the user interface for managing Fibre Channel connectivity products. (2) The software application that implements the management user interface for all managed hardware products. The HAFM application can run both locally on the HAFM server and remotely on a user workstation.

HAFM Product Status Log

Enterprise Fabric Connectivity *Product Status Log*. Log displayed though the HAFM application that records an entry when the status of a Director or Edge Switch changes. The log reflects the previous status and current status of a managed product, and indicates the instance of a Product Manager application that should be opened to investigate a problem. The information is useful to maintenance personnel for fault isolation and repair verification. *See also* HAFM Audit Log; HAFM Event Log; HAFM Session Log.

HAFM server

HAFM server. A laptop shipped with the product for the purpose of running the HAFM application and HAFM Services applications.

HAFM Session Log

HAFM *Session Log*. Log displayed though the HAFM application that records a session (login and logout) history for the HAFM server, including the date and time, user name, and network address of each session. This information is useful for system administrators and users. *See also* HAFM Audit Log; HAFM Event Log; HAFM Product Status Log.

half duplex

The capacity to transmit in two directions, but not simultaneously.

hardware

Physical equipment (director, switch, or personal computer) as opposed to computer programs or software.

Hardware Log

Director or switch *Hardware Log*. Log displayed through the Product Manager application that provides a history of FRU removals and replacements (insertions) for an individual Director or Edge Switch. The information is useful to maintenance personnel for fault isolation and repair verification. *See also* Audit Log; Event Log; Link Incident Log; Threshold Alert Log.

HBA

See host bus adapter.

Hertz

Hz. A unit of frequency equal to one cycle per second.

heterogeneous fabric

A fabric containing open-fabric-compliant products from various vendors. *Contrast with* homogeneous fabric.

hexadecimal

A numbering system with base of sixteen; valid numbers use the digits 0 through 9 and characters A through F, where A represents 10 and F represents 15 *(D)*.

high availability

A performance feature characterized by hardware component redundancy and concurrent maintenance. High-availability systems maximize system uptime while providing superior reliability, availability, and serviceability.

homogeneous fabric

A fabric consisting of only one vendor's products. *Contrast with* heterogeneous fabric.

hop

(1) Data transfer from one node to another node. (2) Describes the number of switches that handle a data frame from its origination point through it's destination point.

hop count

The number of hops a unit of information traverses in a fabric.

host bus adapter

HBA. 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.

host processor

(1) A processor that controls all or part of a user application network *(T)*. (2) In a network, the processing unit in which resides the access method for the network *(D)*.

hot pluggable

See concurrent maintenance.

hot spare

See field-replaceable unit.

hot swap

See concurrent maintenance.

hot-swapping

See concurrent maintenance.

HTTP

See hypertext transport protocol.

hub

(1) In Fibre Channel protocol, a device that connects nodes into a logical loop by using a physical star topology. (2) In Ethernet, a device used to connect the HAFM server and the directors it manages.

hyperlink

A predefined link for jumping from one location to another, within the same computer or network site or even to a location at a completely different physical location. Commonly used on the world wide web for navigation, reference, and depth where published text will not suffice.

hypertext transport protocol

HTTP. A simple protocol that allows world wide web pages to be transferred quickly between web browsers and servers.

Hz

See Hertz.

I

ID

See identifier.

identifier

ID. (1) One or more characters used to identify or name a data element and possibly to indicate certain properties of that data element *(D, T)*. (2) A sequence of bits or characters that identifies a program, device, or system to another program, device, or system. *See also* port name.

IEEE

See Institute of Electrical and Electronics Engineers.

IML

See initial machine load.

inband management

Management of the Director or Edge Switch through Fibre Channel. An interface connection to a port card. *Contrast with* out-of-band management.

initial machine load

IML. Hardware reset for all installed control processor (CTP) cards on the Director or Edge Switch. This reset does not affect other hardware. It is initiated by pushing the IML button on a director’s or switch’s operating panel.

initial program load
IPL. The process of initializing the device and causing the operating system to start. An IPL may be initiated through a menu option or a hardware button.

initial program load configuration
IPL configuration. In S/390 mode, information stored in a Director or Edge Switch's nonvolatile memory that contains default configurations. The Director or Edge Switch loads the file for operation when powered on.

Institute of Electrical and Electronics Engineers
IEEE. An organization of engineers and technical professionals that promotes the development and application of electronic technology and allied sciences.

integrated product
Hardware product that is mounted in the Fabricenter cabinet. For example, any Director or Edge Switch shipped with in the Fabricenter cabinet is an integrated product.

interface
(1) A shared boundary between two functional units, defined by functional, signal, or other characteristics. The concept includes the specification of the connection of two devices having different functions *(T)*. (2) Hardware, software, or both, that link systems, programs, or devices *(D)*.

Internet protocol
IP. Network layer for the transmission control protocol/Internet protocol (TCP/IP) protocol used on Ethernet networks. IP provides packet routing, fragmentation, and reassembly through the data link layer *(D)*.

Internet protocol address
IP 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.

interoperability mode
Interop mode. An operating mode set through management software that allows products to operate in homogeneous or heterogeneous fabrics.

interop mode
See interoperability mode.

interrupt
A signal sent by a subsystem to the central processing unit (CPU) that signifies a process has either completed or could not be completed.

interswitch link
ISL. Physical expansion port (E_Port) connection between two directors in a fabric.

interswitch link hop
ISL hop. *See* hop.

IOPS
Input/output operations per second.

IP
See Internet protocol.

IP address
See Internet protocol address.

IPL
See initial program load.

IPL configuration
See initial program load configuration.

ISL
See interswitch link.

ISL hop
Interswitch link hop. *See* hop.

isolated E_Port
Isolated expansion port. *See* segmented expansion port.

isolated expansion port
Isolated E_Port. *See* segmented expansion port.

ITE
Information technology equipment.

J

Java
An object-oriented programming language derived from C++ that produces code that is platform independent. Developed by Sun Microsystems designed for distribution and distributable applications development. Java applications require a program called the Java Virtual Machine (JVM) to execute. JVMs have been developed for many of the mainstream platforms and operating systems.

jumper cable

Optical cable that provides physical attachment between two devices or between a device and a distribution panel. *Contrast with* trunk cable. *See also* optical cable.

K

Kb

See kilobit.

KB

See kilobyte.

kilobit

Kb. A unit of measure for data storage, equaling 1,024 bits, or two to the tenth power. Kilobits are generally approximated as being one thousand bits.

kilobyte

KB. A unit of measure for data storage, equaling 1,024 bytes, or two to the tenth power. Kilobytes are generally approximated as being one thousand bytes.

L

laser

Laser is an acronym for light amplification by stimulated emission of radiation. A device that produces a very powerful narrow beam of coherent light of a single wavelength by simulating the emissions of photons from atoms, molecules, or ions.

latency

Amount of time elapsed between receipt of a data transmission at a switch’s incoming fabric port (F_Port) from the originating node port (N_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.

LCD

Liquid crystal display.

LED

See light-emitting diode.

light-emitting diode

LED. A semiconductor chip that emits visible or infrared light when electricity passes through it. LEDs are used on switch or director field-replaceable units (FRUs) and the front bezel to provide visual indications of hardware status or malfunctions.

LIN

See link incident.

link

Physical connection between two devices on a switched fabric. A link consists of two conductors, one used for sending and the other for receiving, thereby providing a duplex communication path.

link incident

LIN. Interruption to link due to loss of light or other causes. *See also* link incident alerts.

link incident alerts

A user notification, such as a graphic symbol in the Product Manager application *Hardware View* that indicates that a link incident has occurred. *See also* link incident.

Link Incident Log

Director or switch *Link Incident Log*. Log displayed through the Product Manager application that provides a history of Fibre Channel link incidents (with associated port numbers) for an individual Director or Edge Switch. The information is useful to maintenance personnel for isolating port problems (particularly expansion port (E_Port) segmentation problems) and repair verification. *See also* Audit Log; Event Log; Hardware Log; Threshold Alert Log.

LMA

See loader/monitor area.

load balancing

Ability to evenly distribute traffic over multiple interswitch links within a fabric. Load balancing on Hewlett-Packard Directors and Edge Switches takes place automatically.

loader/monitor area

LMA. Code that resides in the loader/monitor area of the control processor (CTP) card. Among other functions, LMA code provides I/O functions available through the maintenance port, operator panel, server interface, terminal window command functions, power up diagnostics, field-replaceable unit (FRU) power-on hours update, and data read/write control, and LMA code/licensed internal code (LIC) download functions *(D)*.

local

Synonym for channel-attached.

logical partition

LPAR. A processor hardware subset defined to support the operation of a system control program, and can be used without affecting any of the applications in another partition *(D)*.

logical port address

In a Director or Edge Switch, the address used to specify port connectivity parameters and to assign link addresses for the attached channels and control units.

logical switch number

LSN. A two-digit number used by the I/O configuration program (IOCP) to identify a Director or Edge Switch *(D)*.

logical unit number

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. Peripherals use LUNs to represent addresses. A small computer system interface (SCSI) device's address can have up to eight LUNs.

login server

Entity within the Fibre Channel fabric that receives and responds to login requests.

longwave

Lasers or light-emitting diodes (LEDs) that emit light with wavelengths around 1300 nm. When using single mode (9 nm) fiber, longwave lasers can be used to achieve lengths greater than 2 Km.

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. *Contrast with* protective plug. *Synonymous with* wrap plug.

loopback test

Test that checks attachment or control unit circuitry, without checking the mechanism itself, by returning the output of the mechanism as input.

LPAR

See logical partition.

LSN

See logical switch number.

LUN

See logical unit number.

M

MAC address

See media access control address.

main panel

(1) The rightmost frame of the windows in HAFM applications. (2) The rightmost frame of the embedded web server interface window. *See also* navigation panel.

maintenance analysis procedure

MAP. A written or online set of procedures that guide maintenance personnel through step-by-step instructions for hardware fault isolation, repair, and verification *(D)*.

maintenance port

Connector on the Director or Edge Switch where a PC running an American National Standard Code for Information Interchange (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 HAFM application. Hewlett-Packard Directors and Edge Switches are managed products. *See also* device.

management information base

MIB. Related set of software objects (variables) containing information about a managed device and accessed via simple network management protocol (SNMP) from a network management station.

management session

A session that exists when a user logs on to the HAFM application. HAFM can support multiple concurrent management sessions. The user must specify the network address of the HAFM application's server at logon time.

MAP

See maintenance analysis procedure.

matrix

See active port address matrix.

Mb

Megabit.

MB

See megabyte.

Mbps

Megabits per second.

MBps

Megabytes per second.

media access control address

MAC address. Hardware address of a node (device) connected to a network.

megabyte

MB. A unit of measure for data storage, equal to 1,048,576 bytes. Generally approximated as one million bytes.

memory

A device or storage system capable of storing and retrieving data.

menu

A list of items displayed on a monitor from which a user can make a selection.

menu bar

The menu bar is located across the top of a monitor window. Pull-down menus are displayed by clicking on the menu bar option with the mouse, or by pressing **Alt** with the underlined letter of the name for the menu bar option *(D)*.

MIB

See management information base.

mirroring

The writing of data to pairs of drives in an array, creating two exact copies of the drive contents. This procedure provides a backup of data in case of a failure.

modem

Modem is an abbreviation for modulator/demodulator. A communication device that converts digital computer data to signals and signals to computer data. These signals can be received or transmitted by the modem via a phone line or other method of telecommunication.

ms

Millisecond.

multimedia

A simultaneous presentation of data in more than one form, such as by means of both visual and audio.

multimode optical fiber

A graded-index or step-index optical fiber that allows more than one mode (light path) to propagate. *Contrast with* singlemode optical fiber.

multiplexer

A device that allows two or more signals to be transmitted simultaneously on a single channel.

multiswitch fabric

Fibre Channel fabric created by linking more than one director or fabric switching device within a fabric.

N

name server

(1) In TCP/IP, *see* domain name server. (2) In Fibre Channel protocol, a server that allows node ports (N_Ports) to register information about themselves. This information allows N_Ports to discover and learn about each other by sending queries to the name server.

name server zoning

Node port (N_Port) access management that allows N_Ports to communicate if and only if they belong to a common name server zone.

NAS

See network-attached storage.

navigation panel

The left side of the embedded web server interface window. Click on words in this panel to display menu options. *See also* main panel.

network

An arrangement of hardware, software, nodes, and connecting branches that comprises a data communication system. The International Organization for Standardization (ISO) seven-layer specification partitions a computer network into independent modules from the lowest (physical) layer to the highest (application) layer *(D)*.

network address

Name or address that identifies a device on a transmission control protocol/Internet protocol (TCP/IP) network. The network address can be either an IP address in dotted-decimal notation (composed of four three-digit octets in the format xxx.xxx.xxx.xxx) or a domain name (as administered on a customer network).

network-attached storage

NAS. Storage connected directly to the network, through a processor and its own operating system. Lacks the processor power to run centralized, shared applications.

network interface card

NIC. An expansion board inserted into a computer so the computer can be connected to a network. Most NICs are designed for specific types of networks, protocols, and medias, although some can serve multiple networks.

network management
The broad subject of managing computer networks. There exists a wide variety of software and hardware products that help network system administrators manage a network. Network management covers a wide area, including security, performance, and reliability.

never principal
The setting that prevents the product from becoming the principal switch for a fabric.

NIC
See network interface card.

nickname
Alternate name assigned to a world-wide name for a node, Director or Edge Switch in the fabric.

node
In Fibre Channel protocol, an end device (server or storage device) that is or can be connected to a switched fabric. *See also* device.

node port
N_Port. Physical interface within an end device that can connect to an fabric port (F_Port) on a switched fabric or directly to another N_Port (in point-to-point communications). *See also* bridge port; expansion port; fabric port; generic port; segmented expansion port.

node port identifier
N_Port ID. In Fibre Channel protocol, a unique address identifier by which an N_Port is uniquely known. It consists of a domain (most significant byte), an area, and a port, each 1 byte long. The N_Port ID is used in the source identifier (S_ID) and destination identifier (D_ID) fields of a Fibre Channel frame.

nondisruptive maintenance
See concurrent maintenance.

nonvolatile random access memory
NV-RAM. RAM that retains its content when the device power is turned off.

N_Port
See node port.

N_Port ID
See node port identifier.

NV-RAM
See nonvolatile random access memory.

O

octet

An 8-bit quantity, often called a byte or word. An octet can equal a byte as long as the byte equals eight bits. *See also* byte.

OEM

See original equipment manufacturer.

offline

Referring to data stored on a medium, such as tape or even paper, that is not available immediately to the user.

offline diagnostics

Diagnostics that only operate in stand alone mode. User operations cannot take place with offline diagnostics running.

offline sequence

OLS. (1) Sequence sent by the transmitting port to indicate that it is attempting to initialize a link and has detected a problem in doing so. (2) Sequence sent by the transmitting port to indicate that it is offline.

offline state

When the switch or director is in the offline state, all the installed ports are offline. The ports transmit an offline sequence (OLS) and they cannot accept a login got connection from an attached device. *Contrast with* online state.

ohm

A unit of electrical resistance equal to that of a conductor in which a current of one ampere is produced by a potential of one volt across the conductor terminals *(D)*.

OLS

See offline sequence.

online

Referring to data stored on the system so it is available immediately to the user.

online diagnostics

Diagnostics that can be run by the customer engineer while the operational software is running. These diagnostics do not impact user operations.

online state

When the switch or director is in the online state, all of the unblocked ports are allowed to log in to the fabric and begin communicating. Devices can connect to the switch or director 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 Architecture

OSI. A model that represents a network as a hierarchical structure of functional layers. Each layer provides a set of functions that can be accessed and used by the layer above. Layers are independent, in that implementation of a layer can be changed without affecting other layers *(D)*.

open systems management server

OSMS. 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 System Interconnection (OSI) device attached to a Director or Edge Switch port.

open systems mode

The mode that is used for Hewlett-Packard or open fabrics. See also operating mode; S/390 mode.

operating mode

In Director or Edge Switch, in managed products, a selection between s/390 and open systems mode. *See also* open systems mode; S/390 mode.

operating system

OS. Software that controls execution of applications and provides services such as resource allocation, scheduling, I/O control, and data management. Most operating systems are predominantly software, but partial hardware implementations are possible *(D, T)*.

Operating System/390

OS/390™. An integrated, open-enterprise server operating system developed by IBM that incorporates a leading-edge and open communications server, distributed data and file services, parallel Sysplex™ support, object-oriented programming, distributed computing environment, and open application interfaces *(D)*.

optical cable

Single fiber, multiple fibers, or a fiber bundle in a structure built to meet optical, mechanical, and environmental specifications *(D, E)*. *See also* jumper cable*;* trunk cable. *Synonymous with* fiber-optic cable.

optical drive backup

A data backup system that uses rewriteable optical cartridges (ROCs) as the storage medium.

optical fiber connector

Synonymous with connector.

ordered set
In Fibre Channel protocol, four 10-bit characters (a combination of data and special characters) providing low-level link functions, such as frame demarcation and signaling between two ends of a link. It provides for initialization of the link after power-on and for some basic recovery functions.

original equipment manufacturer
OEM. A company that has a special relationship with computer producers. OEMs buy components and customize them for a particular application. They sell the customized computer under their own name. OEMs may not actually be the original manufacturers. They are usually the customizers and marketers.

OS
See operating system.

OS/390™
See Operating System/390.

OSI
See Open Systems Architecture.

OSMS
See open systems management server.

out-of-band management
Transmission of management information, using frequencies or channels other than those routinely used for information transfer.

P

packet
In Fibre Channel protocol, 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
A logical component of the interface window. Typically, a heading and/or frame marks the panel as an individual entity of the window. Size and shape of the panel and its data depend upon the purpose of the panel and may or may not be modified.

PC
See personal computer.

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. *See also* access control.

personal computer

PC. A portable computer that consists of a system unit, display, keyboard, mouse, one or more diskette drives, and internal fixed-disk storage *(D)*.

point-to-point

A Fibre Channel protocol topology that provides a single, direct connection between two communication ports. The Director or Edge Switch supports only point-to-point topology.

port

Receptacle on a device to which a cable leading to another device can be attached. Ports provide Fibre Channel connections *(D)*.

port address name

A user-defined symbolic name of 24 characters or less that identifies a particular port address.

port authorization

Feature of the password definition function that allows an administrator to extend operator-level passwords to specific port addresses for each Director or Edge Switch definition managed by a personal computer (PC). Port authorization affects only operator-level actions for active and saved matrices *(D)*.

port name

Name that the user assigns to a particular port through the Product Manager application. *See also* identifier. *Synonymous with* address name.

POST

See power-on self-test.

power-on self-test

POST. Series of diagnostic tests that are run automatically by a device when the power is turned on

preferred domain ID

Configured value that a switch will request from the Principal Switch. If the preferred value is already in use, the Principal Switch will assign a different value.

preventive service planning bucket

PSP bucket. Collected problems after early ship of an IBM product.

principal switch
In a multiswitch 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.

printed wiring assembly
PWA. A thin board on which integrated circuits and other electronic components are placed and connected to each other via thin copper traces.

private device
A loop device that cannot transmit a fabric login command (FLOGI) command to a switch or director, nor communicate with fabric-attached devices. *Contrast with* .public device.

processor complex
A system configuration that consists of all the machines required for operation, for example, a processor unit, a processor controller, a system display, a service support display, and a power and coolant distribution unit.

Product Manager application
Application that implements the management user interface for a Director or Edge Switch. There are two Product Manager applications: Director or Edge Switch Product Manager, and HAFM Product Manager. (1) In the HAFM Services application, the software component that provides a graphical user interface for managing and monitoring HAFM products. When a product instance is opened from the HAFM application *Product View* or Fabric Manager *Topology View*, the corresponding HAFM Product Manager application is invoked.

product name
User-configurable identifier assigned to a managed product. Typically, this name is stored on the product itself. A Director or Edge Switch product name can also be accessed by a simple network management protocol (SNMP) manager as the system name.

Product View
The top-level display in the HAFM software user interface that displays icons of managed products.

prohibited port connection
In a Director or Edge Switch, in S/390 operating mode, an attribute that removes dynamic connectivity capability.

proprietary
Privately owned and controlled. In the computer industry, proprietary is the opposite of open. A proprietary design or technique is one that is owned by a company. It also implies that the company has not divulged specifications that would allow other companies to duplicate the product. Increasingly, proprietary architectures are seen as a disadvantage. Consumers prefer open and standardized architectures, which allow them to mix and match products from different manufacturers.

protective plug

In a fiber-optic environment, a type of duplex connector (or cover) that provides physical protection *(D)*. *Contrast with* loopback plug.

protocol

(1) Set of semantic and syntactic rules that determines the behavior of functional units in achieving communication. (2) In systems network architecture, the meanings of and sequencing rules for requests and responses for managing the network, transferring data, and synchronizing network component states. (3) A specification for the format and relative timing of data exchanged between communicating devices *(D, I)*.

.public device

A loop device that can transmit a fabric login command (FLOGI) to a switch, receive acknowledgement from the switch's login server, register with the switch's name server, and communicate with fabric-attached devices. Public devices communicate with fabric-attached devices through the switch's bridge port (B_Port) connection to a Director or Edge Switch. *Contrast with* private device.

pull-down menu

See drop-down menu.

PWA

See printed wiring assembly.

R

radio frequency interference

RFI. Electromagnetic radiation which is emitted by electrical circuits carrying rapidly changing signals, as a by-product of the normal operation, and which causes unwanted signals (interference or noise) to be induced in other circuits.

RAM

See random access memory.

random access memory

RAM. A group of computer memory locations that is numerically identified to allow high-speed access by the controlling microprocessor. A memory location is randomly accessed by referring to its numerical identifier *(D)*. *Contrast with* read-only memory. *See* also dynamic random access memory; nonvolatile random access memory; static random access memory.

R_A_TOV

See resource allocation time-out value.

read-only memory

ROM. An information storage chip with permanent memory. Stored information cannot be changed or deleted except under special circumstances *(D)*. *Contrast with* random access memory.

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 hours/7 days per week) computer systems and networks.

remote notification

A process by which a system is able to inform remote users and workstations of certain classes of events that occur on the system. E-mail notification and the configuration of simple network management protocol (SNMP) trap recipients are two examples of remote notification programs that can be implemented on director-class switches.

remote user workstation

Workstation, such as a personal computer (PC), using HAFM application and Product Manager application software that can access the HAFM server over a local area network (LAN) connection.

repeater

A device that generates and often amplifies signals to extend transmission distance.

rerouting delay

An option that ensures that frames are delivered in order through the fabric to their destination.

resource allocation time-out value

R_A_TOV. 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.

RFI

See radio frequency interference.

ROM

See read-only memory. *Contrast with* random access memory.

router

An attaching device that connects two local area network (LAN) segments, which use similar or different architectures, at the reference model network layer *(D)*. *Contrast with* bridge.

RS-232

The Electronic Industry Association (EIA)-recommended specification for asynchronous serial interfaces between computers and communications equipment. It specifies both the number of pins and type of connection, but does not specify the electrical signals *(D)*.

S

S/390 mode

The mode that is most useful when attaching to IBM S/390 Enterprise Servers. *See also* open systems mode; operating mode.

SA/MVS™

See System Automation for Operating System/390.

SAN

See storage area network; system area network.

SA OS/390™

See System Automation for Operating System/390.

scalable

Refers to how well a system can adapt to increased demands. For example, a scalable network system could start with just a few nodes but easily expands to thousands of nodes. Scalability is important because it allows the user to invest in a system with confidence that a business will not outgrow it. Refers to anything whose size can be changed.

SCSI

See small computer system interface.

segment

A fabric segments when one or more switches cannot join the fabric because of various reasons. The switch or switches remain as separate fabrics.

segmented E_Port

See segmented expansion port.

segmented expansion port

Segmented E_Port. E_Port that has ceased to function as an E_Port within a multiswitch fabric due to an incompatibility between the fabrics that it joins. *See also* bridge port; fabric port; generic port; node port.

serial port

A full-duplex channel that sends and receives data at the same time. It consists of three wires: two that move data one bit at a time in opposite directions, and a third wire that is a common signal ground wire.

server

A computer that provides shared resources, such as files and printers, to the network. Used primarily to store data, providing access to shared resources. Usually contains a network operating system.

SFP transceivers
See small form factor pluggable transceivers.

shortwave
Lasers or light-emitting diodes (LEDs) that emit light with wavelengths around 780 nm or 850 nm. When using multimode fiber (50 nm) shortwave lasers can be used with Fibre Channel links less than 500 m. To achieve longer lengths, single-mode fiber is required. The preferred fiber core size is 50 micron as this fiber has large bandwidth so that the distance is limited by the fiber attenuation. A 62.5 micron core size is also supported for compatibility with existing FDDI installations. Fiber of this type has smaller bandwidth and, in this case, the distance is limited by the fiber bandwidth.

simple mail transfer protocol
SMTP. A transmission control protocol/Internet protocol (TCP/IP) protocol that allows the user to create, send, and receive text messages. SMTP protocols specify how messages are passed across a link from one system to another. They do not specify how the mail application accepts, presents, or stores the mail.

simple network management protocol
SNMP. A transmission control protocol/Internet protocol (TCP/IP)-derived protocol governing network management and monitoring of network devices.

simple network management protocol community
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.

simple network management protocol community name
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.

simple network management protocol management station
SNMP management station. An SNMP workstation personal computer (PC) used to oversee the SNMP network.

simple network management protocol version 1
SNMP v1. The original standard for SNMP is now referred to as SNMP v1.

simple network management protocol version 2
SNMP v2. The second version of the SNMP standard. This version expands the functionality of SNMP and broadens its ability to include OSI-based, as well as TCP/IP-based, networks as specified in RFC 1441 through 1452.

singlemode optical fiber
An optical fiber that allows one wavelength-dependent mode (light path) to propagate. *Contrast with* multimode optical fiber.

small computer system interface
SCSI. An interface standard that enables computers to communicate with peripherals connected to them. Commonly used in enterprise computing and in Apple Macintosh systems. Usually pronounced as “scuzzy.” The equivalent interface in most personal computers is enhanced integrated drive electronics (EIDE).

A narrow SCSI adapter supports up to eight devices, including itself. SCSI address 7 has the highest priority followed by 6, 5, 4, 3, 2, 1, 0, with 0 being the lowest priority.

small form factor pluggable transceivers
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.

SMTP
See simple mail transfer protocol.

SNMP
See simple network management protocol.

SNMP community
See simple network management protocol community.

SNMP community name
See simple network management protocol community name.

SNMP management station
See simple network management protocol management station.

SNMP v1
See simple network management protocol version 1.

SNMP v2
See simple network management protocol version 2.

SRAM
See static random access memory.

SSP
See system services processor.

state
The state of the switch or director. Possible values include online, offline, testing, and faulty. See offline state; online state.

static random access memory
SRAM. SRAM is microprocessor-cache random access memory. It is built internal to the microprocessor or on external chips. SRAM is fast, but relatively expensive *(D). Contrast with* dynamic random access memory.

storage area network
SAN. A high-performance data communications environment that interconnects computing and storage resources so that the resources can be effectively shared and consolidated.

stored addresses
In S/390 mode, a method for configuring addresses.

subnet
A portion of a network that shares a common address component. On transmission control protocol/Internet protocol (TCP/IP) networks, subnets are defined as all devices whose IP addresses have the same prefix. Dividing a network into subnets is useful for both security and performance reasons. IP networks are divided using a subnet mask.

subnet mask
A mask used by a computer to determine whether another computer with which it needs to communicate is located on a local or remote network. The network mask depends upon the class of networks to which the computer is connecting. The mask indicates which digits to look at in a longer network address and allows the router to avoid handling the entire address. Subnet masking allows routers to move the packets more quickly. Typically, a subnet may represent all the machines at one geographic location, in one building, or on the same local area network.

switch
A device that connects, filters and forwards packets between local area network (LAN) segments or storage area network (SAN) nodes or devices.

switchover
Changing a backup field-replaceable unit (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. Lower values indicate higher likelihood of becoming the principal switch. A value of 1 indicates the highest priority; 225 is the lowest priority. A value of 225 indicates that the switch is not capable of acting as the principal switch. The value 0 is illegal.

System Automation for Operating System/390

SA OS/390™. IBM licensed software that provides System/390 Parallel Sysplex™ management, automation capabilities, and integrated systems and network management. SA OS/390 manages host, remote processor, and I/O operations. SA OS/390 integrates the functions of Automated Operations Control for Multiple Virtual Storage (MVS™), ESCON™ Manager, and Target System Control Facility *(D)*.

system name

See product name.

system services processor

SSP. In a Director or Edge Switch, the central controlling processor. Controls the RS-232 maintenance port and the Ethernet port of a Fibre Channel Director or Edge Switch.

T

TB

See terabyte.

TCP

See transmission control protocol.

TCP/IP

See transmission control protocol/Internet protocol.

technical support

Single point of contact for a customer when assistance is needed in managing or troubleshooting a product. Technical support provides assistance twenty-four hours a day, seven days a week, including holidays. The technical support number is **(800) 652 6672**. *Synonymous with* customer support.

Telecommunications Industry Association

TIA. A member organization of the Electronic Industries Association (EIA), TIA is the trade group representing the communications and information technology industries. *See also* Electronic Industries Association.

telnet

The Internet standard protocol for remote terminal connection over a network connection.

terabyte

TB. One thousand (1,000) gigabytes; one terabyte of text on paper would consume 42,500 trees. At 12 characters per inch, 1 TB of data in a straight line would encircle the earth 56 times and stretch some 1.4 million miles equalling nearly three round trips from the earth to the moon.

Threshold Alert Log

Director or switch *Threshold Alert Log*. Log displayed through the Product Manager application that provides details of threshold alert notifications for an individual Director or Edge Switch. The log displays the date and time an alert occurred, and displays details about the alert as configured for the product. The information is useful to maintenance personnel for fault isolation and repair verification. *See also* Audit Log; Event Log; Hardware Log; Link Incident Log.

TIA

See Telecommunications Industry Association.

topology

Logical and/or physical arrangement of stations on a network.

transceiver modules

Transceiver modules come in longwave, extra longwave, or shortwave laser versions, providing a single fiber connection.

transfer rate

The speed with which data can be transmitted from one device to another. Data rates are often measures in megabits (Mbps) or megabytes (MBps) per second, or gigabits (Gbps) or gigabytes per second (GBps).

transmission control protocol

TCP. The transport layer for the transmission control protocol/Internet protocol (TCP/IP) protocol widely used on Ethernet networks and any network that conforms to U.S. Department of Defense standards for network protocol. TCP provides reliable communication and control through full-duplex connections *(D)*.

transmission control protocol/Internet protocol

TCP/IP. A layered set of protocols (network and transport) that allows sharing of applications among devices on a high-speed local area network (LAN) communication environment *(D)*. *See also* transmission control protocol; Internet protocol.

trap

Unsolicited notification of an event originating from a simple network management protocol (SNMP) managed device and directed to an SNMP network management station.

trap host
Simple network management protocol (SNMP) management workstation that is configured to receive traps.

trap recipient
In simple network management protocol (SNMP), a network management station that receives messages through SNMP for specific events that occur on the arbitrated loop device.

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 *(D)*. *Contrast with* jumper cable. *See also* optical cable.

U

UDP
See user datagram protocol.

UL
See Underwriters Laboratories.

ULP
See upper level protocol.

unblocked connection
In a Director or Edge Switch, the absence of the blocked attribute for a specific port. *Contrast with* blocked connection. *See* connectivity attribute. *See also* allowed connection; dynamic connection; dynamic connectivity.

unblocked port
Devices communicating with an unblocked port can login to the Director or Edge Switch and communicate with devices attached to any other unblocked port (assuming that this is supported by the current zoning configuration).

Underwriters Laboratories
UL. A laboratory organization accredited by the Occupational Safety and Health Administration and authorized to certify products for use in the home and workplace *(D)*.

unicast
Communication between a single sender and a single receiver over a network.

uninterruptable power supply
UPS. A buffer between public utility power or another power source, and a system that requires precise, uninterrupted power *(D)*.

UNIX

A popular multi-user, multitasking operating system originally designed to be a small, flexible system used exclusively by programmers. UNIX was one of the first operating systems to be written in a high-level programming language, namely C. This meant that it could be installed on virtually any computer for which a C compiler existed. Due to its portability, flexibility, and power, UNIX has become the leading operating system for workstations. Historically, it has been less popular in the personal computer market, but the emergence of a new version called Linux is revitalizing UNIX across all platforms.

upper level protocol

ULP. Protocols that map to and run on top of the Fibre Channel FC-4 layer. ULPs include Internet protocol (IP) and small computer system interface (SCSI).

UPS

See uninterruptable power supply.

user datagram protocol

UDP. A connectionless protocol that runs on top of Internet protocol (IP) networks. User datagram protocol/Internet protocol (UDP/IP) offers very few error recovery services, instead providing a direct way to send and receive datagrams over an IP network. UDP/IP is primarily used for broadcasting messages over an entire network. *Contrast with* transmission control protocol/Internet protocol.

V

VAC

See volts alternating current.

VDC

See volts direct current.

virtual machine

VM®. (1) A virtual data processing system that appears to be at the exclusive disposal of a single user, but whose functions are accomplished by sharing the resources of a real data processing system. (2) A functional simulation of a computer system and its associated devices, multiples of which can be controlled concurrently by one operating system *(D, T)*.

virtual storage
VS. (1) Storage space that may be regarded as addressable main storage by the user of a computer system in which virtual addresses are mapped to real addresses. The size of virtual storage is limited by the addressing scheme of the computer system and by the amount of auxiliary storage available, not by the number of main storage locations. (2) Addressable space that is apparent to the user as processor storage space, from which the instructions and the data are mapped to the processor storage locations *(A, D, I)*.

volt
A measure of the difference in electrical potential between two points in a conductor, equal to one ohm resistance carrying a constant current of one ampere, with a power dissipation of one watt *(D)*. *See* volts alternating current; volts direct current.

volts alternating current
VAC. A term for classifying the system in which volts exist. VAC means that the volts exist in a circuit where the electricity can travel in either direction. *Contrast with* volts direct current. *See* volt.

volts direct current
VDC. A term for classifying the system in which volts exist. VDC means that the electricity has a specific path it must follow. *Contrast with* volts alternating current. *See* volt.

W

warning message
A message that indicates a possible error has been detected. *See also* error message.

watt
A unit of power in the International System equal to one joule (Newton-meter) per second *(D)*.

window
The main window for the HAFM application or Product Manager applications. Each application has a unique window that is divided into separate panels for the title, navigation control, alerts, and the main or *Product View*. The user performs all management and monitoring functions for these Fibre Channel products through the application window.

workstation
A terminal or microcomputer usually connected to a network or mainframe at which a user can perform applications.

world-wide names
WWN. Eight-byte string that uniquely identifies a Fibre Channel entity (that is, a port, a node, a switch, a fabric), even on global networks.

wrap plug

Synonym for loopback plug.

wrap test

A test that checks attachment or control unit circuitry, without checking the mechanism itself, by returning the output of the mechanism as input. A wrap test can transmit a specific character pattern through a system and compare the pattern received with the pattern transmitted *(D)*.

write authorization

Permission for an simple network management protocol (SNMP) management station with the proper community name to modify writable management information base (MIB) variables.

WWN

See world-wide names.

Z

zip drive

A high capacity floppy disk and disk drive developed by the Iomega Corporation. Zip disks are slightly larger than conventional floppy disks. The storage capacity for zip disks is between 100 and 250 MB of data. The zip drive and disk is used for backing up the HAFM server, and is located on the communications tray behind the HAFM server.

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. *See also* active zone set; zone set; zoning.

zone member

Specification of a device to be included in a zone. A zone member can be identified by the port number of the Director or Edge Switch to which it is attached or by its port world-wide name (WWN). In multiswitch fabrics, identification of end-devices or nodes by WWN is preferable.

zone set

A collection of zones that may be activated as a unit. *See also* active zone set; zone.

zoning

Grouping of several devices by function or by location. All devices connected to a connectivity product, such as the Director or Edge Switch, may be configured into one or more zones. *See also* access control; zone.

Index

Figures

Tables