

hp StorageWorks

director 2/140 service manual

Part Number: AA-RTDTA-TE

First Edition (January 2003)

This guide provides procedures for servicing the HP StorageWorks Director 2/140.



i n v e n t

© Hewlett-Packard Company, 2003. All rights reserved.

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.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard. The information contained in this document is subject to change without notice.

Microsoft, MS-DOS, Windows, and Windows 2000 are trademarks of Microsoft Corporation in the U.S. and/or other countries.

All other product names mentioned herein may be trademarks of their respective companies.

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.

director 2/140 service manual
First Edition (January 2003)
Part Number: AA-RTDTA-TE

Contents

About This Guide

Intended Audience	xi
Related Documentation	xi
Document Conventions	xii
Symbols in Text	xii
Symbols on Equipment	xiii
Rack Stability	xiv
Getting Help	xiv
HP Technical Support	xiv
HP Website	xv
HP Authorized Reseller	xv

1 General Information

Director Description	1-1
Director Management	1-2
Error-Detection, Reporting, and Serviceability Features	1-3
Zoning Feature	1-4
Multiswitch Fabrics	1-5
Director Specifications	1-7
HAFM Server Description	1-9
HAFM Server Specifications	1-10
Ethernet Hub	1-10
Embedded Web Server Interface	1-11
Maintenance Approach	1-11
Remote Workstation Configurations	1-12
Minimum Remote Console Hardware Specifications	1-15
Field-Replaceable Units	1-16
Power Module Assembly	1-17
CTP Card	1-18
UPM Card	1-18

Power Supply	1–20
AC Module	1–20
Fan Module	1–21
SBAR Assembly	1–21
Backplane	1–21
Software Diagnostic Features	1–21
HAFM and Product Manager Diagnostics	1–22
HAFM Services Application	1–23
Embedded Web Server Diagnostics	1–25
SNMP Trap Message Support	1–27
E-Mail and Call-Home Support	1–27
Tools and Test Equipment	1–28
Tools Supplied with the Director	1–28
Tools Supplied by Service Personnel	1–30

2 Diagnostics

Maintenance Analysis Procedures	2–1
MAP 0000: Start MAP	2–12
MAP 0100: Power Distribution Analysis	2–36
MAP 0200: POST Failure Analysis	2–46
MAP 0300: Console Application Problem Determination	2–51
MAP 0400: Loss of Console Communication	2–58
MAP 0500: FRU Failure Analysis	2–71
MAP 0600: UPM Card Failure and Link Incident Analysis	2–79
MAP 0700: Fabric, ISL, and Segmented Port Problem Determination	2–99
MAP 0800: Console PC Problem Determination	2–112

3 Repair Information

Procedural Notes	3–2
Using Log Information	3–3
HAFM Audit Log	3–3
HAFM Event Log	3–3
Session Log	3–4
Product Status Log	3–5
Fabric Log	3–5
Director 2/140 Audit Log	3–6
Director 2/140 Event Log	3–6
Hardware Log	3–8

Link Incident Log	3-10
Threshold Alert Log	3-11
Using Views	3-13
Port List View	3-13
FRU List View	3-15
Node List View	3-17
Performance View	3-18
Topology View	3-18
Zone Set View	3-20
Performing Port Diagnostics	3-21
UPM card LEDs	3-22
Port Card View	3-22
Performance View	3-30
Perform Loopback Tests	3-32
Swapping Ports (S/390 only)	3-38
Collecting Maintenance Data	3-40
Clean Fiber-Optic Components	3-42
Power-On Procedure	3-43
Power-Off Procedure	3-43
IPL the Director	3-44
Set the Director Online or Offline	3-46
Set Online State	3-46
Set Offline State	3-47
Block and Unblock Ports	3-47
Block a Port	3-48
Block a UPM Card	3-49
Unblock a Port	3-49
Unblock a UPM Card	3-50
Manage Firmware Versions	3-51
Determine a Director Firmware Version	3-51
Add a Firmware Version	3-52
Modify a Firmware Version Description	3-55
Delete a Firmware Version	3-56
Download a Firmware Version to a Director	3-56
Manage Configuration Data	3-58
Backup the Configuration	3-59
Restore the Configuration	3-60
Reset Configuration Data	3-61

Install or Upgrade Software 3–62

4 FRU Removal and Replacement

Procedural Notes 4–1

Removing and Replacing FRUs 4–2

 ESD Information 4–2

 Concurrent FRUs 4–4

 Nonconcurrent FRUs 4–5

 RRP: Redundant CTP Card 4–5

 RRP: UPM Card 4–9

 RRP: SFP Optical Transceiver 4–14

 RRP: UPM Filler Blank 4–17

 RRP: Redundant Power Supply 4–19

 RRP: AC Module 4–21

 RRP: Redundant SBAR Assembly 4–24

 RRP: Redundant Fan Module 4–27

 RRP: Power Module Assembly 4–30

 RRP: Backplane 4–32

5 Illustrated Parts Breakdown

Front-Accessible FRUs 5–1

Rear-Accessible FRUs 5–3

Miscellaneous Parts 5–5

 Power Plugs and Receptacles 5–5

A Messages

HAFM Application Messages A–1

Director 2/140 Product Manager Messages A–24

B Event Code Tables

System Events (000 through 199) B–3

Power Supply Events (200 through 299) B–18

Fan Module Events (300 through 399) B–22

CTP Card Events (400 through 499) B–29

UPM Card Events (500 through 599) B–44

SBAR Assembly Events (600 through 699) B–56

Thermal Events (800 through 899) B–61

Glossary

Index

Figures

1-1	HAFM server	1-9
1-2	12-Port Ethernet hub	1-10
1-3	Typical network configuration (one Ethernet connection)	1-13
1-4	Typical network configuration (two Ethernet connections)	1-14
1-5	Director FRUs (front access)	1-16
1-6	Director FRUs (rear access)	1-17
1-7	UPM card LEDs and connectors.	1-19
1-8	HAFM Services window.	1-24
1-9	Torque tool and hex adapter	1-28
1-10	SFP fiber-optic loopback plug	1-29
1-11	Fiber-optic protective plug	1-29
1-12	Null modem cable	1-29
2-1	Products View	2-14
2-2	Port Properties dialog box.	2-20
2-3	Link Incident Log	2-21
2-4	Event Log	2-23
2-5	View panel	2-28
2-6	View Port Properties panel	2-31
2-7	View FRU Properties panel	2-33
2-8	Monitor Log panel	2-35
2-9	Task Manager dialog box, Applications tab	2-53
2-10	HAFM Login dialog box.	2-55
2-11	Modify Network Address dialog box	2-69
2-12	New Product dialog box	2-70
2-13	UPM card diagram (front).	2-84
2-14	UPM card diagram (rear)	2-84
2-15	Clear Link Incident Alert(s)	2-94
2-16	UPM card diagram (front).	2-100
2-17	UPM card diagram (rear)	2-100
2-18	Zone Set View.	2-109
3-1	HAFM Event Log	3-4
3-2	Product Status Log	3-5
3-3	Director 2/140 Event Log	3-7

3-4	Hardware Log	3-9
3-5	Link Incident Log	3-10
3-6	Threshold Alert Log	3-12
3-7	Port List View	3-14
3-8	FRU List View.....	3-16
3-9	Node List View	3-18
3-10	Topology View	3-19
3-11	Zone Set View.....	3-20
3-12	Port Card View	3-23
3-13	Port Properties dialog box	3-26
3-14	Performance View.....	3-30
3-15	Port Diagnostics dialog box.....	3-33
3-16	Channel Wrap On for Port n dialog box	3-38
3-17	Swap Ports dialog box	3-39
3-18	Save Data Collection dialog box.....	3-41
3-19	Data Collection dialog box	3-41
3-20	Clean Fiber-Optic components	3-42
3-21	Information dialog box	3-45
3-22	Set Online State dialog box (offline).....	3-46
3-23	Set Online State dialog box (online)	3-47
3-24	Blocking Port warning box	3-48
3-25	Block All Ports dialog box	3-49
3-26	Unblocking Port warning box	3-50
3-27	Unblock All Ports dialog box	3-51
3-28	Firmware Library dialog box.....	3-52
3-29	New Firmware Version dialog box	3-54
3-30	New Firmware Description dialog box	3-54
3-31	Modify Firmware Description dialog box	3-55
3-32	Send Firmware dialog box.....	3-57
3-33	Send Firmware Complete dialog box	3-58
3-34	Backup and Restore Configuration dialog box	3-59
3-35	Backup Complete dialog box	3-60
3-36	Backup and Restore Configuration dialog box	3-60
3-37	Warning dialog box	3-61
3-38	Restore Complete dialog box	3-61
3-39	Reset Configuration dialog box.....	3-62
3-40	Run dialog box.....	3-63
3-41	InstallAnywhere dialog box (Introduction).....	3-64

4-1	ESD grounding points	4-3
4-2	CTP card removal and replacement	4-7
4-3	UPM card removal and replacement	4-12
4-4	SFP optical transceiver removal and replacement	4-15
4-5	UPM filler blank removal and replacement	4-18
4-6	Redundant power supply removal and replacement	4-20
4-7	AC module removal and replacement	4-23
4-8	SBAR assembly removal and replacement	4-25
4-9	Fan module removal and replacement	4-28
4-10	Power module assembly removal and replacement	4-31
4-11	Backplane removal and replacement	4-34
5-1	Front-accessible FRUs	5-2
5-2	Rear-accessible FRUs (part 1)	5-3
5-3	Rear-accessible FRUs (part 2)	5-4
5-4	Power plugs and receptacles	5-6

Tables

1	Document Conventions	xii
1-1	HAFM Services Status Symbols	1-25
2-1	Factory-set Defaults	2-1
2-2	MAP Summary	2-2
2-3	Event Codes Versus Maintenance Action	2-2
2-4	MAP 100: Event Codes	2-37
2-5	MAP 200: Event Codes	2-48
2-6	Byte 0 FRU Codes	2-48
2-7	MAP 400: Event Codes	2-61
2-8	MAP 400: Error Messages and Actions	2-63
2-9	MAP 500: Event Codes	2-73
2-10	MAP 600: Event Codes	2-82
2-11	MAP 600: Port Operational and LED States	2-86
2-12	MAP 600: Invalid Attachment Reasons and Actions	2-89
2-13	MAP 600: Port Operational States and Actions	2-99
2-14	MAP 700: Event Codes	2-101
2-15	MAP 700: Segmentation Reasons and Actions	2-103
2-16	MAP 700: Byte 4, Segmentation Reasons	2-106
2-17	MAP 700: Segmentation Reasons and Actions	2-113
3-1	Factory-set Defaults	3-2
3-2	Port Operational States	3-24

3-3	Invalid Attachment Messages and Explanations	3-27
4-1	Factory-set Defaults	4-1
4-2	Concurrent FRU Names and ESD Requirements	4-4
4-3	Nonconcurrent FRU Names and ESD Precautions	4-5
5-1	Front-Accessible FRU Parts List	5-2
5-2	Rear-Accessible FRU Parts List (Part 1)	5-4
5-3	Rear-Accessible FRU Parts List (Part 2)	5-5
5-4	Miscellaneous Parts	5-5
5-5	Power Plugs and Receptacles	5-6
A-1	HAFM Messages	A-1
A-2	Product Manager Messages	A-24

About This Guide

This guide describes the service procedures for the HP StorageWorks Director 2/140.

Intended Audience

This publication is intended for service personnel, and any individuals who monitor, configure, and repair the Director 2/140.

Related Documentation

For a list of corresponding documentation included with this product, see the Related Documents section of the *hp StorageWorks director 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 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	<i>Italics</i>
User input, command names, system responses (output and messages)	Monospace font COMMAND NAMES are uppercase unless they are case sensitive
Variables	<i>Monospace, italic font</i>
Website addresses	Sans serif font (http://thenew.hp.com)

Symbols in Text

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



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



CAUTION: Text set off in this manner indicates that failure to follow directions could result in damage to equipment or data.

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

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

Symbols on Equipment



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

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



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

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



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

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



Power supplies or systems marked with these symbols indicate the presence of multiple sources of power.

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



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

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

Rack Stability



WARNING: To reduce the risk of personal injury or damage to the equipment, be sure that:

- The leveling jacks are extended to the floor.
 - The full weight of the rack rests on the leveling jacks.
 - In single rack installations, the stabilizing feet are attached to the rack.
 - In multiple rack installations, the racks are coupled.
 - Only one rack component is extended at any time. A rack may become unstable if more than one rack component is extended for any reason.
-

Getting Help

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

HP Technical Support

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

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

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

Be sure to have the following information available before calling:

- Technical support registration number (if applicable)

- Product serial numbers
- Product model names and numbers
- Applicable error messages
- Operating system type and revision level
- Detailed, specific questions

HP Website

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

HP Authorized Reseller

For the name of your nearest HP Authorized Reseller:

- In the United States, call 1-800-345-1518
- In Canada, call 1-800-263-5868
- Elsewhere, see the HP website for locations and telephone numbers:
<http://thenew.hp.com>.

General Information

The HP StorageWorks Director 2/140 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 multiswitch 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 director implements Fibre Channel technology that provides scalable bandwidth (2.125 gigabits per second), redundant switched data paths, and long transmission distances (up to 35 kilometers with extended reach optical transceivers, or 100 kilometers with repeaters).

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

- Director management, error detection and reporting features, serviceability features, zoning, multiswitch fabrics, and specifications.
- The HAFM server and minimum hardware specifications.
- Maintenance approach.
- Remote workstation configurations and hardware specifications.
- Field-replaceable units (FRUs).
- Software diagnostic features.
- Tools and test equipment.

Director Description

The director is a second-generation, 140-port product that provides dynamic switched connections between Fibre Channel servers and devices in a SAN environment. Directors (from one to three) can be configured to order in an HP-supplied equipment rack, which can provide up to 420 ports in a single cabinet.

Directors are managed and controlled through an HP-supplied HAFM server with the *HAFM* and *Director 2/140 Product Manager* applications installed. The HAFM server is a notebook personal computer (PC) that provides a central point of control for up to 48 directors and/or edge switches. Multiple directors and the HAFM server communicate through the customer's local area network (LAN).

The director 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 director can also connect to one or more additional directors or switches to form a Fibre Channel multiswitch fabric.

Director Management

The following management access methods are provided:

- Management through the *HAFM* application. This graphical user interface (GUI) resides on the HAFM server and provides a single point of management for all directors, and a launching point for the *Director 2/140 Product Manager* application.
- Management using simple network management protocol (SNMP). An SNMP agent is implemented through the *HAFM* application that allows administrators on SNMP management workstations to access director management information using any standard network management tool. Administrators can assign internet protocol (IP) addresses and corresponding community names for up to 12 SNMP workstations functioning as SNMP trap message recipients. Refer to the *hp StorageWorks SNMP reference guide for directors and edge switches* for more information.
- Management through the Internet using the Embedded Web Server interface installed on the director. This interface supports configuration, statistics monitoring, and basic operation of the director, but does not offer all the capabilities of the *Director 2/140 Product Manager* application. Administrators launch the web server interface from a remote PC by entering the director's IP address as the Internet uniform resource locator (URL), then entering a user name and password at a login screen. The PC browser then becomes a management console.
- Management through a customer-supplied remote workstation communicating with the HAFM server through a corporate intranet.

- Management through the command line interface (CLI). The CLI allows you to access many HAFM and *Product Manager* applications while entering commands during a telnet session with the director. The primary purpose of the CLI is to automate management of a large number of directors using scripts. The CLI is not an interactive interface; no checking is done for pre-existing conditions and no prompts display to guide users through tasks. Refer to the *hp StorageWorks CLI reference guide for directors and edge switches* for more information.

Error-Detection, Reporting, and Serviceability Features

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

- Light-emitting diodes (LEDs) on director FRUs and the front bezel that provide visual indicators of hardware status or malfunctions.
- System and threshold alerts, event logs, audit logs, link incident logs, threshold alert logs, and hardware logs that display director, Ethernet link, and Fibre Channel link status at the HAFM server or on a remote workstation.
- Diagnostic software that performs power-on self-tests (POSTs) and port diagnostics (internal loopback and external loopback).
- Automatic notification of significant system events (to support personnel or administrators) through e-mail messages or the call-home feature.
- An internal modem in the HAFM server for HP call-home support.

NOTE: For directors and switches installed in some legacy environments, call-home notification requires installation of HP Proactive Service software. This service is offered at no additional charge for subsystems covered under an on-site warranty or on-site storage hardware support contract. To register or order Proactive Service software, contact your HP authorized service provider.

- An RS-232 maintenance port at the rear of the director (port access is password protected) that enables installation or service personnel to change the director's internet protocol (IP) address, subnet mask, and gateway address; or to run diagnostics and isolate system problems through a local or remote terminal.
- Redundant FRUs (logic cards, power supplies, and cooling fans) that are removed or replaced without disrupting director or Fibre Channel link operation.
- A modular design that enables quick removal and replacement of FRUs without the use of special tools or equipment.
- Concurrent port maintenance. UPM cards are added or replaced and fiber-optic cables are attached to ports without interrupting other ports or director operation.

- Beaconing to assist service personnel in locating a specific port, FRU, or director in a multiswitch environment. When port beaconing is enabled, the amber LED associated with the port flashes. When FRU beaconing is enabled, the amber (service required) LED on the FRU flashes. When unit beaconing is enabled, the system error indicator on the front bezel flashes. Beaconing does not affect port, FRU, or director operation.
- Data collection through the *Product Manager* application to help isolate system problems. The data includes a memory dump file and audit, hardware, and engineering logs.
- Status monitoring of redundant FRUs and alternate Fibre Channel data paths to ensure continued director availability in case of failover. The *HAFM* application queries the status of each backup FRU daily. A backup FRU failure is indicated by an illuminated amber LED.
- Simple network management protocol (SNMP) using the Fibre Alliance management information base (MIB) that runs on the HAFM server. Up to 12 authorized management workstations can be configured through the *HAFM* application to receive unsolicited SNMP trap messages. The trap messages indicate operational state changes and failure conditions.
- SNMP using the Fibre Channel Fabric Element MIB (Version 2.2), transmission control protocol/internet protocol (TCP/IP) MIB-II definition (RFC 1213), or a product-specific MIB that runs on each director. Up to six authorized management workstations can be configured through the *Product Manager* application to receive unsolicited SNMP trap messages. The trap messages indicate operational state changes and failure conditions.

Zoning Feature

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

Zoning is configured by authorizing or restricting access to name server information associated with device N_Ports that attach to director fabric ports (F_Ports). A zone member is specified by the director port number to which a device is attached, or by the 8-byte (16-digit) world-wide name (WWN) assigned to the host bus adapter (HBA) or Fibre Channel interface installed in a device. A device can belong to multiple zones.



CAUTION: If zoning is implemented by port number, a change to the director fiber-optic cable configuration disrupts zone operation and may incorrectly include or exclude a device from a zone.

If zoning is implemented by WWN, removal and replacement of a device HBA or Fibre Channel interface (thereby changing the device WWN) disrupts zone operation and may incorrectly include or exclude a device from a zone.

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

Multiswitch Fabrics

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

Because a multiswitch fabric is typically complex, service personnel should be aware that several factors can degrade fabric performance or cause connectivity failures. These factors include:

- **Domain ID assignment**—Each director in a fabric is identified by a unique domain ID that ranges from 1 through 31. A domain ID of 0 is invalid. If two operational fabrics join, they determine if any domain ID conflicts exist between the fabrics. If one or more conflicts exist, the E_Ports that form the interswitch link (ISL) segment to prevent the fabrics from joining.
- **Zoning**—In a multiswitch fabric, zoning is configured on a fabric-wide basis, and a change to the zoning configuration is applied to all directors and switch elements in the fabric. To ensure zoning is consistent across a fabric, the following rules are enforced when two fabrics (zoned or unzoned) join:
 - **Fabric A unzoned and Fabric B unzoned**—The fabrics join successfully, and the resulting fabric remains unzoned.
 - **Fabric A zoned and Fabric B unzoned**—The fabrics join successfully, and fabric B automatically inherits the zoning configuration from fabric A.

- **Fabric A unzoned and Fabric B zoned**—The fabrics join successfully, and fabric A automatically inherits the zoning configuration from fabric B.
- **Fabric A zoned and Fabric B zoned**—The fabrics join successfully only if the zone configurations can be merged. If the fabrics cannot join, the connecting E_Ports segment and the fabrics remain independent.

Zone configurations for two fabrics are compatible (the zones can join) if the active zone set name is identical for each fabric, and if zones with the same name have identical elements.

- **Port segmentation**—When an ISL activates, directors exchange operating parameters to determine if they are compatible and can join to form a single fabric. If incompatible, the connecting E_Port at each director segments to prevent the creation of a single fabric. A segmented link transmits only Class F traffic; the link does not transmit Class 2 or Class 3 traffic. The following conditions cause ports to segment:
 - **Incompatible operating parameters**—Either the resource allocation time-out value (R_A_TOV) or error-detect time-out value (E_D_TOV) is inconsistent between directors. To prevent E_Port segmentation, the same E_D_TOV and R_A_TOV must be specified for each director.
 - **Duplicate domain IDs**—One or more domain ID conflicts are detected.
 - **Incompatible zoning configurations**—Zoning configurations for the directors are not compatible.
 - **Build fabric protocol error**—A protocol error is detected during the process of forming the fabric.
 - **No principal switch**—No director in the fabric is capable of becoming the principal switch.
 - **No response from attached switch**—After a fabric is created, each director in the fabric periodically verifies operation of all attached switches and directors. An ISL segments if a switch or director does not respond to a verification request.
 - **ELP retransmission failure timeout**—A director that exhibits a hardware failure or connectivity problem cannot transmit or receive Class F frames. The director did not receive a response to multiple exchange link protocol (ELP) frames, did not receive a fabric login (FLOGI) frame, and cannot join an operational fabric.

Director Specifications

This section lists physical characteristics, storage and shipping environment, operating environment, and service clearances for the Director 2/140.

Physical Characteristics

Dimensions:

Height: 52.7 centimeters (20.9 inches)

Width: 44.1 centimeters (17.5 inches)

Depth: 61.0 centimeters (24.2 inches)

Weight: 75.9 kilograms (167.0 pounds)

Shipping weight: 76.4 kilograms (168 pounds)

Power requirements:

Input voltage: 180 to 264 VAC

Input frequency: 47/63 Hz

Plan for single phase or phase-to-phase connections and 5-ampere dedicated service

Heat dissipation:

35 UPM cards (maximum): 842 watts (2,873 BTUs/hr)

Cooling airflow clearances (director chassis):

Right and left side: 2.5 centimeters (1.0 inches)

Front and rear: 7.6 centimeters (3.0 inches)

Top and bottom: No clearance required

Shock and vibration tolerance:

60 Gs for 10 milliseconds without nonrecoverable errors

Acoustical noise:

7.0 Bels "A" scale

Inclination:

10° maximum

Storage and Shipping Environment

Protective packaging must be provided to protect the director under all shipping methods (domestic and international).

Shipping temperature:

-40° C to 60° C (-40° F to 140° F)

Storage temperature:

1° C to 60° C (34° F to 140° F)

Shipping relative humidity:

5% to 100%

Storage relative humidity:

5% to 80%

Maximum wet-bulb temperature:

29° C (84° F)

Altitude:

12,192 meters (40,000 feet)

Operating Environment

Temperature:

4° C to 40° C (40° F to 104° F)

Relative humidity:

8% to 80%

Maximum wet-bulb temperature:

27° C (81° F)

Altitude:

3,048 meters (10,000 feet)

Equipment Cabinet Service Clearances

Front: 1 meter (39.37 inches)

Rear: 1 meter (39.37 inches)

Right side: No clearance required

Left side: No clearance required

HAFM Server Description

The HAFM server ([Figure 1-1](#)) is a notebook personal computer (PC) that provides a central point of control for up to 48 LAN-connected directors or edge switches.

The server is mounted in a slide-out drawer in the HP-supplied equipment rack. The HAFM server or Internet access to the Embedded Web Server interface is required to install, configure, and manage the director.

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



Figure 1-1: HAFM server

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

HAFM Server Specifications

The following list summarizes hardware specifications for the HAFM server notebook platform. Current platforms may ship with more enhanced hardware, such as a faster processor, additional random-access memory (RAM), or a higher-capacity hard drive or removable disk drive.

- HP laptop server PC with color monitor, keyboard, keyboard-mounted trackpad (mouse), and U. S. power cord.
- Intel® Pentium III™ processor with an 800 megahertz (MHz) or greater clock speed, running the Microsoft Windows 2000 operating system.
- Eighteen gigabyte (GB) or greater internal hard drive.
- 160 megabyte (MB) or greater RAM.
- Removable DVD/CD-ROM drive.
- Removable 100 MB disk (Zip®) drive.
- 56K internal modem.
- One internal 10/100 Mbps Ethernet adapter with RJ-45 connector (provides public LAN interface to directors and remote clients).

Ethernet Hub

The HAFM server and managed directors connect through a rack-mounted 10/100 Base-T Ethernet hub. [Figure 1-2](#) illustrates the optional 12-port hub.

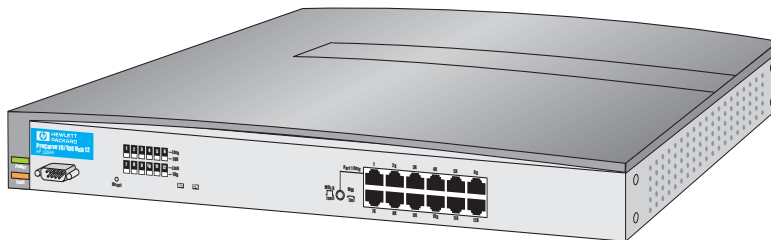


Figure 1-2: 12-Port Ethernet hub

Embedded Web Server Interface

Administrators or operators with a browser-capable PC and an Internet connection can monitor and manage the director through an Embedded Web Server interface. The application provides a graphical user interface (GUI) similar to the *Product Manager* application, and supports director configuration, statistics monitoring, and basic operation.

Maintenance Approach

Whenever possible, the director maintenance approach instructs service personnel to perform fault isolation and repair procedures without degrading or interrupting operation of the director, attached devices, or associated applications. Director 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 director front bezel 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 a:

- Director or HAFM server failure (hardware or software).
- Ethernet LAN communication failure between the director 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 2](#). 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 director failure to a single FRU, remove and replace the failed FRU, and verify director operation. The fault isolation process normally begins with [MAP 0000: Start MAP on page 2–12](#).

Ensure the correct director is selected for service (if the HAFM server manages multiple directors or other HP products) by enabling unit beaconing at the failed director. The amber system error LED on the director front bezel blinks when beaconing is enabled. Instructions to enable beaconing are incorporated into MAP steps.

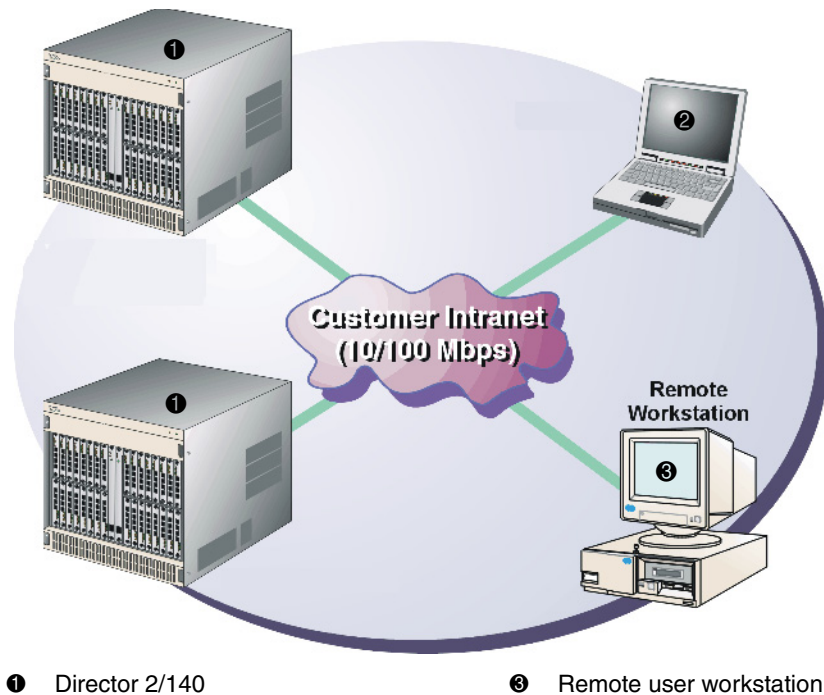
Remote Workstation Configurations

Using a standard Web browser, the HAFM and *Product Manager* applications can be downloaded and installed on remote user workstations that are LAN-attached to the HAFM server. Operators at these workstations can manage and monitor directors controlled by the HAFM server. A maximum of nine concurrent users (including a local user) can log in to the *HAFM* application.

Each remote workstation must have access to the LAN segment on which the HAFM server is installed. Director administrative functions are accessed through the LAN and HAFM server. The LAN interface can be:

- Part of the customer's public 10/100 Mbps LAN segment that provides access to managed directors. This director-to-HAFM server Ethernet connection is part of the equipment rack installation and is required. Connection of remote workstations through the hub is optional. This type of network configuration using one Ethernet connection through the HAFM server is shown in [Figure 1-3](#).

This single Ethernet connection is supported by HP, is Open View-Storage Node Manager (OV-SNM) compatible, and is the recommended configuration for a typical HP installation at a customer site. LAN security is provided by restricting password access and disabling the SNMP agent, embedded Web server interface, and command line interface (telnet access) for each managed director.

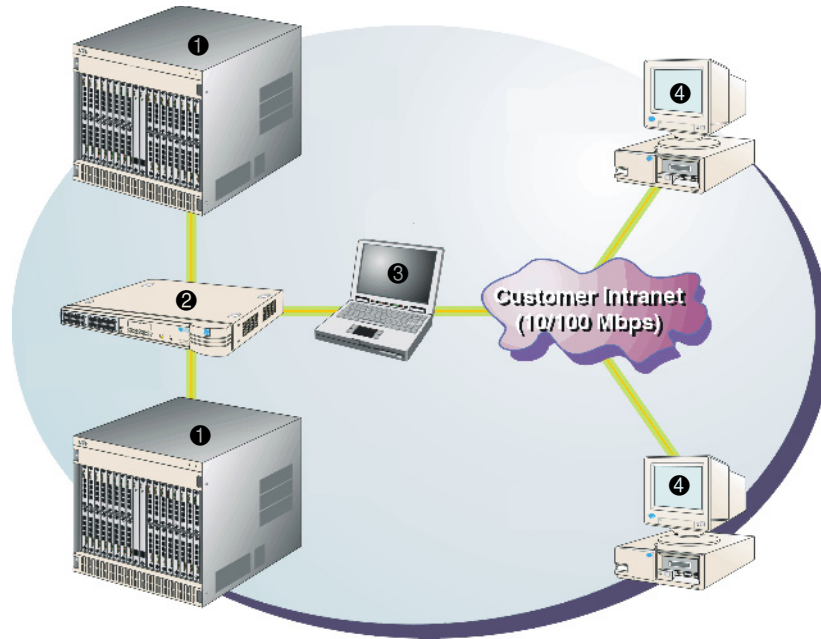


- ❶ Director 2/140
- ❷ HAFM server

- ❸ Remote user workstation

Figure 1–3: Typical network configuration (one Ethernet connection)

- Part of a second HAFM server interface that connects to the customer’s private intranet and allows operation of the *Product Manager* application from remote user PCs or workstations. Connection to this LAN segment is optional and depends on customer requirements. This type of network configuration using both Ethernet connections is shown in [Figure 1–4](#).



- | | |
|-------------------|--------------------------------|
| ❶ Director 2/140 | ❸ HAFM server |
| ❷ HP Ethernet hub | ❹ Two remote user workstations |

Figure 1–4: Typical network configuration (two Ethernet connections)

- Although this dual Ethernet connection is supported by HP, it is not OV-SNM compatible, and requires installation of an additional PCMCIA LAN adapter card (not supplied by HP). HP does not recommend using this configuration for a typical new HP installation at a customer site.

Refer to the *hp StorageWorks SAN high availability planning guide* for additional information about network configurations.



CAUTION: Prior to servicing a director or HAFM server, determine the Ethernet LAN configuration. Installation of directors and the HAFM server on a public customer intranet can complicate problem determination and fault isolation.

Minimum Remote Console Hardware Specifications

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

- Desktop or notebook PC with color monitor, keyboard, and mouse, using an Intel Pentium processor with a 400 MHz or greater clock speed, and using the Microsoft Windows 95, Windows 98, Windows 2000, Windows XP, or Linux 2.2 operating system.
- Unix workstation with color monitor, keyboard, and mouse, using a:
 - Hewlett-Packard HA PA-RISC processor with a 400 MHz or greater clock speed, using the HP-UX 11 or higher operating system.
 - Sun Microsystems UltraSPARC-II processor with a 400 MHz or greater clock speed, using the SunOS Version 5.5.1 or higher operating system, or Solaris Version 2.5.1 or higher operating system.
 - IBM PowerPC microprocessor with a 400 MHz or greater clock speed, or POWER3 microprocessor with a 400 MHz or greater clock speed, using the AIX Version 4.3.3 or higher operating system.
- At least 15 MB available on the internal hard drive.
- 128 MB or greater RAM.
- Video card supporting 256 colors at 800 x 600 pixel resolution.
- Ethernet network adapter.
- Java-enabled Internet browser, such as Microsoft Internet Explorer (Version 4.0 or later) or Netscape Navigator (Version 4.6 or later).

Field-Replaceable Units

The director provides a modular design that enables quick removal and replacement of FRUs. This section describes director FRUs and controls, connectors, and indicators associated with the FRUs.

Figure 1-5 illustrates the front of the director.

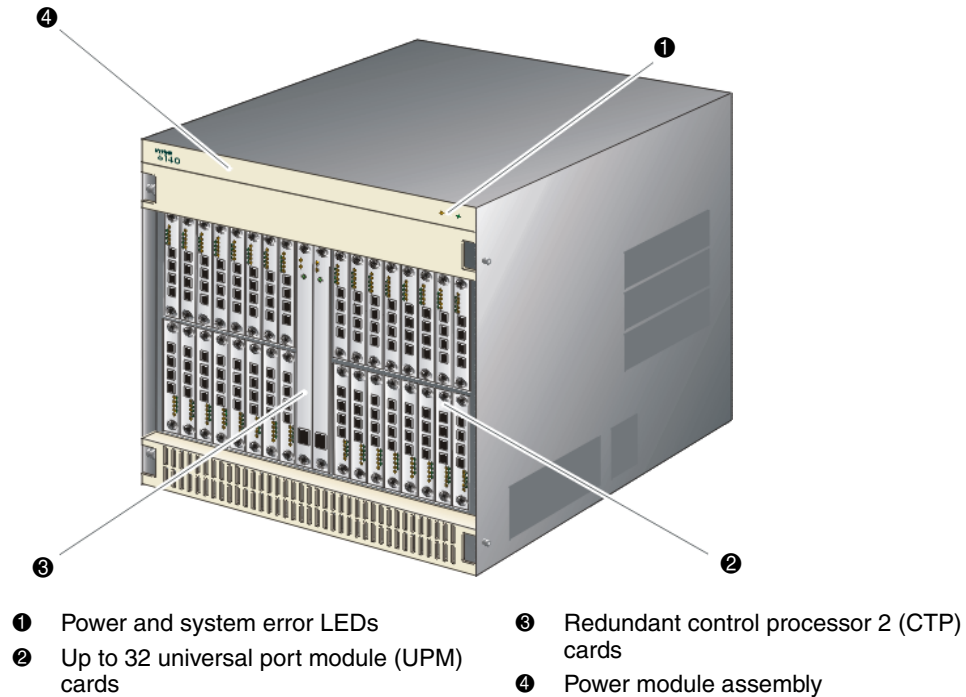


Figure 1-5: Director FRUs (front access)

Figure 1–6 illustrates the rear of the director.

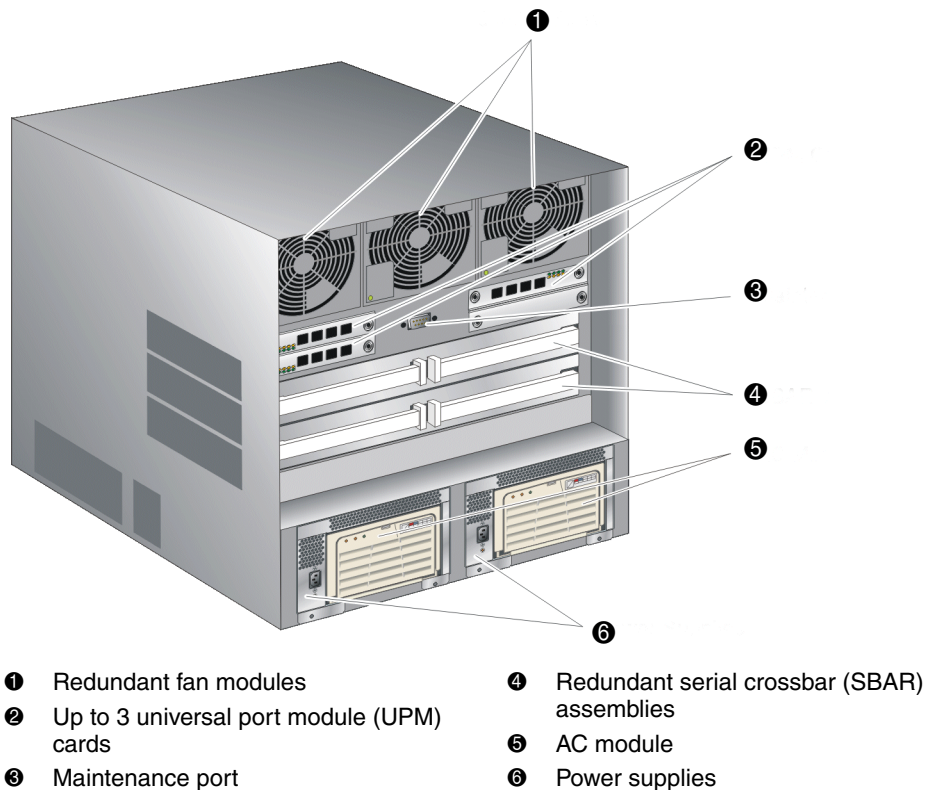


Figure 1–6: Director FRUs (rear access)

Power Module Assembly

The bezel at the top front of the director includes an amber system error light-emitting diode (LED) and a green power LED. These LEDs are actuated and controlled by a power module assembly which is accessed from the rear of the director.

The power LED illuminates when the director is powered on and operational. If the LED extinguishes, a facility power source, alternating current (AC) power cord, or director power distribution failure is indicated.

The system error LED illuminates when the director detects an event requiring immediate operator attention, such as a FRU failure. The LED remains illuminated as long as an event is active. The LED extinguishes when the **Clear System Error Light**

function is selected from the *Product Manager* application. The LED blinks if unit beaconing is enabled. An illuminated system error LED (indicating a failure) takes precedence over unit beaconing.

CTP Card

The director is delivered with two CTP cards. The active CTP card initializes and configures the director after power on and contains the microprocessor and associated logic that coordinate director operation. A CTP card provides an initial machine load (IML) button on the faceplate. When the button is pressed and held for three seconds, the director reloads firmware and resets the CTP card without switching off power or affecting operational fiber-optic links.

Each CTP card also provides a 10/100 megabit per second (Mbps) RJ-45 twisted pair connector on the faceplate that attaches to an Ethernet local area network (LAN) to communicate with the HAFM server or a simple network management protocol (SNMP) management station.

Each CTP card provides system services processor (SSP) and embedded port (EP) subsystems. The SSP subsystem runs director applications and the underlying operating system, communicates with director ports, and controls the RS-232 maintenance port and 10/100 Mbps Ethernet port. The EP subsystem provides Class F and exception frame processing, and manages frame transmission to and from the SBAR assembly. In addition, a CTP card provides nonvolatile memory for storing firmware, director configuration information, persistent operating parameters, and memory dump files. Director firmware is upgraded concurrently (without disrupting operation).

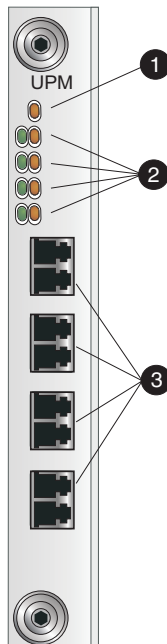
The backup CTP card takes over operation if the active card fails. Failover from a faulty card to the backup card is transparent to attached devices.

Each card faceplate contains a green LED that illuminates if the card is operational and active, and an amber LED that illuminates if the card fails. Both LEDs are extinguished on an operational backup card. The amber LED blinks if FRU beaconing is enabled.

UPM Card

Each UPM card provides four full-duplex generic ports (G_Ports) that transmit or receive data at 2.125 gigabits per second (Gb/s). G_Port functionality depends on the type of cable attachment. UPM cards use nonopen fiber control (OFC) Class 1 laser transceivers that comply with Section 21 of the Code of Federal Regulations (CFR), Subpart (J) as of the date of manufacture.

Figure 1–7 illustrates the faceplate of a UPM card.



SHR-2274

- ❶ An amber LED (at the top of the card) that illuminates if any port fails or blinks if FRU beaconing is enabled.
- ❷ A bank of amber and green LEDs above the ports. One amber LED and one green LED are associated with each port and indicate port status as follows:
 - The green LED illuminates (or blinks if there is active traffic) and the amber LED extinguishes to indicate normal port operation.
 - The amber LED illuminates and the green LED extinguishes to indicate a port failure.
 - Both LEDs extinguish to indicate a port is operational but not communicating with an N_Port (no cable attached, loss of light, port blocked, or link recovery in process).
 - The amber LED flashes and the green LED either remains on, extinguishes, or flashes to indicate a port is beaconing or running online diagnostics.
- ❸ Four duplex LC connectors for attaching fiber-optic cables.

Figure 1–7: UPM card LEDs and connectors

The director is delivered with 35 UPM cards installed (143 ports). A UPM card is a concurrent FRU and can be added or replaced while the director is powered on and operating.

Depending on device connections, G_Ports behave as follows:

- If the G_Port is attached to a Fibre Channel device, the port functions as a fabric port (F_Port). An F_Port is the interface on a director that connects to a device N_Port.
- If the G_Port is attached to another director or edge switch to form an interswitch link (ISL), the port functions as an expansion port (E_Port). A multiswitch fabric is formed through multiple directors, edge switches, and ISLs.

Singlemode or multimode fiber-optic cables attach to UPM cards through small form factor pluggable (SFP) optic transceivers. The fiber-optic transceivers provide duplex LC connectors, and can be detached from UPM cards (through a 10-pin interface) for easy replacement. Three fiber-optic transceiver types are available:

- **Shortwave Laser**—Shortwave laser transceivers provide connections for transferring data over short distances (2 to 500 meters) through 50-micron or 62.5-micron multimode fiber.
- **Longwave Laser**—Longwave laser transceivers provide connections for transferring data over long distances (up to 10 kilometers) through 9-micron singlemode fiber.
- **Extended-Reach Longwave Laser**—Longwave laser transceivers provide connections for transferring data over extended distances (up to 35 kilometers) through 9-micron singlemode fiber.

Power Supply

Redundant, load-sharing power supplies step down and rectify facility input power to provide 48-volt direct current (VDC) power to director FRUs. The power supplies also provide overvoltage and overcurrent protection. Either power supply can be replaced while the director is powered on and operational.

Each power supply has a separate backplane connection to allow for different AC power sources. The power supplies are input rated at 180 to 264 volts alternating current (VAC). The faceplate of each power supply provides the following status LEDs:

- A green **PWR OK** LED illuminates if the power supply is operational and receiving AC power.
- An amber **FAULT** LED illuminates if the power supply fails.
- An amber **TEMP** LED illuminates if the power supply shuts down due to an overtemperature condition.
- An amber **ILIM** LED illuminates if the power supply is overloaded and operating at the current limit (15.6 amperes).

AC Module

The AC module is located at the bottom rear of the director. Either AC module can be replaced while the director is powered on and operational. The module provides:

- Two single-phase AC power connectors. Each connector is input rated at 220 VAC.
- An input filter and AC system harness (internal to the FRU) that provides the wiring to connect the AC power connectors to the power switch and power supplies (through the backplane).

Fan Module

Three fan modules, each containing one system fan (three system fans total), provide cooling for director FRUs, as well as redundancy for continued operation if a fan fails.

A fan module can be replaced while the director is powered on and operating, provided the module is replaced within ten minutes (after which software powers off the director). An amber LED for each fan module illuminates if one or more fans fail or rotate at insufficient angular velocity.

SBAR Assembly

The director is delivered with two SBAR assemblies. The active SBAR is responsible for Fibre Channel frame transmission from any director port to any other director port. Connections are established without software intervention. The assembly accepts a connection request from a port, determines if a connection can be established, and establishes the connection if the destination port is available. The assembly also stores busy, source connection, and error status for each director port.

The backup SBAR takes over operation if the active assembly fails, and provides the ability to maintain connectivity and data frame transmission without interruption. Failover to the backup assembly is transparent to attached devices.

Each SBAR assembly consists of a card and steel carriage that mounts flush on the backplane. The carriage provides protection for the back of the card, distributes cooling airflow, and assists in aligning the assembly during installation. The rear of the carriage contains a green LED that illuminates if the assembly is operational and active, and an amber LED that illuminates if the assembly fails. Both LEDs are extinguished on an operational backup assembly. The amber LED blinks if FRU beaconing is enabled.

Backplane

The backplane provides 48 VDC power distribution and connections for all logic cards. The backplane is a nonconcurrent FRU. The director must be powered off prior to FRU removal and replacement.

Software Diagnostic Features

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

- Director FRUs provide on-board diagnostic and monitoring circuits that continuously report FRU status to the HAFM and *Product Manager* applications. These applications provide system alerts and logs that display failure and diagnostic information at the HAFM server or a remote workstation communicating with the HAFM server.
- The *HAFM* application that runs as a Windows 2000 service and provides an additional user interface to display director operational status.
- The Embedded Web Server interface that provides Internet access to isolate problems for a single director.
- Unsolicited SNMP trap messages that indicate operational state changes or failures can be transmitted to up to 12 authorized management workstations.
- E-mail messages or call-home reports provide automatic notification of significant system events to designated support personnel or administrators.

HAFM and Product Manager Diagnostics

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 HAFM and *Product Manager* applications provide a Java-based GUI to manage, monitor, and isolate problems for multiple directors and multiswitch fabrics.

The *HAFM* application opens automatically when the HAFM server is powered on, and the default display is the **Products View**. Managed products (including directors) display as icons at the top of the window.

Double-click a director icon to open the *Product Manager* application. The *Product Manager* application provides a Java-based GUI to manage, monitor, and isolate problems for a specific director. The application operates locally on the HAFM server or through an Ethernet LAN connection from a remote user workstation.

When the application opens, the default display is the **Hardware View**. A Director 2/140 Status table and a graphical representation of the director hardware (front and rear) display.

From the **Products View**, click the **Fabrics** tab to access the **Fabrics View**. The left panel of this view is the Fabric Tree, which is an expandable list of the fabrics, the products in the fabrics, and the nodes connected to the products.

Click the Topology tab to display the Topology View. This view displays graphical fabric elements and ISLs for a multiswitch fabric. The graphical representation of the fabric emulates the configuration and operational status of the corresponding real fabric. Note that a single director without ISLs is still considered a fabric.

Click the Zone Set tab to display the Zone Set View. This view displays the active zone set for the selected fabrics. The zones and zone members in the zone set display in a scrollable tree structure below the name of the active zone set.

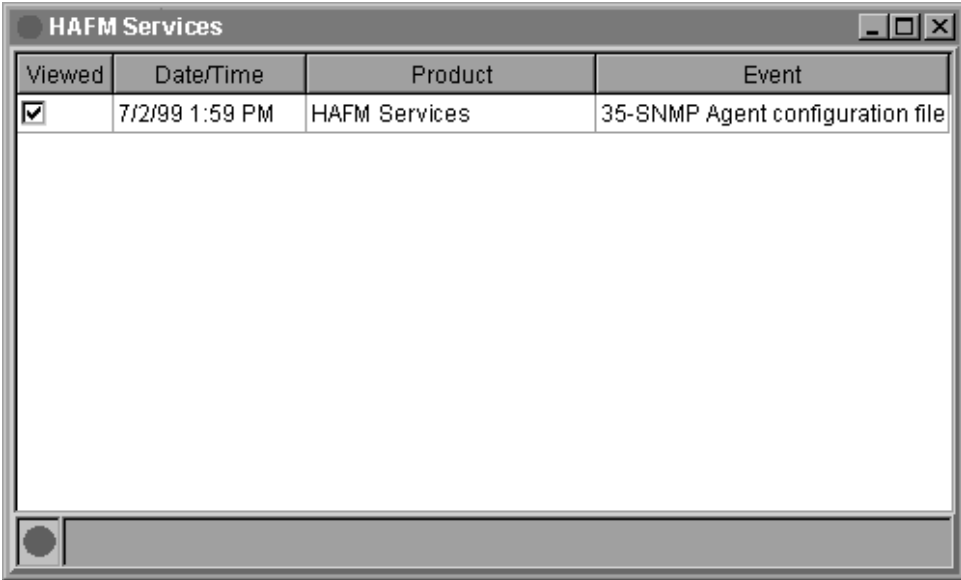
- For a description of the *Product Manager* application, refer to the *hp StorageWorks director product manager user guide*.
- For a description of the *HAFM* application, refer to the *hp StorageWorks ha-fabric manager user guide*.

HAFM Services Application

The HP StorageWorks High Availability Fabric Manager (*HAFM*) Services application provides a central control point and server-side functionality (in a client-server environment). The application runs as a Windows 2000 service and starts automatically when the HAFM server is powered on.

The user interface consists of the HAFM Services window ([Figure 1–8](#)), which provides *HAFM* application status and diagnostic information. The HAFM Services window consists of:

- An event table that displays *HAFM* application events that occurred since the *HAFM* application was started.
- A status line at the bottom of the panel that provides a status indicator and message area.



The screenshot shows a window titled "HAFM Services" with a table containing one row of event data. The table has four columns: "Viewed", "Date/Time", "Product", and "Event". The "Viewed" column contains a checked checkbox, "Date/Time" contains "7/2/99 1:59 PM", "Product" contains "HAFM Services", and "Event" contains "35-SNMP Agent configuration file".

Viewed	Date/Time	Product	Event
<input checked="" type="checkbox"/>	7/2/99 1:59 PM	HAFM Services	35-SNMP Agent configuration file

Figure 1–8: HAFM Services window

Event Table

The event table displays the last ten events that occurred since the *HAFM* application was started. Events that occurred during a prior instance of the application do not display. If a new event occurs while ten events display, the oldest event is discarded. A deeper event history is maintained in the form of a log file viewed through the *HAFM* application.

The events are internal error conditions detected by the *HAFM* application, and are not related to product-specific events reported by a director. Events typically relate to HAFM audit log and file corruption, invalid product definition and firmware files, missing product services class, or missing version information.

The event table contains the following columns:

- **Viewed**—This column provides a check box associated with each event. Each check box allows service personnel to mark an event as viewed (acknowledged with appropriate action taken).
- **Date/Time**—The date and time the event was reported to the HAFM server.

- **Product**—The product associated with the event. Some events are associated with the *HAFM* application, while others are associated with a specific instance of the *Product Manager* application. In the latter case, the product (Director 2/140) and configured name (or IP address) associated with the instance are displayed.
- **Event**—The numeric event code and a brief description of the event.





Status Line

The status line provides a status indicator and message area. HAFM status symbols are explained in [Table 1–1](#).

The *HAFM* application icon (upper left corner of the window) is dynamic and matches the status indicator. This feature allows users and service personnel to observe the status when the application is minimized to the **Windows 2000** task bar.

The message area briefly displays messages during *HAFM* application startup to indicate the progress of startup activities.

Table 1–1: HAFM Services Status Symbols

Alert Symbol	Meaning
Blank 	The status indicator is blank during <i>HAFM</i> application initialization.
Green circle 	All events are viewed (acknowledged with appropriate action taken).
Yellow triangle 	One or more nonfatal events have not been viewed.
Red diamond (with yellow background) 	A fatal error occurred.

Embedded Web Server Diagnostics

If HAFM server access is not available, the Embedded Web Server interface provides a GUI accessed through the Ethernet (locally or remotely) to manage, monitor, and isolate problems for a single director. This interface does not replace nor offer the full management capability of the HAFM and *Product Manager* applications.

The Embedded Web Server interface can be opened from a standard web browser running Netscape Navigator Version 4.6 (or higher) or Microsoft Internet Explorer Version 4.0 (or higher). At the browser, enter the IP address of the director as the Internet uniform resource locator (URL). When prompted at a login screen, enter a user name and password. When the interface opens, the default display is the View panel. Service personnel can perform monitoring, configuration, maintenance and diagnostic functions as follows:

- **View panel**—Quickly inspect and determine the operational status of the director, and inspect director properties and operating parameters, FRU properties, and Fibre Channel port properties.
- **Configure panel**—Configure or change:
 - Director Fibre Channel ports.
 - Director identification, date and time, operating parameters, and network addresses.
 - SNMP trap message recipients.
 - User passwords.
- **Monitor panel**—Inspect and monitor:
 - Fibre Channel ports and port performance statistics.
 - The active zone set.
 - Event log entries, and clear the system error LED at the director front bezel.
 - Information about attached devices (nodes).
- **Operations panel**—Perform the following operations and maintenance tasks:
 - Enable port beaconing and perform port diagnostics (internal and external loopback tests).
 - Reset Fibre Channel ports.
 - Set the director online state.
 - Upgrade director firmware.

General tasks performed through the web server interface are very similar in form and function to tasks performed through the HAFM and *Product Manager* applications; therefore, they are not documented in this publication. For task information and descriptions, open the online user documentation (Help selection) that supports the interface.

This publication provides instructions for director fault isolation using the Embedded Web Server interface. See [Diagnostics on page 2–1](#) for the fault isolation tasks.

SNMP Trap Message Support

Unsolicited SNMP trap messages that indicate director operational state changes or failure conditions can be customer-configured to be transmitted to up to 12 management workstations. If installed on a dedicated Ethernet LAN, the workstations communicate directly with each director. If installed on a customer intranet, workstations communicate with directors through the HAFM server.

SNMP data and trap messages are defined in the Fibre Channel FE-MIB definition, a subset of the TCP/IP MIB-II definition (RFC 1213), and a custom, director-specific MIB. Customers can install these MIBs (in standard ASN.1 format) on any SNMP management workstation.

Although SNMP trap messages are typically transmitted to customer personnel only, the messages may be provided to service personnel as initial notification of a director problem or as information included in the fault isolation process. Generic SNMP traps include:

- **coldStart**—Reports that the SNMP agent is reinitializing due to a director reset.
- **warmStart**—Reports that the SNMP agent is reinitializing due to a director IPL.
- **authorizationFailure**—Reports attempted director access by an unauthorized SNMP manager. This trap is configurable and is disabled by default.

Director-specific SNMP traps specified in the custom MIB include Fibre Channel port operational state changes and FRU operational state changes.

If authorized through the **Configure SNMP** dialog box in the *Product Manager* application, users at SNMP management workstations can modify MIB variables.

- Director modifications performed through SNMP management work stations are recorded in the associated director audit log and are available through the *Product Manager* application. For additional information, refer to the *hp StorageWorks SNMP reference guide for directors and edge switches*.

E-Mail and Call-Home Support

If e-mail notification and call-home support are configured for the director as part of the customer support process, service personnel may be:

- Notified of a director problem by e-mail message, either directly or through a system administrator at the customer site or call center.

- Assigned a service call from call center personnel upon receipt and confirmation of a director call-home event.

Tools and Test Equipment

This section describes tools and test equipment that may be required to test, service, and verify operation of the director and attached HAFM server. These tools are either supplied with the director or must be supplied by service personnel.

Tools Supplied with the Director

The following tools are supplied with the director. These tools may be required to perform test, service, or verification tasks.

- **Torque tool with hexagonal adapter**—The torque tool with 5/32” hexagonal adapter (Figure 1–9) is required to remove and replace director logic cards.



CAUTION: The torque tool supplied with the director is designed to tighten director logic cards and is set to release at a torque value of six inch-pounds. Do not use an Allen wrench or torque tool designed for use with another HP product. Use of the wrong tool may overtighten and damage logic cards.

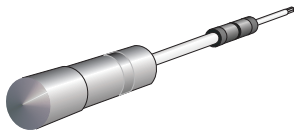


Figure 1–9: Torque tool and hex adapter

- **Fiber-optic loopback plug**—An SFP multimode (shortwave laser) or singlemode (longwave laser) loopback plug (Figure 1–10) is required to perform port loopback diagnostic tests. Four multimode loopback plugs are shipped with the director. Both plug types are shipped if shortwave laser and longwave laser transceivers are installed.

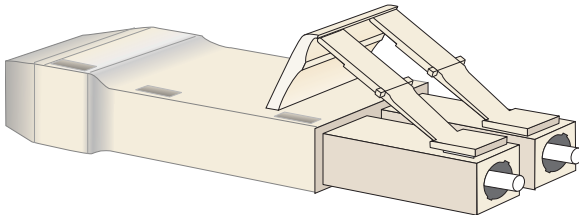
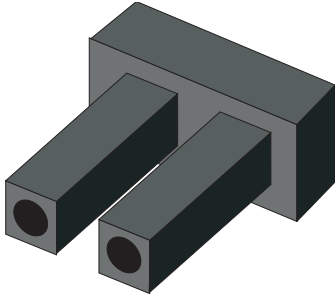
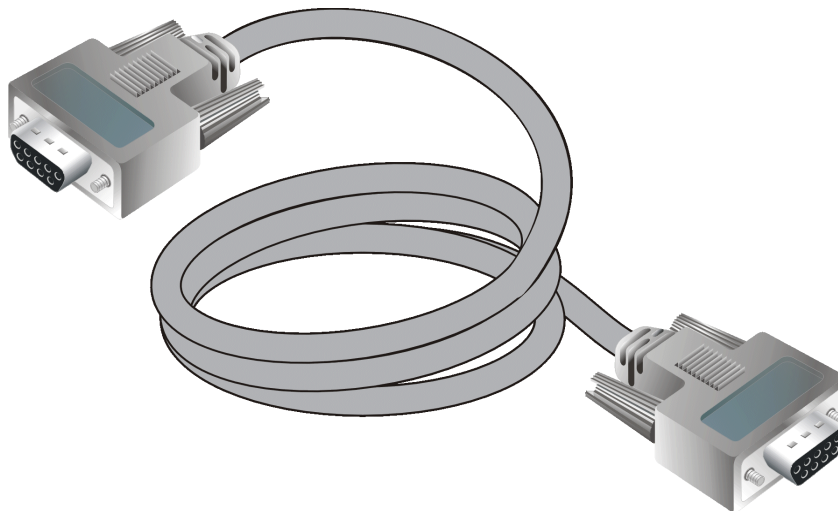


Figure 1–10: SFP fiber-optic loopback plug

- **Fiber-optic protective plug**—For safety and port transceiver protection, fiber-optic protective plugs ([Figure 1–11](#)) must be inserted in all director ports without fiber-optic cables attached. The director is shipped with protective plugs installed in all ports.

**Figure 1–11: Fiber-optic protective plug**

- **Null modem cable**—An asynchronous RS-232 null modem cable ([Figure 1–12](#)) is required to configure director network addresses and acquire event log information through the maintenance port. The cable has nine conductors and DB-9 male and female connectors.

**Figure 1–12: Null modem cable**

Tools Supplied by Service Personnel

The following tools are expected to be supplied by service personnel performing director maintenance actions. Use of the tools may be required to perform one or more 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 replacement FRUs.
- **Standard flat-tip and cross-tip (Phillips) screwdrivers**—Screwdrivers are required to remove, replace, adjust or tighten various FRUs, chassis, or cabinet components.
- **Electrostatic discharge (ESD) grounding cable with attached wrist strap**—Use of the ESD wrist strap is required when working in and around the director card cage.
- **Maintenance terminal (desktop or notebook PC)**—The PC is required to configure director network addresses and acquire event log information through the maintenance port. The PC must have:
 - The Microsoft Windows 98, Windows 2000, Windows XP, or Windows Millennium Edition operating system installed.
 - RS-232 serial communication software installed, such as ProComm Plus or HyperTerminal. 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.

Diagnostics

This chapter describes diagnostic procedures used by service representatives to fault isolate the Director 2/140 problems or failures to the field-replaceable unit (FRU) level. The chapter describes how to perform the maintenance analysis procedures (MAPs).

Maintenance Analysis Procedures

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.

Fault isolation and related service procedures are provided through MAPs. The procedures vary depending on the diagnostic information provided. 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 events, isolate a director failure to a single FRU, remove and replace the failed FRU, and verify director 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. Fault isolation normally begins at [MAP 0000: Start MAP on page 2–12](#).

However, [Table 2–3](#) lists the event codes and the corresponding MAPs. It is a quick start, if an event code is readily available.

Table 2–2: MAP Summary

MAP	Page
MAP 0000: Start MAP	2–12
MAP 0100: Power Distribution Analysis	2–36
MAP 0200: POST Failure Analysis	2–46
MAP 0300: Console Application Problem Determination	2–51
MAP 0400: Loss of Console Communication	2–58
MAP 0500: FRU Failure Analysis	2–71
MAP 0600: UPM Card Failure and Link Incident Analysis	2–79
MAP 0700: Fabric, ISL, and Segmented Port Problem Determination	2–99
MAP 0800: Console PC Problem Determination	2–112

Table 2–3: Event Codes Versus Maintenance Action

Event Code	Explanation	Action
001	System power-down.	Power on director.
010	Login server unable to synchronize databases.	Go to MAP 0700: Fabric, ISL, and Segmented Port Problem Determination .
011	Login server database invalid.	Go to MAP 0700: Fabric, ISL, and Segmented Port Problem Determination .
020	Name server unable to synchronize databases.	Go to MAP 0700: Fabric, ISL, and Segmented Port Problem Determination .

Table 2-3: Event Codes Versus Maintenance Action (Continued)

Event Code	Explanation	Action
021	Name server database invalid.	Go to MAP 0700: Fabric, ISL, and Segmented Port Problem Determination .
031	SNMP request received from unauthorized community.	Add community name.
050	Management server unable to synchronize databases.	Go to MAP 0700: Fabric, ISL, and Segmented Port Problem Determination .
051	Management server database invalid.	Go to MAP 0700: Fabric, ISL, and Segmented Port Problem Determination .
052	Management server internal error.	Go to MAP 0700: Fabric, ISL, and Segmented Port Problem Determination .
060	Fabric controller unable to synchronize databases.	Go to MAP 0700: Fabric, ISL, and Segmented Port Problem Determination .
061	Fabric controller database invalid.	Go to MAP 0700: Fabric, ISL, and Segmented Port Problem Determination .
062	Maximum interswitch hop count exceeded.	Go to MAP 0700: Fabric, ISL, and Segmented Port Problem Determination .
063	Received link state record too large.	Go to MAP 0700: Fabric, ISL, and Segmented Port Problem Determination .
070	E_Port is segmented.	Go to MAP 0700: Fabric, ISL, and Segmented Port Problem Determination .
071	Director is isolated.	Go to MAP 0700: Fabric, ISL, and Segmented Port Problem Determination .

Table 2-3: Event Codes Versus Maintenance Action (Continued)

Event Code	Explanation	Action
072	E_Port connected to unsupported switch.	Go to MAP 0700: Fabric, ISL, and Segmented Port Problem Determination .
073	Fabric initialization error.	Event data intended for engineering evaluation. Perform data collection procedure (Collecting Maintenance Data on page 3-40) and return Zip disk to HP support personnel.
074	ILS frame delivery error threshold exceeded.	Event data intended for engineering evaluation. Perform data collection procedure (Collecting Maintenance Data on page 3-40) and return Zip disk to HP support personnel.
080	Unauthorized world-wide name.	Go to MAP 0600: UPM Card Failure and Link Incident Analysis .
081	Invalid attachment.	Go to MAP 0600: UPM Card Failure and Link Incident Analysis .
090	Database replication time out.	Perform the data collection procedure and return the information to HP for analysis by third-level support personnel.
091	Database replication discontinued.	No action required, unless this Event occurs without the backup CTP failing or being removed. If so, perform the data collection procedure and return the information to HP for analysis by third-level support personnel.

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

Event Code	Explanation	Action
120	Error while processing system management command.	If this event persists, perform data collection procedure (Collecting Maintenance Data on page 3–40) and return Zip disk to HP support personnel.
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: Power Distribution Analysis .
201	Power supply DC voltage failure.	Go to MAP 0100: Power Distribution Analysis .
202	Power supply thermal failure.	Go to MAP 0100: Power Distribution Analysis .
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.
208	Power supply false shutdown.	Go to MAP 0100: Power Distribution Analysis .
300	Cooling fan propeller failed.	Go to MAP 0500: FRU Failure Analysis
301	Cooling fan propeller failed.	Go to MAP 0500: FRU Failure Analysis .
302	Cooling fan propeller failed.	Go to MAP 0500: FRU Failure Analysis .
303	Cooling fan propeller failed.	Go to MAP 0500: FRU Failure Analysis .
304	Cooling fan propeller failed.	Go to MAP 0500: FRU Failure Analysis .
305	Cooling fan propeller failed.	Go to MAP 0500: FRU Failure Analysis .

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

Event Code	Explanation	Action
310	Cooling fan propeller recovered.	No action required.
311	Cooling fan propeller recovered.	No action required.
312	Cooling fan propeller recovered.	No action required.
313	Cooling fan propeller recovered.	No action required.
314	Cooling fan propeller recovered.	No action required.
315	Cooling fan propeller recovered.	No action required.
320	Fan module removed.	Replace FRU.
321	Fan module installed.	No action required.
400	Power-up diagnostic failure.	Go to MAP 0200: POST Failure Analysis .
410	CTP card reset.	No action required.
411	Firmware fault.	Go to MAP 0200: POST Failure Analysis .
413	Backup CTP card POST failure.	Go to MAP 0200: POST Failure Analysis .
414	Backup CTP card failed.	Go to MAP 0500: FRU Failure Analysis .
415	Backup CTP card removed.	Replace FRU.
416	Backup CTP card installed.	No action required.
417	CTP card firmware synchronization initiated.	No action required.
418	User-initiated CTP card switchover.	No action required.
420	Backup CTP card NV-RAM failure.	Go to MAP 0500: FRU Failure Analysis .
421	Firmware download complete.	No action required.

Table 2-3: Event Codes Versus Maintenance Action (Continued)

Event Code	Explanation	Action
422	CTP firmware synchronization complete.	No action required.
423	CTP firmware download initiated.	No action required.
430	Excessive Ethernet transmit errors.	Go to MAP 0400: Loss of Console Communication .
431	Excessive Ethernet receive errors.	Go to MAP 0400: Loss of Console Communication .
432	Ethernet adapter reset.	Go to MAP 0400: Loss of Console Communication .
433	Non-recoverable Ethernet fault.	Go to MAP 0500: FRU Failure Analysis .
440	Embedded port hardware failed.	Go to MAP 0500: FRU Failure Analysis .
442	Embedded port anomaly detected.	No action required.
450	Serial Number mismatch detected.	No action required – any configured Feature Keys will be cleared, configuration information will be synched with the backplane VPD and the CTP will automatically be IPLed.
451	Switch speed incompatibility detected.	No action required – Switch speed configuration and port speed configuration data will be set to a level that is compatible with the CTP and the CTP will automatically be IPLed.

Table 2-3: Event Codes Versus Maintenance Action (Continued)

Event Code	Explanation	Action
452	Backup CTP incompatible with configured system settings.	Replace the backup CTP with a version of hardware capable of supporting the user-configured settings, or adjust the user settings to be compatible with the backup CTP, and reseal the backup CTP.
453	New feature key installed.	No action required.
460	Management request out of range.	The director found request data from the management tool (typically the <i>HAFM</i> application) to be larger or smaller than expected. The connection to the management tool will be temporarily lost. After the link is reestablished, verify that all information changed in the managing tool is within the specified ranges. For example, verify that the zones and zone members in a zone set fall within the limits stated in the user manual. Try sending the request again.
500	UPM card hot-insertion initiated.	No action required.
501	UPM card recognized.	No action required.
502	UPM card anomaly detected.	No action required.
503	UPM card hot-removal completed.	No action required.
504	UPM card failure.	Go to MAP 0600: UPM Card Failure and Link Incident Analysis .

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

Event Code	Explanation	Action
505	UPM card revision not supported.	Go to MAP 0600: UPM Card Failure and Link Incident Analysis .
506	Fibre Channel port failure.	Go to MAP 0600: UPM Card Failure and Link Incident Analysis .
507	Loopback diagnostics port failure.	Go to MAP 0600: UPM Card Failure and Link Incident Analysis .
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: UPM Card Failure and Link Incident Analysis .
513	SFP optical transceiver hot-removal completed.	No action required.
514	SFP optical transceiver failure.	Go to MAP 0600: UPM Card Failure and Link Incident Analysis .
581	Implicit incident.	Go to MAP 0600: UPM Card Failure and Link Incident Analysis .
582	Bit error threshold exceeded.	Go to MAP 0600: UPM Card Failure and Link Incident Analysis .
583	Loss of signal or loss of synchronization.	Go to MAP 0600: UPM Card Failure and Link Incident Analysis .
584	Not operational primitive sequence received.	Go to MAP 0600: UPM Card Failure and Link Incident Analysis .

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

Event Code	Explanation	Action
585	Primitive sequence timeout.	Go to MAP 0600: UPM Card Failure and Link Incident Analysis .
586	Invalid primitive sequence received for current link state.	Go to MAP 0600: UPM Card Failure and Link Incident Analysis .
600	SBAR assembly hot-insertion initiated.	No action required.
601	SBAR assembly recognized.	No action required.
602	SBAR assembly anomaly detected.	No action required.
603	SBAR assembly hot-removal completed.	No action required.
604	SBAR assembly failure.	Go to MAP 0500: FRU Failure Analysis .
605	SBAR assembly revision not supported.	Go to MAP 0500: FRU Failure Analysis .
607	Director contains no operational SBAR assemblies.	Go to MAP 0500: FRU Failure Analysis .
608	User initiated SBAR switch-over.	No action required.
800	High temperature warning (UPM card thermal sensor).	Go to MAP 0600: UPM Card Failure and Link Incident Analysis .
801	Critically hot temperature warning (UPM card thermal sensor).	Go to MAP 0600: UPM Card Failure and Link Incident Analysis .
802	UPM card shutdown due to thermal violation.	Go to MAP 0600: UPM Card Failure and Link Incident Analysis .
805	High temperature warning (SBAR assembly thermal sensor).	Go to MAP 0500: FRU Failure Analysis .

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

Event Code	Explanation	Action
806	Critically hot temperature warning (SBAR assembly thermal sensor).	Go to MAP 0500: FRU Failure Analysis .
807	SBAR assembly shutdown due to thermal violation.	Go to MAP 0500: FRU Failure Analysis .
810	High temperature warning (CTP card thermal sensor).	Go to MAP 0500: FRU Failure Analysis .
811	Critically hot temperature warning (CTP card thermal sensor).	Go to MAP 0500: FRU Failure Analysis .
812	CTP card shutdown due to thermal violation.	Go to MAP 0500: FRU Failure Analysis .
850	System shutdown due to CTP card thermal violations.	Go to MAP 0500: FRU Failure Analysis .

MAP 0000: Start MAP

This MAP describes initial fault isolation for the Director 2/140. Fault isolation begins at the HAFM server, failed director, or Internet-connected personal computer (PC) running the Embedded Web Server 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, directors, other HP products, and device connections.
- The location of the HAFM server and all directors.
- The internet protocol (IP) address, gateway address, and subnet mask for the director reporting the problem.
- If performing fault isolation using the HAFM server:
 - The Windows 2000 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 the Embedded Web Server interface, the director user name and password. Both are case sensitive and required when prompted at the **Username and Password Required** dialog box.

Continue.

2

Are you at the HAFM server?

YES **NO**

↓ Go to [step 24](#).

3

Did the HAFM 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 2000** dialog box?

NO YES

- ↓ An HAFM server application problem is indicated. Event codes are not recorded. Go to [MAP 0300: Console Application Problem Determination on page 2–51](#). **Exit MAP.**

4

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

NO YES

- ↓ An HAFM server application problem is indicated. Event codes are not recorded. Go to [MAP 0300: Console Application Problem Determination on page 2–51](#). **Exit MAP.**

5

Is the *HAFM* application active?

NO YES

- ↓ Go to [step 7](#).

6

Reboot the HAFM server PC.

1. Choose **Start > Shut Down**. The **Shut Down Windows** dialog box displays.
2. Choose **Shut Down The Computer** and click **Yes** to power off the PC.
3. Wait approximately 30 seconds and power on the PC. After POSTs complete, the **Begin Logon** dialog box displays.
4. Simultaneously press **Ctrl + Alt + Delete** to display the **Logon Information** dialog box. Type a user name and password (obtained in [step 1](#)) and click **OK**. The *HAFM* application starts and the **HAFM Logon** dialog box displays.
5. 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** ([Figure 2–1](#)) displays.

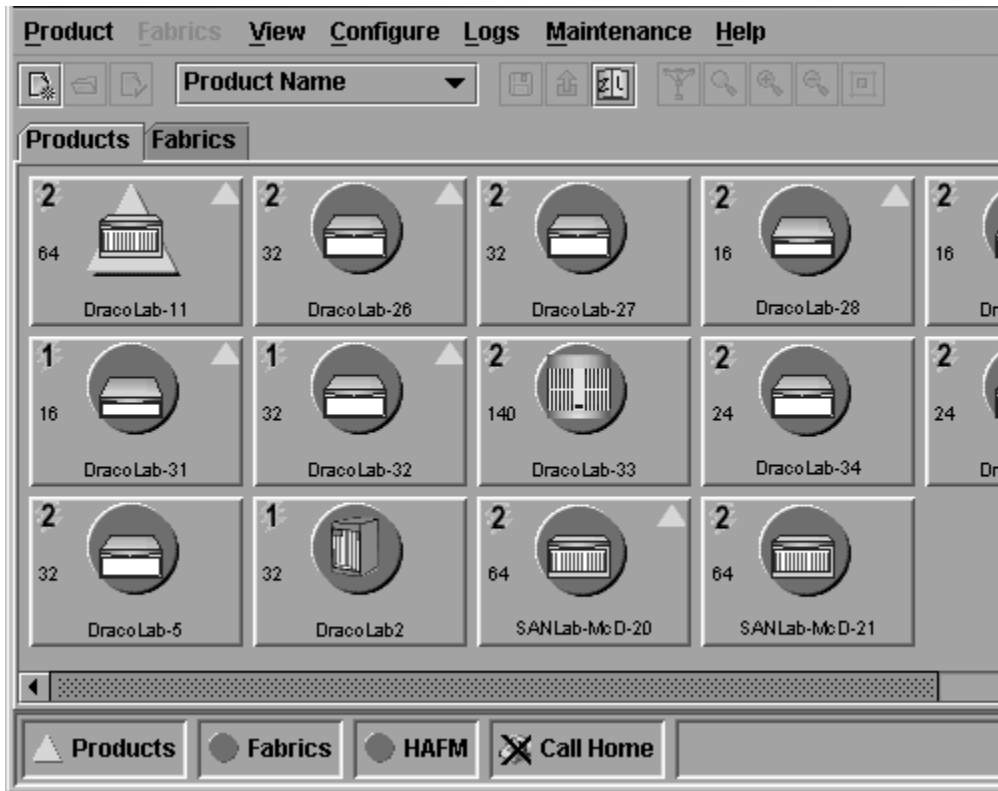


Figure 2-1: Products View

Did the **Products View** display and is the *HAFM* application operational?

YES **NO**

- ↓ An HAFM server hardware problem is indicated. Event codes are not recorded. Go to [MAP 0800: Console PC Problem Determination on page 2-112](#). **Exit MAP.**

7

Inspect the alert indicators of each managed director at the top of the **Products View**. The indicator shows the status of managed directors or the status of the link between the HAFM server and managed directors as follows:

- A green circle indicates that the director is operational.
- A yellow triangle indicates that the director is operating in degraded mode.

- A red diamond with yellow background indicates that the director is not operational.
- A grey square indicates that the status of the director is unknown.

Does a grey square display as the background to the icon representing the director reporting the problem?

YES **NO**

↓ Go to [step 11](#).

The grey square indicates the HAFM server cannot communicate with the director because:

- The director-to-HAFM server Ethernet link failed.
- AC power distribution in the director failed, or AC power was disconnected.
- Both of the director's control processor (CTP) cards failed.

Continue.

8

Ensure the director reporting the problem is connected to facility AC power and the power switch (circuit breaker) at the rear of the director is set to the **ON** (up) position. Inspect the director for indications of being powered on, such as:

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- An illuminated green LED on the active CTP card, and illuminated green **PWR OK** LEDs on both power supplies.
- Audio emanations and airflow from cooling fans.

Is the director powered on?

YES **NO**

↓ A power distribution problem is indicated. Go to [step 23](#) to obtain event codes. If no event codes are found, go to [MAP 0100: Power Distribution Analysis on page 2–36](#). **Exit MAP.**

9

At the director, inspect the amber LED at the top of each CTP card.

Is the amber LED illuminated on both CTP cards?

NO YES

↓ Failure of both CTP cards is indicated. Event codes are not recorded. Go to [MAP 0500: FRU Failure Analysis on page 2–71](#). **Exit MAP.**

10

A director-to-HAFM server Ethernet link failure is indicated.

Go to [step 23](#) to obtain event codes. If no event codes are found, go to [MAP 0400: Loss of Console Communication on page 2–58](#).

Exit MAP.

11

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

YES NO

↓ Go to [step 14](#).

12

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

- Observe the director Status table is yellow and the director 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 all UPM card graphics?

NO YES

↓ Failure of all installed UPM cards is indicated. **Go to [step 23](#)** to obtain event codes. If no event codes are found, go to [MAP 0600: UPM Card Failure and Link Incident Analysis on page 2–79](#). **Exit MAP.**

13

Blinking red and yellow diamonds overlay both serial crossbar (SBAR) assembly graphics or both fan module graphics.

Redundant FRU failures are indicated. **Go to step 23** to obtain event codes. If no event codes are found, go to [MAP 0500: FRU Failure Analysis on page 2–71](#). **Exit MAP.**

14

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

YES **NO**

↓ Go to [step 18](#).

15

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

- Observe the Director 2/140 Status table is yellow and the director 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 23](#) to obtain event codes. If no event codes are found, go to [MAP 0100: Power Distribution Analysis on page 2–36](#). **Exit MAP.**

16

Does a blinking red and yellow diamond overlay a UPM card graphic?

NO **YES**

↓ A UPM card failure is indicated. Go to [step 23](#) to obtain event codes. If no event codes are found, go to [MAP 0600: UPM Card Failure and Link Incident Analysis on page 2–79](#). **Exit MAP.**

17

A blinking red and yellow diamond overlays a control processor (CTP) card, SBAR assembly, or fan module graphic.

A FRU failure is indicated. Go to [step 23](#) to obtain event codes. If no event codes are found, go to [MAP 0500: FRU Failure Analysis on page 2–71](#). **Exit MAP.**

18

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

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

- Inspect CTP cards, SBAR assemblies, and fan modules for a yellow triangle that overlays the FRU graphic and indicates FRU beaconing is enabled.
- Inspect UPM cards for a yellow triangle (attention indicator) that overlays the UPM card graphic.

Does a yellow triangle overlay a CTP card, SBAR assembly, or fan module graphic?

YES **NO**

↓ Go to [step 20](#).

19

Beaconing is enabled for the FRU.

1. Consult the customer and next level of support to determine the reason FRU beaconing is enabled.
2. Disable FRU beaconing.
 - a. At the **Hardware View**, right-click the FRU graphic. A menu displays.
 - b. Click **Enable Beaconing**. 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 director is operational. **Exit MAP.**

Go to [step 22](#).

20

Does a yellow triangle (attention indicator) overlay a UPM card graphic?

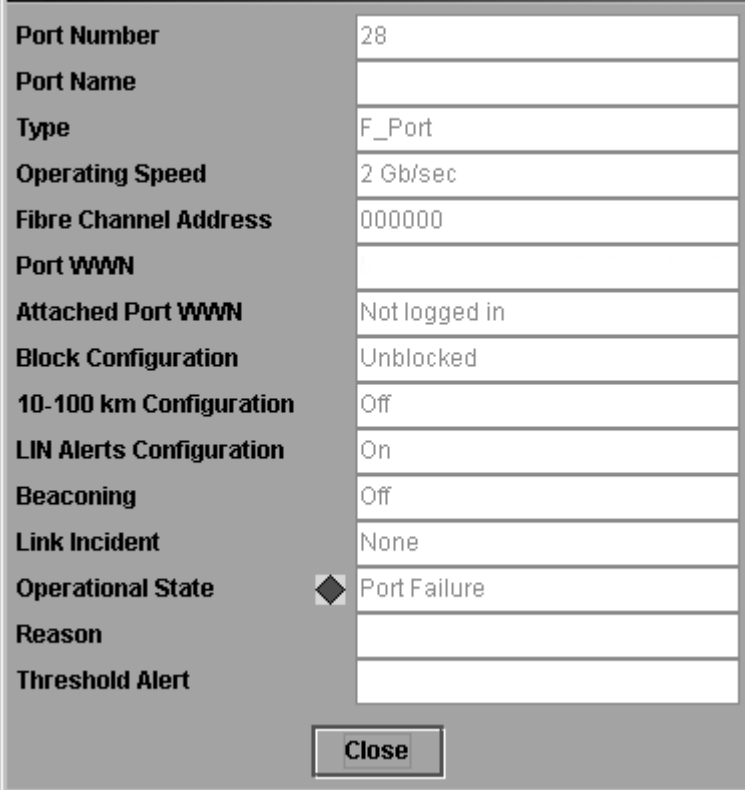
YES **NO**

↓ Go to [step 22](#).

21

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

1. Double-click the UPM card. The **Port Card View** displays.
2. Double-click the port graphic with the attention indicator. The **Port Properties** dialog box displays, as shown in [Figure 2-2](#).



Port Number	28
Port Name	
Type	F_Port
Operating Speed	2 Gb/sec
Fibre Channel Address	000000
Port WWN	
Attached Port WWN	Not logged in
Block Configuration	Unblocked
10-100 km Configuration	Off
LIN Alerts Configuration	On
Beaconing	Off
Link Incident	None
Operational State	◆ Port Failure
Reason	
Threshold Alert	

Figure 2-2: Port Properties dialog box

3. 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 23](#) to obtain event codes. If no event codes are found, go to [MAP 0700: Fabric, ISL, and Segmented Port Problem Determination on page 2–99](#). **Exit MAP.**

A message displays indicating a link incident problem. Go to [step 23](#) to obtain event codes. If no event codes are found, go to [MAP 0600: UPM Card Failure and Link Incident Analysis on page 2–79](#).

Exit MAP.

22

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

1. At the **Hardware View** or **Port Card View**, choose **Logs > Link Incident Log**. The **Link Incident Log** displays, as shown in [Figure 2–3](#).

Date/Time	Port	Link Incident
11/25/02 1:50:34 PM	43	Loss-of-Signal or Loss-of-Synchronization.
11/25/02 1:45:05 PM	43	Loss-of-Signal or Loss-of-Synchronization.
11/21/02 4:12:17 PM	43	Loss-of-Signal or Loss-of-Synchronization.
11/21/02 4:09:30 PM	43	Loss-of-Signal or Loss-of-Synchronization.
11/21/02 3:59:31 PM	43	Loss-of-Signal or Loss-of-Synchronization.
11/21/02 3:55:25 PM	43	Loss-of-Signal or Loss-of-Synchronization.
11/21/02 3:48:23 PM	43	Loss-of-Signal or Loss-of-Synchronization.
11/21/02 3:14:55 PM	43	Loss-of-Signal or Loss-of-Synchronization.
11/21/02 3:12:36 PM	0	Loss-of-Signal or Loss-of-Synchronization.
11/21/02 3:12:36 PM	26	Loss-of-Signal or Loss-of-Synchronization.
11/21/02 3:06:02 PM	43	Loss-of-Signal or Loss-of-Synchronization.
11/21/02 2:58:20 PM	8	Loss-of-Signal or Loss-of-Synchronization.
11/21/02 2:40:56 PM	8	Loss-of-Signal or Loss-of-Synchronization.
11/21/02 2:40:27 PM	26	Not Operational primitive sequence (NOS) received.
11/21/02 2:40:01 PM	43	Loss-of-Signal or Loss-of-Synchronization.
11/21/02 2:01:30 PM	43	Loss-of-Signal or Loss-of-Synchronization.

Export... Clear Refresh Close

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 display in the **Link Incident Log**?

YES NO

↓ The director is operational. **Exit MAP.**

A link incident problem is indicated. Go to [step 23](#) to obtain event codes. If no event codes are found, go to [MAP 0600: UPM Card Failure and Link Incident Analysis on page 2–79](#). **Exit MAP.**

23

Obtain event codes from the director Event Log.

NOTE: 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 has been recovered.

1. At the **Hardware View**, choose **Logs > Event Log**. The **Event Log** displays, as shown in [Figure 2–4](#).
2. Record the event code, date, time, and severity (**Informational**, **Minor**, **Major**, or **Severe**).
3. Record all event codes that may relate to the reported problem.

Date/Time	Event	Description	Severity	FR
11/21/02 10:56:53 AM	430	Excessive Ethernet transmit errors.	Informational	CTF
11/21/02 9:51:14 AM	430	Excessive Ethernet transmit errors.	Informational	CTF
11/21/02 8:50:22 AM	430	Excessive Ethernet transmit errors.	Informational	CTF
11/21/02 7:58:03 AM	430	Excessive Ethernet transmit errors.	Informational	CTF
11/21/02 7:13:26 AM	430	Excessive Ethernet transmit errors.	Informational	CTF
11/21/02 6:29:17 AM	430	Excessive Ethernet transmit errors.	Informational	CTF
11/21/02 5:42:50 AM	506	Fibre Channel port failure.	Major	GSF
11/21/02 5:42:50 AM	508	Fibre Channel port anomaly detected.	Informational	GSF
11/21/02 5:42:48 AM	508	Fibre Channel port anomaly detected.	Informational	GSF
11/21/02 5:42:46 AM	508	Fibre Channel port anomaly detected.	Informational	GSF
11/21/02 5:28:27 AM	430	Excessive Ethernet transmit errors.	Informational	CTF
11/21/02 4:17:43 AM	430	Excessive Ethernet transmit errors.	Informational	CTF
11/21/02 3:16:45 AM	430	Excessive Ethernet transmit errors.	Informational	CTF
11/21/02 2:15:23 AM	430	Excessive Ethernet transmit errors.	Informational	CTF
11/21/02 1:27:06 AM	430	Excessive Ethernet transmit errors.	Informational	CTF
11/21/02 12:35:51 AM	430	Excessive Ethernet transmit errors.	Informational	CTF
11/20/02 11:34:57 PM	430	Excessive Ethernet transmit errors.	Informational	CTF

◀

Export... Clear Refresh

Figure 2–4: Event Log

Were one or more event codes found?

NO YES

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

Return to the MAP step that sent you here.

24

Are you at the director reporting the problem?

YES NO

↓ Go to [step 36](#).

25

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

NO YES

↓ Go to [step 30](#).

26

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

NO YES

↓ Go to [step 29](#).

27

Connect the director to facility AC power and set the power switch (circuit breaker) at the rear of the director to the **ON** (up) position. Inspect the director for indications of being powered on, such as:

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- An illuminated green LED on the active CTP card, and illuminated green **PWR OK** LEDs on both power supplies.
- Audio emanations and airflow from cooling fans.

Is the director powered on?

YES NO

- ↓ A power distribution problem is indicated. Go to [step 23](#) to obtain event codes. If no event codes are found, go to [MAP 0100: Power Distribution Analysis on page 2–36](#). **Exit MAP.**
-

28

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

NO YES

- ↓ Go to [step 30](#).

A faulty power LED is indicated, but director 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 ([RRP: Redundant Fan Module on page 4–27](#)). **Exit MAP.**

29

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

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- An illuminated green LED on the active CTP card, and illuminated green **PWR OK** LEDs on both power supplies.
- Audio emanations and airflow from cooling fans.

Is the director powered on?

YES NO

- ↓ A power distribution problem is indicated. Go to [step 23](#) to obtain event codes. If no event codes are found, go to [MAP 0100: Power Distribution Analysis on page 2–36](#). **Exit MAP.**

A faulty power LED is indicated, but director 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 ([RRP: Redundant Fan Module on page 4–27](#)). **Exit MAP.**

30

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

YES NO

↓ Go to [step 32](#).

31

Unit beaconing is enabled for the director.

1. Consult the customer and next level of support to determine the reason unit beaconing is enabled.
2. Disable unit beaconing.
 - a. At the **Hardware View**, right-click the front bezel graphic (away from a FRU). A menu displays.
 - b. Click **Enable Unit Beaconing**. The check mark disappears from the box adjacent to the option, and unit beaconing is disabled.

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

YES **NO**

↓ The director is operational. **Exit MAP.**

Go to [step 24](#).

32

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

YES **NO**

↓ The director is operational. Verify operation at the HAFM server. Go to [step 3](#).

33

Check FRUs (UPM cards, CTP cards, SBAR assemblies, power supplies, and fan modules) for failure symptoms.

Is the amber LED at the top of a UPM card illuminated or are any amber LEDs associated with Fibre Channel ports illuminated?

NO **YES**

↓ A UPM card or Fibre Channel port failure is indicated. Go to [step 23](#) to obtain event codes. If no event codes are found, go to [MAP 0600: UPM Card Failure and Link Incident Analysis on page 2-79](#). **Exit MAP.**

34

Is the amber LED on a CTP card, SBAR assembly, or fan module illuminated?

NO **YES**

↓ A FRU failure is indicated. Go to [step 23](#) to obtain event codes. If no event codes are found, go to [MAP 0500: FRU Failure Analysis on page 2–71](#). **Exit MAP.**

35

Is the green **PWR OK** LED on a power supply extinguished?

NO **YES**

↓ A power supply failure is indicated. Go to [step 23](#) to obtain event codes. If no event codes are found, go to [MAP 0100: Power Distribution Analysis on page 2–36](#). **Exit MAP.**

The director is operational. **Exit MAP.**

36

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

YES **NO**

↓ Go to [step 53](#).

37

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

NO **YES**

↓ Go to [step 39](#).

38

Boot the web browser PC.

1. Power on the PC in accordance with the instructions delivered with the PC. The Windows desktop displays.
-

2. Launch the PC browser application by double-clicking the appropriate icon at the Windows desktop.
3. 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 director (obtained in step 1 on page 2-12). The **Username And Password Required** dialog box displays.
4. Type the user name and password obtained in [step 1](#), and click **OK**. The **Embedded Web Server** interface opens with the **View** panel displayed, as shown in [Figure 2-5](#).

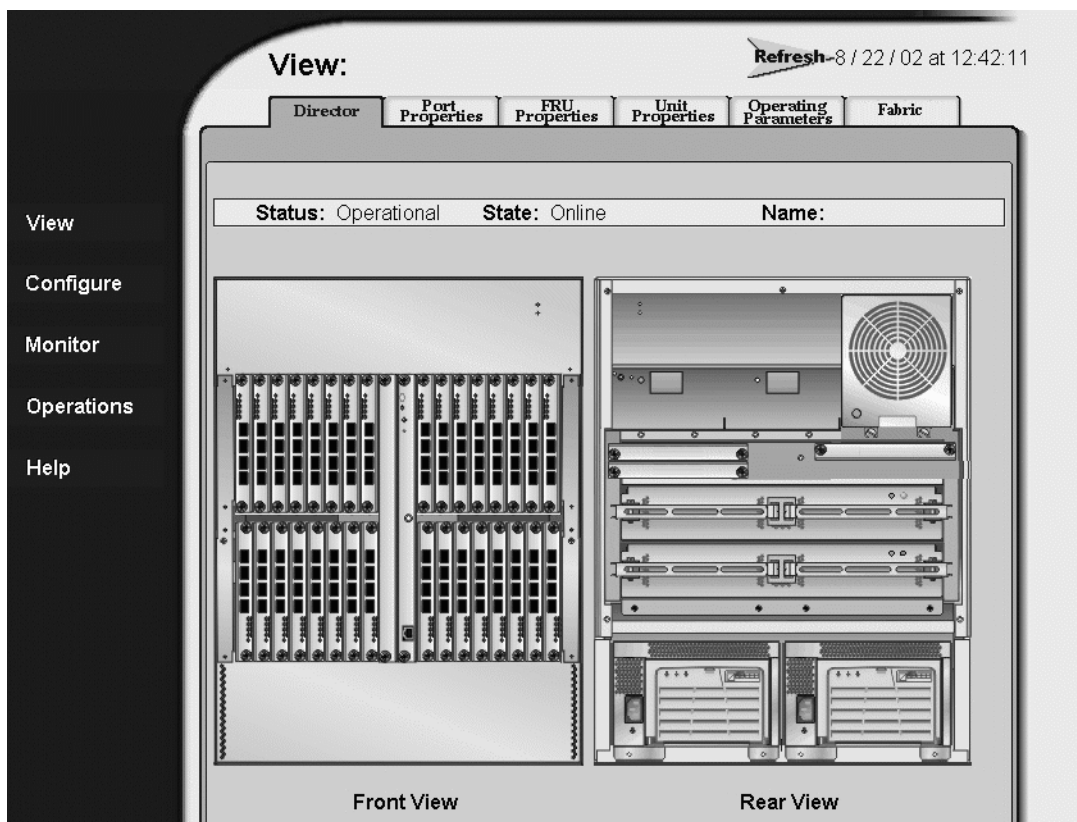


Figure 2-5: View panel

Continue.

39

Is the Embedded Web Server interface operational with the **View** panel displayed?

NO **YES**

↓ Go to [step 44](#).

40

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

- The director-to-PC Internet link could not be established.
- AC power distribution in the director failed, or AC power was disconnected.
- Both of the director's CTP cards failed.

Continue.

41

Ensure the director reporting the problem is connected to facility AC power and the power switch (circuit breaker) at the rear of the director is set to the **ON** (up) position. Inspect the director for indications of being powered on, such as:

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- An illuminated green LED on the active CTP card, and illuminated green **PWR OK** LEDs on both power supplies.
- Audio emanations and airflow from cooling fans.

Is the director powered on?

YES **NO**

↓ A power distribution problem is indicated. Go to [MAP 0100: Power Distribution Analysis on page 2–36](#). **Exit MAP.**

42

At the director, inspect the amber LED at the top of each CTP card.

Is the amber LED illuminated on both CTP cards?

NO YES

- ↓ Failure of both CTP cards is indicated. Event codes are not recorded. Go to [MAP 0500: FRU Failure Analysis on page 2–71](#). **Exit MAP.**

43

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

1. Wait approximately five minutes, then attempt to login to the director again.
2. 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 director (obtained in [step 1](#)). The **Username and Password Required** dialog box displays.
3. 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.

Is the Embedded Web Server interface operational with the **View** panel displayed?

YES NO

- ↓ Perform director fault isolation at the HAFM server. Go to [step 3](#).

44

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

Does the director status indicate **Operational**?

NO YES

- ↓ The director is operational. **Exit MAP.**

45

Inspect Fibre Channel port operational states.

1. At the **View** panel, click the **Port Properties** tab. The **View Port Properties** panel displays, as shown in [Figure 2–6](#).
2. Inspect the **Beaconing** and **Operational State** fields.

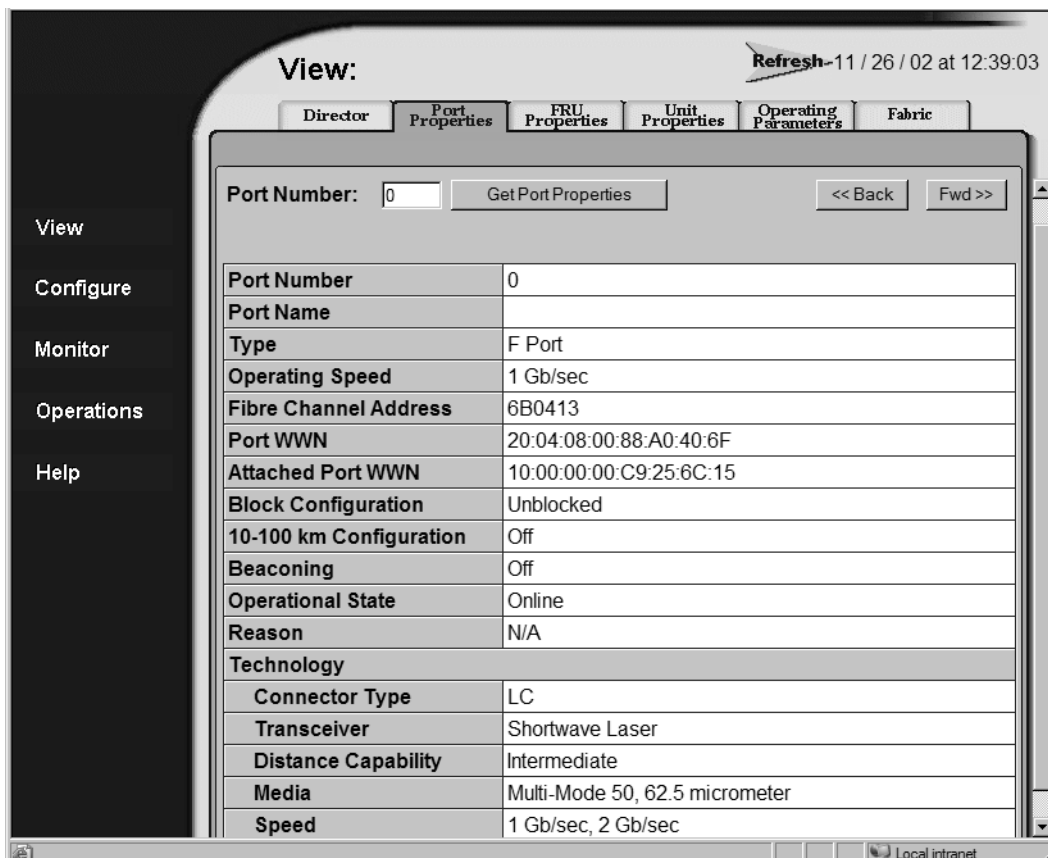


Figure 2–6: View Port Properties panel

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

YES NO

↓ Go to [step 47](#).

46

Port beaoning is enabled.

1. Consult the customer and next level of support to determine the reason port beaoning is enabled.

2. Disable port beaconing:
 - a. At the **View** panel, choose **Operations** option at the left side of the panel. The **Operations** panel opens with the **Port Beaconing** page displayed.
 - b. Click the **Beaconing State** check box for the port. The check mark disappears from the box and port beaconing is disabled.
 - c. Return to the **View** panel (**Port Properties** tab).

Continue.

47

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

NO **YES**

- ↓ Port segmentation is indicated. Go to [step 52](#) to obtain event codes. If no event codes are found, go to [MAP 0700: Fabric, ISL, and Segmented Port Problem Determination on page 2–99](#). **Exit MAP.**

48

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

NO **YES**

- ↓ Go to [step 52](#) to obtain event codes. If no event codes are found, go to [MAP 0600: UPM Card Failure and Link Incident Analysis on page 2–79](#). **Exit MAP.**

49

Repeat [step 45](#) through [step 48](#) for each remaining Fibre Channel port for which a problem is suspected.

Is a problem indicated for any of the ports?

NO **YES**

- ↓ Go to [step 52](#) to obtain event codes. If no event codes are found, go to [MAP 0600: UPM Card Failure and Link Incident Analysis on page 2–79](#). **Exit MAP.**

50

Inspect power supply operational states.

1. At the **View** panel, click the **FRU Properties** tab. The **View FRU Properties** panel displays, as shown in [Figure 2-7](#).

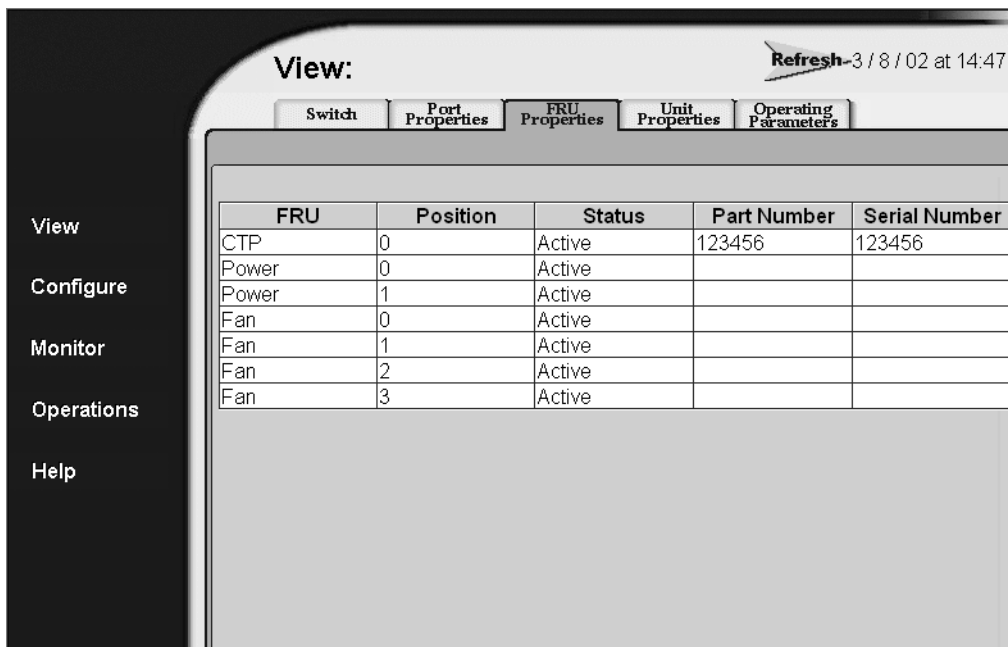


Figure 2-7: View FRU Properties panel

2. 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 52](#) to obtain event codes. If no event codes are found, go to [MAP 0100: Power Distribution Analysis on page 2-36](#). **Exit MAP.**

51

Inspect the **Status** fields for director FRUs, including CTP cards, SBAR assemblies, fan modules, and the backplane.

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

YES **NO**

↓ The director is 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 2–71](#). **Exit MAP.**

52

Obtain event codes from the Embedded Web Server event log.

NOTE: 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.

1. At the **View** panel, choose the **Monitor** option at the left side of the panel. The **Monitor** panel opens with the **Status** page displayed.
2. At the **Monitor** panel, click the **Log** tab. The **Monitor** panel displays, as shown in [Figure 2–8](#).
3. Record the event code, date, time, and severity (**Informational**, **Minor**, **Major**, or **Severe**).
4. Record all event codes that may relate to the reported problem.

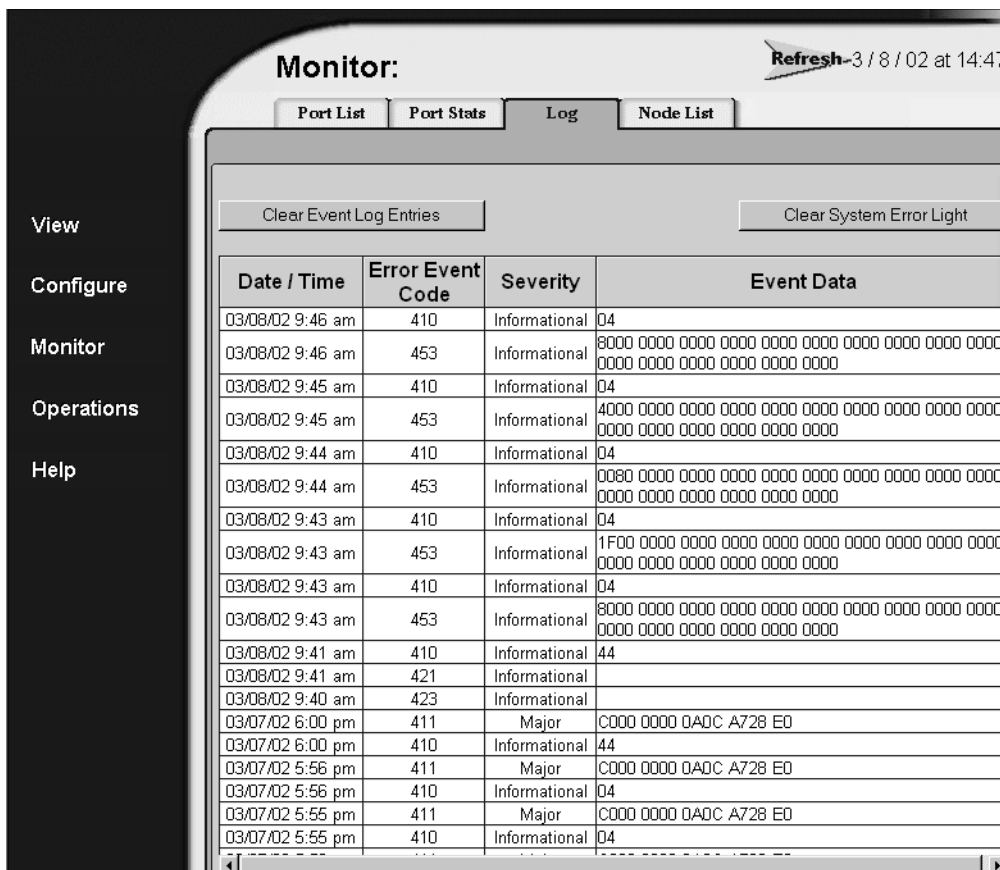


Figure 2–8: Monitor Log panel

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.

53

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

Was a link incident record generated and sent to the director-attached OSI or FICON server?

YES NO

↓ Perform director fault isolation at the HAFM server (or customer-supplied server).
Go to [step 3](#).

54

The link incident record provides the attached director 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 director fault isolation at the HAFM server (or customer-supplied server).
Go to [step 3](#).

Go to [Table 2-3 on page 2-2](#).

MAP 0100: Power Distribution Analysis

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

1

Was an event code **200**, **201**, **202**, or **208** observed at the Director 2/140 Event Log (HAFM server) or at the Embedded Web Server 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.

1. Ensure the AC power cord associated with the power supply (**PS0** or **PS1**) is connected to the rear of the director and a facility power receptacle. If not, connect the cord as directed by the customer.
2. Ensure the associated facility circuit breaker is on. If not, ask the customer to set the circuit breaker on.
3. 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.

1. Inspect the power supply and ensure the green **PWR OK** LED illuminates and all amber LEDs extinguish.
2. At the HAFM server's **Hardware View**, observe the graphic representing the power supply and ensure a failure symbol (blinking red and yellow diamond) does not display.

Is a failure indicated?

YES **NO**

↓ The director is operational. **Exit MAP.**

5

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

Was a corrective action performed?

YES **NO**

↓ Go to [step 7](#).

6

Verify redundant power supply operation.

1. Inspect the power supply and ensure the green **PWR OK** LED illuminates and all amber LEDs extinguish.
2. At the HAFM server's **Hardware View**, observe the graphic representing the power supply and ensure a failure symbol (blinking red and yellow diamond) does not display.

Is a failure indicated?

YES NO

↓ The director is operational. **Exit MAP.**

7

A redundant power supply failed and must be removed and replaced ([RRP: Redundant Power Supply on page 4–19](#)).

- This procedure is concurrent and can be performed while director 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 director is 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 100 and 240 VAC, and between 2 and 4 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 director operation:

1. Inspect the director front bezel and ensure the green power LED illuminates. Inspect the active CTP card and ensure the green LED illuminates.
2. Inspect both power supplies. Ensure both green **PWR OK** LEDs illuminate and all amber LEDs extinguish.
3. At the HAFM server's **Hardware View**, observe all graphics representing FRUs and power supplies, and ensure emulated green LEDs illuminate.

Is a failure indicated?

YES **NO**

↓ The director is operational. **Exit MAP.**

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

10

Is fault isolation being performed at the director?

YES **NO**

↓ Fault isolation is being performed at the HAFM server or Embedded Web Server interface. Go to [step 21](#).

11

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

1. Ensure AC power cords (**PS0** and **PS1**) are connected to the rear of the director and to facility power receptacles. If not, connect the cords as directed by the customer.
2. Ensure associated facility circuit breakers are on. If not, ask the customer set the circuit breakers on.
3. Ensure the AC power cords are not damaged. If damaged, replace the cords.
4. Ensure the power switch (circuit breaker) at the rear of the director is set to the **ON** (up) position.

Continue.

12

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

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- An illuminated green LED on the active CTP card.
- At least one green **PWR OK** LED illuminated on a power supply.
- Audio emanations and airflow from cooling fans.

Is the director powered on?

YES **NO**

↓ Go to [step 14](#).

13

Does inspection of a power supply indicate a failure (green **PWR OK** LED extinguished and one or more amber LEDs illuminated)?

NO **YES**

↓ A redundant power supply failed. Go to [step 7](#).

The director is operational. **Exit MAP.**

14

The director's AC power distribution system failed. Possible causes include failure of:

- Both power supplies.
- Power module assembly.
- Backplane.

Does inspection of both power supplies indicate a dual failure (both green **PWR OK** LEDs extinguished and one or more amber LEDs illuminated on each power supply)?

YES **NO**

↓ One or both power supplies are operational, but a power distribution failure through the backplane is indicated. Go to [step 19](#).

15

Ensure both power supplies are correctly installed and seated in the director. 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 the green **PWR OK** LEDs illuminate and all amber LEDs extinguish.
- b. At the HAFM server's **Hardware View**, observe the graphics representing the power supplies and ensure failure symbols (blinking red and yellow diamonds) do not display.

Is a dual power supply failure still indicated?

YES **NO**

↓ The director is operational. **Exit MAP.**

17

Both power supplies failed and must be removed and replaced ([RRP: Redundant Power Supply on page 4–19](#)). Perform the data collection procedure as part of FRU removal and replacement.

Did dual power supply replacement solve the problem?

NO **YES**

↓ The director is 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

A power module assembly failure is indicated and must be removed and replaced ([RRP: Power Module Assembly on page 4–30](#)). This procedure is non concurrent and must be performed while director power is off.

Did power module assembly replacement solve the problem?

NO **YES**

↓ The director is operational. **Exit MAP.**

A power module assembly failure is not confirmed. Replace the original power module assembly to avoid the cost of expending a replacement FRU. Continue.

19

One or both power supplies are 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 backplane failed.

Power cycle the director to reset all logic cards ([Power-On Procedure on page 3–43](#)).

Did power cycling the director solve the problem?

NO **YES**

↓ The director is operational. **Exit MAP.**

20

The backplane failed and must be removed and replaced ([RRP: Backplane on page 4–32](#)).

- This procedure is nonconcurrent and must be performed while director power is off.
- Perform the data collection procedure as part of FRU removal and replacement.

Did backplane replacement solve the problem?

NO **YES**

↓ The director is operational. **Exit MAP.**

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

21

Is fault isolation being performed at the HAFM server?

YES **NO**

↓ Fault isolation is being performed at the Embedded Web Server interface. Go to [step 25](#).

22

At the HAFM server's **Hardware View**, does a yellow triangle display at the alert panel and a blinking red and yellow diamond (failed FRU indicator) display over a power supply graphic?

NO **YES**

↓ A redundant power supply failed. Go to [step 7](#).

23

At the HAFM server's **Hardware View**, does a grey square display at the alert panel, a **No Link** status displays at the director Status table, and graphical FRUs are uninstalled?

YES **NO**

↓ A green circle displays at the alert panel and the director is operational. **Exit MAP.**

The grey square indicates the HAFM server cannot communicate with the director because:

- The director-to-HAFM server Ethernet link failed.
- AC power distribution in the director failed, or AC power was disconnected.
- Both of the director's CTP cards failed.

Continue.

24

Ensure the director reporting the problem is connected to facility AC power and the power switch (circuit breaker) at the rear of the director is set to the **ON** (up) position. Inspect the director for indications of being powered on, such as:

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- An illuminated green LED on the active CTP card.
- At least one green **PWR OK** LED illuminated on a power supply.
- Audio emanations and airflow from cooling fans.

Is the director powered on?

YES **NO**

↓ Go to [step 14](#).

Analysis for an Ethernet link or dual CTP card failure is not described in this MAP. Go to [MAP 0000: Start MAP on page 2–12](#). If this is the second time at this step, contact the next level of support. **Exit MAP.**

25

Is the Embedded Web Server interface operational?

NO **YES**

↓ Go to [step 28](#).

26

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

- The director-to-PC Internet link could not be established.
- AC power distribution in the director failed, or AC power was disconnected.
- Both of the director's CTP cards failed.

Continue.

27

Ensure the director reporting the problem is connected to facility AC power and the power switch (circuit breaker) at the rear of the director is set to the **ON** (up) position. Inspect the director for indications of being powered on, such as:

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- An illuminated green LED on the active CTP card.
- At least one green **PWR OK** LED illuminated on a power supply.
- Audio emanations and airflow from cooling fans.

Is the director powered on?

YES **NO**

↓ Go to [step 14](#).

Analysis for an Ethernet link or dual CTP card failure is not described in this MAP. Go to [MAP 0000: Start MAP on page 2–12](#). If this is the second time at this step, contact the next level of support. **Exit MAP.**

28

Inspect power supply operational states at the Embedded Web Server 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 director is operational. **Exit MAP.**

MAP 0200: POST Failure Analysis

When the director is powered on, it performs a series of power-on self-tests (POSTs). When POSTs complete, the director 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 director and bring it online. An event code **400** is displayed when the director completes the POST/IPL process.

1

Ensure the director reporting the problem is connected to facility AC power and the power switch (circuit breaker) at the rear of the director is set to the **ON** (up) position. Inspect the director for indications of being powered on, such as:

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- An illuminated green LED on the active CTP card.
- At least one green **PWR OK** LED illuminated on a power supply.
- Audio emanations and airflow from cooling fans.

Is the director 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 2–36](#). **Exit MAP.**

2

Was an event code **400**, or **411**, or **413** observed at the director Event Log (HAFM server) or at the Embedded Web Server event log?

YES **NO**

- ↓ Analysis for the failure is not described in this MAP. Go to [MAP 0000: Start MAP on page 2–12](#). **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 11 .
413	Backup CTP card POST failure.	Go to step 12 .

4

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

1. At the HAFM server's **Hardware View**, click **Logs** and choose **Event Log**. The **Event Log** displays.
2. Examine the first two bytes (**0** and **1**) of event data.
3. 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, **00** or **01** for redundant FRUs, and **00** through **35** for UPM cards, and slot **32** is for internal use only).

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

Table 2–6: Byte 0 FRU Codes

Byte 0	Failed FRU	Action
01	Backplane.	Go to step 5 .
02	CTP card.	Go to step 6 .
03	SBAR assembly.	Go to step 7 .
05	Fan module.	Go to step 8 .
06	Power supply.	Go to step 9 .
08-22	UPM card.	Go to step 10 .

5

The backplane failed POSTs (indicated by a **01** FRU code) and must be removed and replaced ([RRP: Backplane on page 4–32](#)).

- This procedure is nonconcurrent and must be performed while director power is off.
- Perform the data collection procedure as part of FRU removal and replacement.

Did backplane replacement solve the problem?

NO **YES**

↓ The director is operational. **Exit MAP.**

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

6

A CTP card failed POSTs (indicated by a **02** FRU code) and must be removed and replaced ([RRP: Redundant CTP Card on page 4–5](#)).

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

Did CTP card replacement solve the problem?

NO **YES**

↓ The director is operational. **Exit MAP.**

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

7

An SBAR assembly failed POSTs (indicated by a **03** FRU code) and must be removed and replaced ([RRP: Redundant SBAR Assembly on page 4–24](#)).

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

Did SBAR assembly replacement solve the problem?

NO **YES**

↓ The director is operational. **Exit MAP.**

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

8

A fan module failed POSTs (indicated by a **05** FRU code) and must be removed and replaced ([RRP: Redundant Fan Module on page 4–27](#)).

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

Did fan module replacement solve the problem?

NO YES

↓ The director is operational. **Exit MAP.**

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

9

A power supply failed POSTs (indicated by a **06** FRU code) and must be removed and replaced ([RRP: Redundant Power Supply on page 4–19](#)).

- This procedure is concurrent and can be performed while director 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 director is operational. **Exit MAP.**

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

10

A UPM card failed POSTs (indicated by a **08** through **22** FRU code) and must be removed and replaced ([RRP: UPM Card on page 4–9](#)).

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

Did UPM card replacement solve the problem?

NO YES

↓ The director is operational. **Exit MAP.**

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

11

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 information to HP for analysis by third-level support personnel. **Exit MAP.**

12

The backup CTP card failed POST/IPL diagnostics (as indicated by an event code **413**) and must be removed and replaced ([RRP: Redundant CTP Card on page 4–5](#)).

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

Did CTP card replacement solve the problem?

NO **YES**

↓ The director is operational. **Exit MAP.**

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

MAP 0300: Console Application Problem Determination

This map describes isolation of HAFM server problems, including problems associated with the Windows 2000 operating system, and HAFM and *Product Manager* applications.

1

Did the HAFM 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.

1. Simultaneously press **Ctrl + Alt + Delete**. The **Windows 2000 Security** dialog box displays.
2. At the **Windows 2000 Security** dialog box, click **Task Manager**. The **Windows 2000 Task Manager** dialog box ([Figure 2-9](#)) displays with the **Applications** page open.



Figure 2–9: Task Manager dialog box, Applications tab

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

Continue.

3

Attempt to clear the problem by rebooting the HAFM server PC.

1. Choose **Start > Shut Down**. The **Shut Down Windows** dialog box displays.
2. At the **Shut Down Windows** dialog box, select **Shut Down The Computer** and click **Yes** to power off the PC.

3. Wait approximately 30 seconds and power on the PC. After POSTs complete, the **Begin Logon** dialog box displays.
4. Simultaneously press **Ctrl + Alt + Delete** to display the **Logon Information** dialog box. Type a user name and password (obtained in [MAP 0000: Start MAP on page 2-12](#)) and click **OK**. The *HAFM* application starts and the **HAFM Login** dialog box ([Figure 2-10](#)) displays.



Figure 2-10: HAFM Login dialog box

5. At the **HAFM Login** dialog box, type a user name, password, and HAFM server name (obtained in [MAP 0000: Start MAP on page 2-12](#), and all are case sensitive), and click **Login**. The application opens and the **Products View** displays.

Did the **Products View** display and is the *HAFM* application operational?

NO **YES**

↓ The problem is transient and the HAFM server is 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 application 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 dialog box and close the *HAFM* application. Go to [step 3](#).

5

Did the *HAFM* application display a dialog box 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 3-62](#)).

Did the software upgrade solve the problem?

NO **YES**

↓ The HAFM server is operational. **Exit MAP.**

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

8

Did the *Product Manager* application display a dialog box 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 dialog box, and close the *HAFM* and *Product Manager* applications. Go to [step 3](#).

9

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

YES **NO**

↓ Go to [step 11](#).

10

An attempt to download a firmware version from the HAFM server hard drive to the director failed. Retry the operation ([Manage Firmware Versions on page 3–51](#)).

Did the firmware version download to the director?

NO **YES**

↓ The HAFM server is operational. **Exit MAP.**

A CTP card failure is suspected. Go to [MAP 0000: Start MAP on page 2–12](#) to isolate the problem. **Exit MAP.**

11

Did the *Product Manager* application display a dialog box 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 3–40](#)).

Did the data collection process complete?

NO **YES**

↓ Return the Zip disk to HP for analysis by third-level support. **Exit MAP.**

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

13

Did the HAFM server lock up or crash and display a **Dr. Watson for Windows 2000** dialog box?

NO **YES**

↓ A Windows 2000 operating system or *HAFM* application error occurred. Click **Cancel** to close the dialog box and *HAFM* application. Go to [step 3](#).

14

Did the HAFM server crash and display a blue screen with the system dump file in hexadecimal format (“blue screen of death”)?

YES **NO**

↓ The HAFM server is operational. **Exit MAP.**

15

Attempt to clear the problem by power cycling the HAFM server PC.

1. Power off the PC.
2. Wait approximately 30 seconds and power on the PC. After POSTs complete, the **Begin Logon** dialog box displays.
3. Simultaneously press **Ctrl + Alt + Delete** to display the **Logon Information** dialog box. Type a user name and password (obtained in [MAP 0000: Start MAP on page 2–12](#)) and click **OK**. The *HAFM* application starts and the **HAFM Login** dialog box displays.

4. At the **HAFM Login** dialog box, type a user name, password, and HAFM server name (obtained in [MAP 0000: Start MAP on page 2–12](#), and all are case sensitive), and click **Login**. The application opens and the **Products View** displays.

Did the **Products View** display and is the *HAFM* application operational?

NO **YES**

↓ The problem is transient and the HAFM server is 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 director and the HAFM server, or between a director and a web browser PC running the Embedded Web Server interface. Failure indicators include:

- At the **Products View**, a grey square at the alert panel and as the background to the icon representing the director reporting the problem.
- At the **Hardware View**, a grey square at the alert panel, a No Link status and reason at the director Status table, and no FRUs visible for the director.
- 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 director Event Log or Embedded Web Server event log.

When the logical connection between the director and HAFM server is initiated, it may take up to five minutes for the link to activate at the **Products View**, and a green circle displays at the alert panel and the background to the icon representing the director. This delay is normal.



CAUTION: Prior to servicing a director or HAFM server, determine the Ethernet LAN configuration. Installation of directors and the HAFM 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 director Event Log (HAFM server) or at the Embedded Web Server 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?

YES **NO**

- ↓ Fault isolation is being performed through the Embedded Web Server interface. Go to [step 25](#).

4

At the HAFM server's **Products View**, does a grey square display at the alert panel and as the background to the icon representing the director reporting the problem?

YES **NO**

- ↓ The director-to-HAFM server connection is restored and is operational. **Exit MAP.**

The grey square indicates the HAFM server cannot communicate with the director because:

- The director-to-HAFM server Ethernet link failed.
- AC power distribution in the director failed, or AC power was disconnected.
- Both of the director's CTP cards failed.

Continue.

5

Ensure the director reporting the problem is connected to facility AC power and the power switch (circuit breaker) at the rear of the director is set to the **ON** (up) position. Inspect the director for indications of being powered on, such as:

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- An illuminated green LED on the active CTP card, and illuminated green **PWR OK** LEDs on both power supplies.
- Audio emanations and airflow from cooling fans.

Is the director powered on?

YES **NO**

- ↓ A power distribution problem is indicated. Go to [MAP 0100: Power Distribution Analysis on page 2–36](#). **Exit MAP.**
-

6

At the director, inspect the amber LED at the top of each CTP card.

Is the amber LED illuminated on both CTP cards?

NO **YES**

- ↓ Failure of both CTP cards is indicated. Go to [MAP 0500: FRU Failure Analysis on page 2–71](#). **Exit MAP.**
-

7

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

- A grey square displays at the alert panel.
- No FRUs are visible for the director.
- The Director 2/140 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 and Actions

Error Message	Action
Never connected.	Go to step 8 .
Link timeout.	Go to step 8 .
Protocol mismatch.	Go to step 15 .
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 director's Ethernet adapter (on each CTP card) exceeded a threshold, the director-to-HAFM server link was not connected, or the director-to-HAFM server link timed out. A problem with the Ethernet cable, Ethernet hub or hubs, or other LAN-attached device is indicated.

Verify the director is connected to the HAFM server through one or more Ethernet hubs.

1. Ensure an RJ-45 Ethernet cable connects both of the director's CTP cards to an Ethernet hub. If not, connect the cables as directed by the customer.
2. 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.
3. 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

If appropriate, verify that the hubs are correctly daisy-chained.

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 director-to-HAFM server connection is restored and is 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 director or HAFM server, go to [MAP 0000: Start MAP on page 2–12](#) 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 director-to-HAFM server connection is restored and is operational. **Exit MAP.**

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

14

The Ethernet adapter on the director's active CTP card reset in response to an error. The connection to the HAFM server terminated briefly, then recovered upon reset.

Perform the data collection procedure and return the Zip disk to HP for analysis by third-level support personnel. **Exit MAP.**

15

A protocol mismatch occurred because the *HAFM* application (running on the HAFM server) and the director 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 3–62](#)).

Did the director-to-HAFM server Ethernet connection recover?

NO **YES**

- ↓ The director-to-HAFM server connection is restored and is operational. **Exit MAP.**

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

17

A director firmware upgrade is required ([Download a Firmware Version to a Director on page 3–56](#)). Perform the data collection procedure after the download.

Did the director-to-HAFM server Ethernet connection recover?

NO **YES**

↓ The director-to-HAFM server connection is restored and is operational. **Exit MAP.**

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

18

An instance of the *HAFM* application is open at another HAFM server and communicating with the director (duplicate session). Notify the customer and either:

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

Does the customer want the second HAFM server configured as a client?

YES **NO**

↓ Power off the HAFM server reporting the **Duplicate Session** communication problem. **Exit MAP.**

19

Determine the internet protocol (IP) address of the HAFM server running the first instance of the *HAFM* application.

1. Choose **Start > Settings > Control Panel**. The **Control Panel** window displays.
2. At the **Control Panel** window, double-click the **Network** icon. The **Network** dialog box displays with the **Identification** page open.
3. Click **Protocols**. The **Protocols** page opens.
4. Choose the **TCP/IP Protocol** entry from the list box and click **Properties**. The **Microsoft TCP/IP Properties** dialog box displays with the **IP Address** page open.

5. Record the IP address, then click **OK** to close the dialog box. At the **Network** dialog box, click **OK** to close the dialog box.
6. Close the **Control Panel** window.

Continue.

20

Configure the HAFM server reporting the **Duplicate Session** communication problem as a client.

1. At the **Products View**, click **Logout/Exit** and choose **Logout**. The **HAFM Login** dialog box displays.
2. At the **HAFM Login** dialog box, type a user name and password (obtained in [MAP 0000: Start MAP on page 2–12](#), and both are case sensitive).
3. Type the IP address of the HAFM server running the first instance of the *HAFM* application in the **HAFM Server** field.
4. Click **Login**. The *HAFM* application opens as a client and the **Products View** displays.

Did the HAFM server reconfigure as a client and did the Ethernet connection recover?

NO **YES**

- ↓ The director-to-HAFM server connection is restored and the second HAFM server is operational as a client.
Exit MAP.

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

21

The IP address defining the director 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 director's IP address. The tools are provided with the director or by service personnel. To verify the IP address:

1. Remove the protective cap from the 9-pin maintenance port at the rear of the director (a phillips-tip screwdriver may be required). Connect one end of the RS-232 null modem cable to the port.
2. Connect the other cable end to a 9-pin communication port (**COM1** or **COM2**) at the rear of the maintenance terminal PC.

3. Power on the maintenance terminal. After the PC powers on, the Windows desktop displays.
4. Choose **Start > Programs > Accessories > HyperTerminal**. The **Connection Description** dialog box displays.
NOTE: The following steps describe inspecting the IP address using *HyperTerminal* serial communication software.
5. Type 64 in the **Name** field and click **OK**. The **Connect To** dialog box displays.
6. Ensure the **Connect using** field displays **COM1** or **COM2** (depending on the serial communication port connection to the director), and click **OK**. The **COMn Properties** dialog box displays (where n is **1** or **2**).
7. Configure the **Port Settings** parameters as follows:
 - Bits per second-**57600**.
 - Data bits-**8**.
 - Parity-**None**.
 - Stop bits-**1**.
 - Flow control-**Hardware**.

When the parameters are set, click **OK**. The **Director 2/140 HyperTerminal** window displays.

8. At the > prompt, type the user-level password (the default is **password**) and click **Enter**. The password is case sensitive. The **Director 2/140 HyperTerminal** window displays with an **C>** prompt at the bottom of the window.
9. At the **C>** prompt, type the **ipconfig** command and click **Enter**. The **Director 2/140 HyperTerminal** window displays with configuration information listed (including the IP address).
10. Record the director's IP address.
11. Choose **Exit** from the **File** menu to close the *HyperTerminal* application.
12. Power off the maintenance terminal.
13. Disconnect the RS-232 null modem cable from the director and the maintenance terminal. Replace the protective cap over the maintenance port.

Continue.

22

Define the director's correct IP address to the HAFM server.

1. At the **Products View**, right-click the icon with the grey square representing the director reporting the problem. A menu displays.
2. Choose **Modify**. The **Modify Network Address** dialog box (Figure 2–11) displays.

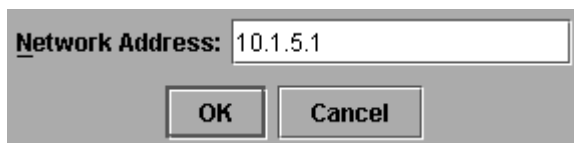


Figure 2–11: Modify Network Address dialog box

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

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

NO **YES**

- ↓ The director-to-HAFM server connection is restored and is operational. **Exit MAP.**

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

23

An incorrect product type is defined to the HAFM server.

1. At the **Products View**, right-click the icon with the grey square representing the product reporting the problem. A menu displays.
2. Choose **Delete**. A **Warning** dialog box displays asking if the product is to be deleted.
3. Click **Yes** to delete the product.
4. At the **Products View**, click **Configure** and choose **New Product**. The **New Product** dialog box (Figure 2–12) displays.

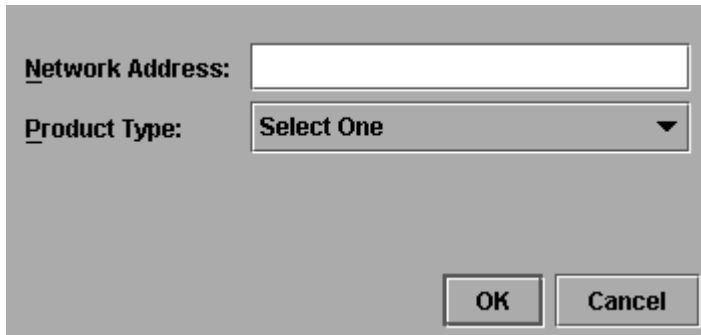


Figure 2–12: New Product dialog box

5. Type the configured IP address in the **Network Address** field.
6. Choose **Director 2/140** from the **Product Type** list box and click **OK**.

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

NO **YES**

- ↓ The director-to-HAFM server connection is restored and is operational. **Exit MAP.**

24

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

1. At the **Products View**, right-click the icon with the grey square representing the product reporting the problem. A menu displays.
2. Choose **Delete**. A **Warning** dialog box displays asking if the product is to be deleted.
3. Click **Yes** to delete the product.

Exit MAP.

25

Is the Embedded Web Server interface operational?

NO **YES**

-
- ↓ The director-to-web server PC connection is restored and is operational. **Exit MAP.**

26

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

- The director-to-PC Internet (Ethernet) link could not be established.
- AC power distribution in the director failed, or AC power was disconnected.
- Both of the director's CTP cards failed.

Continue.

27

Ensure the director reporting the problem is connected to facility AC power and the power switch (circuit breaker) at the rear of the director is set to the **ON** (up) position. Inspect the director for indications of being powered on, such as:

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- An illuminated green LED on the active CTP card, and illuminated green **PWR OK** LEDs on both power supplies.
- Audio emanations and airflow from cooling fans.

Is the director powered on?

YES **NO**

- ↓ A power distribution problem is indicated. Go to [MAP 0100: Power Distribution Analysis on page 2-36](#). **Exit MAP.**

28

At the director, inspect the amber LED at the top of each CTP card.

Is the amber LED illuminated on both CTP cards?

NO **YES**

- ↓ Failure of both CTP cards is indicated. Go to [MAP 0500: FRU Failure Analysis on page 2-71](#). **Exit MAP.**

29

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

1. Wait approximately five minutes, then attempt to login to the director again.
2. 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 director (obtained in [MAP 0000: Start MAP on page 2–12](#)). The **Username And Password Required** dialog box displays.
3. Type the user name and password obtained in [MAP 0000: Start MAP on page 2–12](#) and click **OK**. If the **View** panel does not display, wait five minutes and perform this step again.

Is the Embedded Web Server interface operational with the **View** panel displayed?

NO **YES**

- ↓ The director-to-web server PC connection is restored and is operational. **Exit MAP.**

Failure of the CTP card's Ethernet port is indicated. Go to [MAP 0500: FRU Failure Analysis on page 2–71](#). **Exit MAP.**

MAP 0500: FRU Failure Analysis

This MAP describes fault isolation for the CTP card, SBAR assembly, and fan module. Failure indicators include:

- The amber LED on the FRU illuminates.
- The amber emulated LED on a fan graphic at the **Hardware View** illuminates.
- A blinking red and yellow diamond (failed FRU indicator) displays over a FRU graphic; or a grey square (status unknown indicator) or yellow triangle (attention indicator) displays at the alert panel of the **Products View** or **Hardware View**.
- An event code recorded at the director Event Log or the Embedded Web Server event log.
- A **Failed** message associated with a FRU at the Embedded Web Server interface.

1

Was an event code **300, 301, 302, 303, 304, 305, 414, 420, 433, 440, 604, 605, 607, 805, 806, 807, 810, 811, 812,** or **850** observed at the director Event Log (HAFM server) or at the Embedded Web Server 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 .
414	Backup CTP card failed.	Go to step 7 .

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

Event Code	Explanation	Action
420	Backup CTP card NV-RAM failure.	Go to step 7 .
433	Non-recoverable Ethernet fault.	Go to step 7 .
440	Embedded port hardware failed.	Go to step 7 .
604	SBAR assembly failure.	Go to step 9 .
605	SBAR assembly revision not supported.	Go to step 16 .
607	Director contains no operational SBAR assemblies.	Go to step 9 .
620	SBAR fan failure.	Go to step 5 .
805	High temperature warning (SBAR assembly thermal sensor).	Go to step 9 .
806	Critically hot temperature warning (SBAR assembly thermal sensor).	Go to step 9 .
807	SBAR assembly shutdown due to thermal violation.	Go to step 9 .
810	High temperature warning (CTP card thermal sensor).	Go to step 7 .
811	Critically hot temperature warning (CTP card thermal sensor).	Go to step 7 .
812	CTP card shutdown due to thermal violation.	Go to step 7 .
850	System shutdown due to CTP card thermal violations.	Go to step 7 .

3

Is fault isolation being performed at the director?

YES **NO**

- ↓ Fault isolation is being performed at the HAFM server or Embedded Web Server interface. Go to [step 10](#).

4

Inspect both fan modules at the rear of the director. Fan module LEDs can be inspected through the hexagonal cooling vents of the radio frequency interference (RFI) shield.

Does inspection of a director fan module indicate a failure? Indicators include:

- The amber LED is illuminated but not blinking (beaconing) on one or both fan modules.
- 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 fan modules must be removed and replaced ([RRP: Redundant Fan Module on page 4–27](#)).

- If one or more fans in a module are operating, do not remove the fan module unless the replacement is immediately available.
- If a multiple fan failure caused a thermal shutdown, power on the director after the fan modules are replaced ([Power-On Procedure on page 3–43](#)).

Are the fan modules functioning?

NO **YES**

↓ The director is operational. **Exit MAP.**

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

6

Inspect the faceplates of both CTP cards at the front of the director.

Is the amber LED at the top of a CTP card illuminated but not blinking (beaconing)?

YES **NO**

↓ Go to [step 8](#).

7

A CTP card failed and must be removed and replaced ([RRP: Redundant CTP Card on page 4-5](#)).

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

Did CTP card replacement solve the problem?

NO **YES**

↓ The director is operational. **Exit MAP.**

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

8

Inspect both SBAR assemblies at the rear of the director. SBAR assembly LEDs can be inspected through the hexagonal cooling vents of the RFI shield.

Is the amber LED on an SBAR assembly illuminated but not blinking (beaconing)?

YES **NO**

↓ The director is operational. **Exit MAP.**

9

An SBAR assembly failed and must be removed and replaced ([RRP: Redundant SBAR Assembly on page 4-24](#)).

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

Did SBAR assembly replacement solve the problem?

NO **YES**

↓ The director is operational. **Exit MAP.**

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

10

Is fault isolation being performed at the HAFM server?

YES **NO**

↓ Fault isolation is being performed at the Embedded Web Server interface. Go to [step 18](#).

11

Is a blinking red and yellow diamond (failed FRU indicator) overlaying a fan module graphic at the **Hardware View**?

NO **YES**

↓ A fan module failure is indicated. Go to [step 5](#).

12

Is a blinking red and yellow diamond (failed FRU indicator) overlaying a CTP card graphic at the **Hardware View**?

NO **YES**

↓ A CTP card failure is indicated. Go to [step 7](#).

13

Is a blinking red and yellow diamond (failed FRU indicator) overlaying an SBAR assembly graphic at the **Hardware View**?

NO **YES**

↓ An SBAR assembly failure is indicated. Go to [step 9](#).

14

At the **Hardware View**, is a grey square displayed at the alert panel, a No Link status displays at the **Director 2/140 Status** table and graphical FRUs are uninstalled?

YES **NO**

↓ A green circle displays at the alert panel and the director is operational. **Exit MAP.**

The grey square indicates the HAFM server cannot communicate with the director because:

- The director-to-HAFM server Ethernet link failed.
- AC power distribution in the director failed, or AC power was disconnected.
- Both of the director's CTP cards failed.

Continue.

15

At the director, inspect the amber LED at the top of each CTP card.

Is the amber LED illuminated on both CTP cards?

NO **YES**

↓ Failure of both CTP cards is indicated. Go to [step 7](#).

Analysis for an Ethernet link or AC power distribution failure is not described in this MAP. Go to [MAP 0000: Start MAP on page 2–12](#). If this is the second time at this step, contact the next level of support. **Exit MAP.**

16

An SBAR assembly is not recognized by director firmware because the firmware version is not supported or the SBAR assembly failed. Advise the customer of the problem and determine the correct firmware version to download from the HAFM server.

Download the firmware ([Download a Firmware Version to a Director on page 3–56](#)). Perform the data collection procedure after the download.

Continue.

17

Did the firmware download solve the problem?

NO **YES**

↓ The director is operational. **Exit MAP.**

An SBAR assembly failure is indicated. Go to [step 9](#).

18

Is the Embedded Web Server interface operational?

NO **YES**

↓ Go to [step 22](#).

19

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

- The director-to-PC Internet link could not be established.
- AC power distribution in the director failed, or AC power was disconnected.
- Both of the director's CTP cards failed.

Continue.

20

Ensure the director reporting the problem is connected to facility AC power and the power switch (circuit breaker) at the rear of the director is set to the **ON** (up) position. Inspect the director for indications of being powered on, such as:

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- An illuminated green LED on the active CTP card.
- At least one green **PWR OK** LED illuminated on a power supply.
- Audio emanations and airflow from cooling fans.

Is the director 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 2-12](#). If this is the second time at this step, contact the next level of support. **Exit MAP.**

21

At the director, inspect the amber LED at the top of each CTP card.

Is the amber LED illuminated on both CTP cards?

NO **YES**

↓ Failure of both CTP cards is indicated. Go to [step 7](#).

Analysis for an Ethernet link failure is not described in this MAP. Go to [MAP 0000: Start MAP on page 2–12](#). If this is the second time at this step, contact the next level of support. **Exit MAP.**

22

Inspect fan module operational states at the Embedded Web Server interface.

1. At the **View** panel, click the **FRU Properties** tab. The **View** panel (**FRU Properties** tab) displays.
2. Inspect the **Status** fields for both fan modules.

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

NO **YES**

↓ A fan module failure is indicated. Go to [step 5](#).

23

Inspect CTP card operational states at the Embedded Web Server interface. Inspect the **Status** fields for both CTP cards.

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

NO **YES**

↓ A CTP card failure is indicated. Go to [step 7](#).

24

Inspect SBAR assembly operational states at the Embedded Web Server interface. Inspect the **Status** fields for both assemblies.

Does the **Status** field display a **Failed** message for either SBAR assembly?

NO **YES**

↓ An SBAR assembly failure is indicated. Go to [step 9](#).

The director is operational. **Exit MAP.**

MAP 0600: UPM Card Failure and Link Incident Analysis

This MAP describes fault isolation for UPM cards, 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 UPM card illuminate.
- One or more emulated amber LEDs on a UPM card graphic at the **Hardware View** illuminate.
- A blinking red and yellow diamond (failed FRU indicator) displays over a UPM card graphic or a yellow triangle (attention indicator) displays at the alert panel of the **Products View**, **Hardware View**, or **Port Card View**.
- An event code recorded at the **Director 2/140 Event Log** or the Embedded Web Server event log.
- A port operational state message or a **Failed** message associated with a UPM card at the Embedded Web Server interface.
- A link incident message recorded in the **Link Incident Log** or **Port Properties** dialog box.

1

Was an event code **080**, **504**, **505**, **506**, **507**, **512**, **514**, **800**, **801**, or **802** observed at the director Event Log (HAFM server) or at the Embedded Web Server event log?

YES **NO**

↓ Go to [step 3](#).

2

Was an event code **581**, **582**, **583**, **584**, **585**, or **586** observed at the console of an OSI or FICON server attached to the director 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 world-wide name.	Go to step 23.
081	Invalid attachment.	Go to step 18.
504	UPM card failure.	Go to step 7.
505	UPM card revision not supported.	Go to step 36.
506	Fibre Channel port failure.	Go to step 7.
507	Loopback diagnostics port failure.	Go to step 14.
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 29.
582	Bit error threshold exceeded.	Go to step 29.
583	Loss of signal or loss of synchronization.	Go to step 29.
584	Not operational primitive sequence received.	Go to step 29.
585	Primitive sequence timeout.	Go to step 29.
586	Invalid primitive sequence received for current link state.	Go to step 29.
800	High temperature warning (UPM card thermal sensor).	Go to step 7.
801	Critically hot temperature warning (UPM card thermal sensor).	Go to step 7.
802	UPM card shutdown due to thermal violation.	Go to step 7.

4

Is fault isolation being performed at the director?

YES NO

-
- ↓ Fault isolation is being performed at the HAFM server or Embedded Web Server interface. Go to [step 8](#).

5

Inspect the faceplates of UPM cards at the front of the director. Each card has an amber LED (at the top of the card) that illuminates if the card fails or if any Fibre Channel port fails.

Each card also has a bank of amber and green LEDs above the ports. Each LED pair is associated with a corresponding port (for example, the top LED pair is associated with the top port). The amber LED illuminates and the green LED extinguishes if the port fails.

Are an amber port LED and the amber LED at the top of the UPM card illuminated but not blinking (beaconing)?

YES NO

- ↓ The director is operational, however a link incident or other problem may have occurred. Perform fault isolation at the HAFM server. Go to [step 8](#).

6

A Fibre Channel port failed, and the SFP optical transceiver must be removed and replaced ([RRP: SFP Optical Transceiver on page 4–14](#)).

- This procedure is concurrent and can be performed while director power is on.
- Verify location of the failed port. [Figure 2–13](#) and [Figure 2–14](#) show the UPM card numbers (**0** through **35**, slot **32** is for internal use only.), port numbers (**00** through **143**, ports **128 - 131** are for internal use only.), and bolded logical port addresses.

UPM Cards								CTP - 1 Card	CTP - 0 Card	UPM Cards							
31	30	29	28	27	26	25	24			23	22	21	20	19	18	17	16
127 7F	123 7B	119 77	115 73	111 6F	107 6B	103 67	99 63			95 5F	91 5B	87 57	83 53	79 4F	75 4B	71 47	67 43
83	7F	7B	77	73	6F	6B	67			63	5F	5B	57	53	4F	4B	47
126 7E	122 7A	118 76	114 72	110 6E	106 6A	102 66	98 62			94 5E	90 5A	86 56	82 52	78 4E	74 4A	70 46	66 42
82	7E	7A	72	6E	6A	66	66			62	5E	5A	56	52	4E	4A	46
125 7D	121 79	117 75	113 71	109 6D	105 69	101 65	97 61			93 5D	89 59	85 55	81 51	77 4D	73 49	69 45	65 41
81	7D	79	75	71	6D	69	65			61	5D	59	55	51	4D	49	45
124 7C	120 78	116 74	112 70	108 6C	104 68	100 64	96 60			92 5C	88 58	84 54	80 50	76 4C	72 48	68 44	64 40
80	7C	78	74	70	6C	68	64			60	5C	58	54	50	4C	48	44
60 3C	56 38	52 34	48 30	44 2C	40 28	36 24	32 20	28 1C	24 18	20 14	16 10	12 0C	08 08	04 04	00 00		
40	3C	38	34	30	2C	28	24	20	1C	18	14	10	0C	08	04		
61 3D	57 39	53 35	49 31	45 2D	41 29	37 25	33 21	29 1D	25 19	21 15	17 11	13 0D	09 09	05 05	01 01		
41	3D	39	35	31	2D	29	25	21	1D	19	15	11	0D	09	05		
62 3E	58 3A	54 36	50 32	46 2E	42 2A	38 26	34 22	30 1E	26 1A	22 16	18 12	14 0E	10 0A	06 06	02 02		
42	3E	3A	36	32	2E	2A	26	22	1E	1A	16	12	0E	0A	06		
63 3F	59 3B	55 37	51 33	47 2F	43 2B	39 27	35 23	31 1F	27 1B	23 17	19 13	15 0F	11 0B	07 07	03 03		
43	3F	3B	37	33	2F	2B	27	23	1F	1B	17	13	0F	0B	07		
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0		

Figure 2–13: UPM card diagram (front)

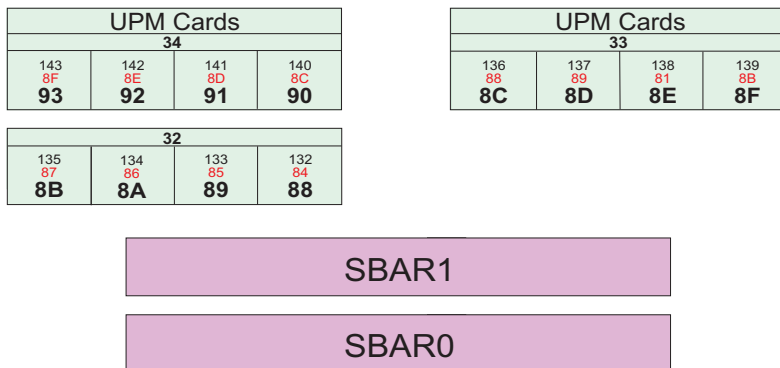


Figure 2–14: UPM card diagram (rear)

- 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 director is operational. **Exit MAP.**

7

A UPM card failed, and the card must be removed and replaced ([RRP: UPM Card on page 4–9](#)).

- This procedure is concurrent and can be performed while director power is on.
- Verify location of the failed card ([Figure 2–13](#) and [Figure 2–14](#)). For an OSI environment, [Figure 2–13](#) shows UPM card numbers (**0** through **35**, slot **32** is for internal use only.), port numbers (**00** through **143**, ports **128 - 131** are for internal use only.). For a FICON environment, [Figure 2–14](#) shows UPM card numbers (**0** through **35**, slot **32** is for internal use only.), port numbers (hexadecimal **04** through **93**, ports **84** through **87** are for internal use only), and bolded logical port addresses.
- Notify the customer that all ports on the defective card are to be blocked. Ensure the customer’s system administrator quiesces Fibre Channel frame traffic through any operational ports on the card and sets attached devices offline.
- Perform an external loopback test for all ports on the replacement card as part of FRU removal and replacement.
- Perform the data collection procedure as part of FRU removal and replacement.

Did UPM card replacement solve the problem?

NO YES

↓ The director is operational. **Exit MAP.**

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

8

Is fault isolation being performed at the HAFM server?

YES NO

↓ Fault isolation is being performed at the Embedded Web Server interface. Go to [step 38](#).

9

Does a blinking red and yellow diamond (failed FRU indicator) display over a UPM card graphic at the **Hardware View** or display adjacent to a Fibre Channel port graphic at the **Port Card View**?

NO **YES**

↓ A port or UPM card failure is indicated. Go to [step 6](#).

10

Did a Fibre Channel port or UPM card (all ports) fail a loopback test?

NO **YES**

↓ Go to [step 14](#).

11

Does a yellow triangle (attention indicator) display over a UPM card graphic at the **Hardware View** or display adjacent to a port graphic at the **Port Card View**?

YES **NO**

↓ Go to [step 13](#).

12

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

1. At the **Port Card View**, double-click the port graphic with the attention indicator. The **Port Properties** dialog box displays.
2. Inspect the **Operational State** field at the **Port Properties** dialog box, and the emulated green and amber LEDs adjacent to the port at the **Port Card View**.
3. [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: MAP 600: Port Operational and LED States

Operational State	Green LED	Amber LED	Action
Offline	Off	Off	Go to step 16 .
Not Operational	Off	Off	Go to step 16 .
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 17 .
Invalid Attachment	On	Off	Go to step 18 .
Link Reset	Off	Off	Go to step 28 .
Link Incident	Off	Off	Go to step 29 .
Segmented E_Port	On	Off	Go to MAP 0700: Fabric, ISL, and Segmented Port Problem Determination .

13

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

At the **Hardware View** or **Port Card View**, click **Logs** and choose **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 display in the **Link Incident Log**?

YES NO

↓ The director is operational. **Exit MAP.**

Go to [step 29](#).

14

A Fibre Channel port or UPM card (all ports) failed an internal or external loopback test.

1. Reset each port that failed the loopback test.
 - a. At the **Port Card View**, right-click the port. A menu displays.
 - b. Choose **Reset Port**. A `Reset Port n` message box displays, where `n` is the port number.
 - c. Click **OK**. The port resets.
2. Perform an external loopback test for all ports that were reset.

Did resetting ports solve the problem?

NO YES

↓ The director is operational. **Exit MAP.**

15

An electronic circuit breaker on the UPM card may have tripped. To reset the circuit breaker, partially remove and reseat the UPM card for which external loopback tests failed ([RRP: UPM Card on page 4–9](#)).

1. Unseat and disconnect the UPM card from the backplane. Unseat the card only, do not remove it from the director chassis.
2. Reseat the UPM card in the backplane.
3. Perform an external loopback test on the UPM card.

Did reseating the UPM card solve the problem?

NO YES

↓ The director is operational. **Exit MAP.**

Go to [step 7](#).

16

A director 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.**

17

Beaconing is enabled for the port.

1. Consult the customer and next level of support to determine the reason port beaconing is enabled.
2. Disable port beaconing.
 - a. At the **Port Card View**, right-click the port graphic. A menu displays.
 - b. Click **Enable Beaconing**. 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 director is operational. **Exit MAP.**

Go to [step 1](#).

18

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

Table 2–12: MAP 600: Invalid Attachment Reasons and Actions

Reasons	Action
Unknown	Contact the next level of support.
ISL connection not allowed on this port.	Go to step 19 .
Incompatible switch at other end of ISL.	Go to step 20 .
External loopback adapter connected to the port.	Go to step 21 .
N-Port connection not allowed on this port.	Go to step 19 .

Table 2–12: MAP 600: Invalid Attachment Reasons and Actions

Reasons	Action
Non-HP switch at other end of the ISL.	Go to step 20 .
Port binding violation-unauthorized WWN.	Go to step 23 .
Unresponsive node connected to port.	Go to step 24 .

19

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 (director or switch).

1. At the HAFM server's **Hardware View** for the selected director, click **Configure** and choose **Ports**. The **Configure Ports** dialog box displays.
2. Use the vertical scroll bar as necessary to display the information row for the port indicating an invalid attachment.
3. Click the **Type** field and configure the port from the list box as follows:
 - Choose fabric port (**F_Port**) if the port is cabled to a device (node).
 - Choose expansion port (**E_Port**) if the port is cabled to a fabric element (director or switch) to form an ISL.
4. Click **Activate** to save the configuration information and close the dialog box.

Did reconfiguring the port type solve the problem?

NO **YES**

↓ The director is operational. **Exit MAP.**

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

20

Open Systems
Only

The director is configured for Open Fabric mode but the switch or director at the other end of the ISL is not configured to Open Fabric mode.

S/390 Only

The director is configured for S/390 mode but the switch or director at the other end of the ISL is not configured to S/390 mode.

Configure the director operating mode:

1. Ensure the director is set offline ([Set Offline State on page 3–47](#)).
2. At the **Hardware View** for the selected director, choose **Configure > Operating Parameters > Switch Parameters**. The **Configure Switch Parameters** dialog box displays.
3. Select the operating mode as follows:
 - Choose the **Open Systems** option to set the director to open systems operating mode, then choose **Open Fabric 1.0** from the **Interop Mode** list box.
 - Choose the **S/390** option to set the director to S/390 operating mode.
4. Click **Activate** to save the selection and close the window.




Did configuring the operating mode solve the problem?

NO **YES**

↓ The director is operational. **Exit MAP.**

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

21

A loopback 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.**

22

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

- 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 director is operational. **Exit MAP.**

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

23

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**, click **Node List**. Note the **Port WWN** column.

The Port WWN is the 8-byte (16-digit) world-wide name (WWN) assigned to the port or Fibre Channel interface installed on the attached device.

- If a 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, the nickname displays 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 director is operational. **Exit MAP.**

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

24

Clean the fiber-optic connectors on the cable.

1. 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.
2. Block the port ([Block a Port on page 3–48](#)).
3. Disconnect both ends of the fiber-optic cable.
4. Clean the fiber-optic connectors. ([Clean Fiber-Optic Components on page 3–42](#)).
5. Reconnect the fiber-optic cable.
6. Unblock the port ([Unblock a Port on page 3–49](#)).
7. Monitor port operation for approximately five minutes.

Did the link incident recur?

YES NO

↓ The Fibre Channel link and director are operational.
Exit MAP.

25

Inspect both SBAR assemblies at the rear of the director. SBAR assembly LEDs can be inspected through the hexagonal cooling vents of the RFI shield.

Is the amber LED on an SBAR assembly illuminated but not blinking (beaconing)?

YES NO

↓ The director is operational. Go to [step 27](#).

26

An SBAR assembly failed and must be removed and replaced ([RRP: Redundant SBAR Assembly on page 4–24](#)).

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

Did SBAR assembly replacement solve the problem?

NO YES

↓ The director is operational. **Exit MAP.**

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

27

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.**

28

The director 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 director are operational. **Exit MAP.**

Go to [step 1](#).

29

A link incident message displayed 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 or FICON server attached to the director reporting the problem.

Clear the link incident for the port.

1. At the **Port Card View**, right-click the port. A menu displays.
2. Choose **Clear Link Incident Alert(s)** option. The **Clear Link Incident Alert(s)** dialog box displays ([Figure 2–15](#)).

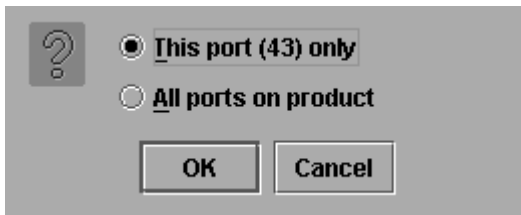


Figure 2–15: Clear Link Incident Alert(s)

3. Choose **This port (n) only** option (where n is the port number) and click **OK**. The link incident clears.
4. Monitor port operation for approximately five minutes.

Did the link incident recur?

YES **NO**

-
- ↓ The problem is transient and the Fibre Channel link and director are operational. **Exit MAP.**

30

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:

1. 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.
2. Block the port ([Block a Port on page 3–48](#)).
3. Remove and replace the fiber-optic jumper cable.
4. Unblock the port ([Unblock a Port on page 3–49](#)).

Was a corrective action performed?

YES **NO**

- ↓ Go to [step 32](#).

31

Monitor port operation for approximately five minutes.

Did the link incident recur?

YES **NO**

- ↓ The Fibre Channel link and director are operational. **Exit MAP.**

32

Clean fiber-optic connectors on the jumper cable.

1. 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.
2. Block the port ([Block a Port on page 3–48](#)).
3. Disconnect both ends of the fiber-optic jumper cable.
4. Clean the fiber-optic connectors ([Clean Fiber-Optic Components on page 3–42](#)).

5. Reconnect the fiber-optic jumper cable.
6. Unblock the port ([Unblock a Port on page 3–49](#)).
7. Monitor port operation for approximately five minutes.

Did the link incident recur?

YES **NO**

↓ The Fibre Channel link and director are operational. **Exit MAP.**

33

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

Is a link incident reported at the new port?

YES **NO**

↓ [Go to step 35.](#)

34

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

1. Inspect and verify operation of the attached device.
2. Repair the attached device if a failure is indicated.
3. Monitor port operation for approximately five minutes.

Did the link incident recur?

YES **NO**

↓ The attached device, Fibre Channel link, and director are operational. **Exit MAP.**

35

The director port reporting the problem is causing the recurrent link incident. The recurring link incident indicates port or UPM card degradation and a possible pending failure. [Go to step 6.](#)

36

A UPM card is not recognized by director firmware because the firmware version is not supported or the UPM card failed. Advise the customer of the problem and determine the correct firmware version to download from the HAFM server.

Download the firmware ([Download a Firmware Version to a Director on page 3–56](#)). Perform the data collection procedure after the download.

Continue.

37

Did the firmware download solve the problem?

NO **YES**

↓ The director is operational. **Exit MAP.**

A UPM card failure is indicated. Go to [step 7](#).

38

Is the Embedded Web Server interface operational?

NO **YES**

↓ Go to [step 41](#).

39

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

- The director-to-PC Internet link could not be established.
- AC power distribution in the director failed, or AC power was disconnected.
- Both of the director's CTP cards failed.

Continue.

40

Ensure the director reporting the problem is connected to facility AC power and the power switch (circuit breaker) at the rear of the director is set to the **ON** (up) position. Inspect the director for indications of being powered on, such as:

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- An illuminated green LED on the active CTP card.
- At least one green **PWR OK** LED illuminated on a power supply.
- Audio emanations and airflow from cooling fans.

Is the director powered on?

YES **NO**

- ↓ Analysis for an Ethernet link, AC power distribution, or dual CTP card failure is not described in this MAP. Go to [MAP 0000: Start MAP on page 2–12](#). If this is the second time at this step, contact the next level of support. **Exit MAP.**

41

Inspect UPM card operational states at the Embedded Web Server interface.

1. At the **View** panel, click the **FRU Properties** tab. The **View** panel (**FRU Properties** tab) displays.
2. Inspect the **Status** fields for UPM cards. Scroll down the **View** panel as necessary.

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

NO **YES**

- ↓ A UPM card failure is indicated. Go to [step 7](#).

42

Inspect Fibre Channel port operational states at the Embedded Web Server interface.

1. At the **View** panel, click the **Port Properties** tab. The **View** panel (**Port Properties** tab) displays with port **0** highlighted in red.
2. Click the port number (**0** through **143**) for which a failure is suspected to display properties for that port.
3. Inspect the **Operational State** field. Scroll down the **View** panel as necessary.
4. [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 16 .
Not Operational	Go to step 16 .
Port Failure	Go to step 6 .
Testing	Internal or external loopback test in process. Exit MAP.
Invalid Attachment	Go to step 18 .
Link Reset	Go to step 28 .
Not Installed	Go to step 43 .

43

Install a SFP optical transceiver in the port receptacle ([RRP: SFP Optical Transceiver on page 4–14](#)).

1. This procedure is concurrent and can be performed while director power is on.
2. Verify location of the uninstalled port transceiver.
 - Verify location of the failed port. [Figure 2–13](#) and [Figure 2–14](#) show the UPM card numbers (**0** through **35**, slot **32** is for internal use only.), port numbers (**00** through **143**, ports **128 - 131** are for internal use only.), and bolded logical port addresses.
3. Perform an external loopback test for the port as part of FRU removal and replacement. **Exit MAP.**

UPM Cards								CTP - 1 Card	CTP - 0 Card	UPM Cards							
31	30	29	28	27	26	25	24			23	22	21	20	19	18	17	16
127 7F	123 7B	119 77	115 73	111 6F	107 6B	103 67	99 63	95 5F	91 5B	87 57	83 53	79 4F	75 4B	71 47	67 43		
83	7F	7B	77	73	6F	6B	67	63	5F	5B	57	53	4F	4B	47		
126 7E	122 7A	118 76	114 72	110 6E	106 6A	102 66	98 62	94 5E	90 5A	86 56	82 52	78 4E	74 4A	70 46	66 42		
82	7E	7A	76	72	6E	6A	66	62	5E	5A	56	52	4E	4A	46		
125 7D	121 79	117 75	113 71	109 6D	105 69	101 65	97 61	93 5D	89 59	85 55	81 51	77 4D	73 49	69 45	65 41		
81	7D	79	75	71	6D	69	65	61	5D	59	55	51	4D	49	45		
124 7C	120 78	116 74	112 70	108 6C	104 68	100 64	96 60	92 5C	88 58	84 54	80 50	76 4C	72 48	68 44	64 40		
80	7C	78	74	70	6C	68	64	60	5C	58	54	50	4C	48	44		
60 3C	56 38	52 34	48 30	44 2C	40 28	36 24	32 20	28 1C	24 18	20 14	16 10	12 0C	08 08	04 04	00 00		
40	3C	38	34	30	2C	28	24	20	1C	18	14	10	0C	08	04		
61 3D	57 39	53 35	49 31	45 2D	41 29	37 25	33 21	29 1D	25 19	21 15	17 11	13 0D	09 09	05 05	01 01		
41	3D	39	35	31	2D	29	25	21	1D	19	15	11	0D	09	05		
62 3E	58 3A	54 36	50 32	46 2E	42 2A	38 26	34 22	30 1E	26 1A	22 16	18 12	14 0E	10 0A	06 06	02 02		
42	3E	3A	36	32	2E	2A	26	22	1E	1A	16	12	0E	0A	06		
63 3F	59 3B	55 37	51 33	47 2F	43 2B	39 27	35 23	31 1F	27 1B	23 17	19 13	15 0F	11 0B	07 07	03 03		
43	3F	3B	37	33	2F	2B	27	23	1F	1B	17	13	0F	0B	07		
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0		

Figure 2–16: UPM card diagram (front)

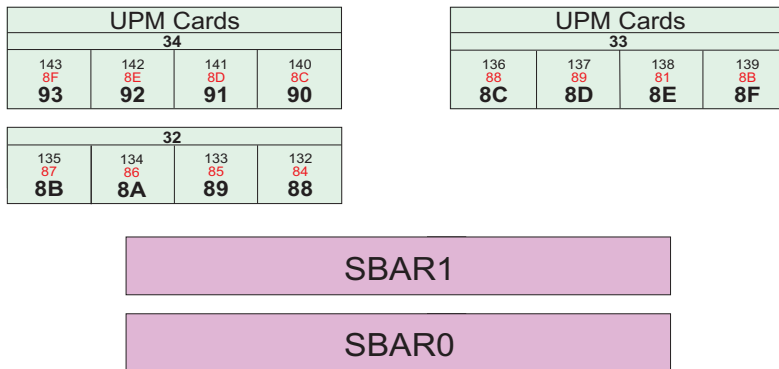


Figure 2–17: UPM card diagram (rear)

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 Director 2/140 Event Log or the Embedded Web Server event log.
- A segmentation reason associated with a Fibre Channel port at the Embedded Web Server interface.
- A yellow triangle (attention indicator) displays over a UPM card graphic or at the alert panel of the **Products View**, **Hardware View**, or **Port Card View**.
- A link incident message recorded in the **Link Incident Log** or **Port Properties** dialog box.

1

Was an event code **010**, **011**, **020**, **021**, **050**, **051**, **052**, **060**, **061**, **062**, **063**, **070**, **071**, or **072** observed at the Director 2/140 Event Log (HAFM server) or at the Embedded Web Server 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 700: Event Codes

Event Code	Explanation	Action
010	Login server unable to synchronize databases.	Go to step 7 .
011	Login server database invalid.	Go to step 7 .
020	Name server unable to synchronize databases.	Go to step 7 .
021	Name server database invalid.	Go to step 7 .

Table 2–14: MAP 700: Event Codes (Continued)

Event Code	Explanation	Action
050	Management server unable to synchronize databases.	Go to step 8 .
051	Management server database invalid.	Go to step 8 .
052	Management server internal error.	Go to step 8 .
060	Fabric controller unable to synchronize databases.	Go to step 9 .
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 .
071	Director 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?

YES NO

- ↓ Fault isolation is being performed through the Embedded Web Server interface. Go to [step 22](#).

4

Does a yellow triangle (attention indicator) display over a UPM card graphic at the **Hardware View** or display adjacent to a Fibre Channel port graphic at the **Port Card View**?

YES NO

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

5

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

1. At the **Port Card View**, double-click the port graphic with the attention indicator. The **Port Properties** dialog box displays as shown on the following page.
2. Inspect the **Operational State** field at the **Port Properties** dialog box.

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

YES **NO**

- ↓ Analysis for a UPM card failure or other link incident is not described in this MAP. Go to [MAP 0600: UPM Card Failure and Link Incident Analysis on page 2–79](#). **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: MAP 700: 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 databases to be reinitialized 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 010**-Following a CTP card reset, the login server attempted to acquire a fabric server database copy from the other CTP card and failed.

- **Event code 011**-Following a CTP card failover, the login server database failed cyclic redundancy check (CRC) validation.
- **Event code 020**-Following a CTP card reset, the name server attempted to acquire a fabric server database copy from the other CTP card and failed.
- **Event code 021**-Following CTP card failover, the name server database CRC validation.

All attached devices resume operation after fabric login. Perform the data collection procedure and return the Zip disk to HP for analysis by third-level support personnel.

Exit MAP.

8

A minor error occurred that caused management server databases to be reinitialized 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 050**-Following CTP card reset, the management server attempted to acquire a database copy from the other CTP card and failed.
- **Event code 051**-Following CTP card failover, 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 by third-level support personnel. **Exit MAP.**

9

A minor error occurred that caused fabric controller databases to be reinitialized to an empty state. As a result, the director briefly lost interswitch link capability. The following list explains the errors.

- **Event code 060**-Following CTP card reset, the fabric controller attempted to acquire a database copy from the other CTP card and failed.
- **Event code 061**-Following CTP card failover, the fabric controller database failed CRC validation.

All interswitch links resume operation after CTP card reset or failover. Perform the data collection procedure and return the Zip disk to HP for analysis by third-level support personnel. **Exit MAP.**

10

As indicated by an event code **062**, the fabric controller software detected a path to another director (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 director and multiswitch fabric are 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 (director 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 director or switch elements have more than 32 ISLs.

Did fabric reconfiguration solve the problem?

NO **YES**

↓ The director and multiswitch fabric are 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 director and prevented the directors 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 director is isolated from all directors 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.

1. At the HAFM server's **Hardware View**, select **Event Log** from the **Logs** menu. The **Event Log** displays.
2. Examine the first five bytes (**0** through **4**) of event data.
3. Byte **0** specifies the director port number (**00** through **143**) of the segmented E_port. Byte **4** specifies the segmentation reason (Table 2–16).

Table 2–16: MAP 700: Byte 4, Segmentation Reasons

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 director 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 director 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.

1. Contact your HP authorized service provider to determine the recommended E_D_TOV and R_A_TOV values for both directors.
2. Notify the customer both directors will set offline. Ensure the system administrator quiesces Fibre Channel frame traffic through the directors and sets attached devices offline.
3. Set both directors offline ([Set Offline State on page 3–47](#)).
4. At the **Hardware View** or **Port Card View** for the first director reporting the problem, choose **Configure > Operating Parameters > Fabric Parameters**. The **Configure Fabric Parameters** dialog box displays.
5. Type the recommended E_D_TOV and R_A_TOV values, then click **Activate**.
6. Repeat steps 4 and 5 at the **Hardware View** or **Port Card View** for the director attached to the segmented E_Port (second director). Use the same E_D_TOV and R_A_TOV values.
7. Set both directors online ([Set Online State on page 3–46](#)).

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

NO **YES**

↓ The directors, associated ISL, and multiswitch fabric are operational. **Exit MAP.**

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

15

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

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

2. Notify the customer both directors will set offline. Ensure the system administrator quiesces Fibre Channel frame traffic through the directors and sets attached devices offline.
3. Set both directors offline ([Set Offline State on page 3–47](#)).
4. At the **Hardware View** or **Port Card View** for the first director reporting the problem, choose **Configure > Operating Parameters > Switch Parameters**. The **Configure Switch Parameters** dialog box displays.
5. Type the customer-determined preferred domain ID value, then click **Activate**.
6. Repeat steps 4 and 5 at the **Hardware View** or **Port Card View** for the director attached to the segmented E_Port (second director). Use a different preferred domain ID value.
7. Set both directors online ([Set Online State on page 3–46](#)).

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

NO **YES**

↓ The directors, associated ISL, and multiswitch fabric are operational. **Exit MAP.**

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

16

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

1. Work with the system administrator to determine the desired zone name change for one of the affected directors. 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 (**_**).
2. Close the *Product Manager* application (**Hardware View**). The main HAFM or **Products View** (still active) displays.

3. Click the **Fabrics** tab. In the left pane of the **Fabrics View** window, select the fabric of which the director is a member. The **Fabrics View** displays with the default **Topology** tab active.
4. Click the **Zone Set** tab at the bottom of the window. The **Zone Set View** displays with the **Active Zone Set** displayed (Figure 2–18).

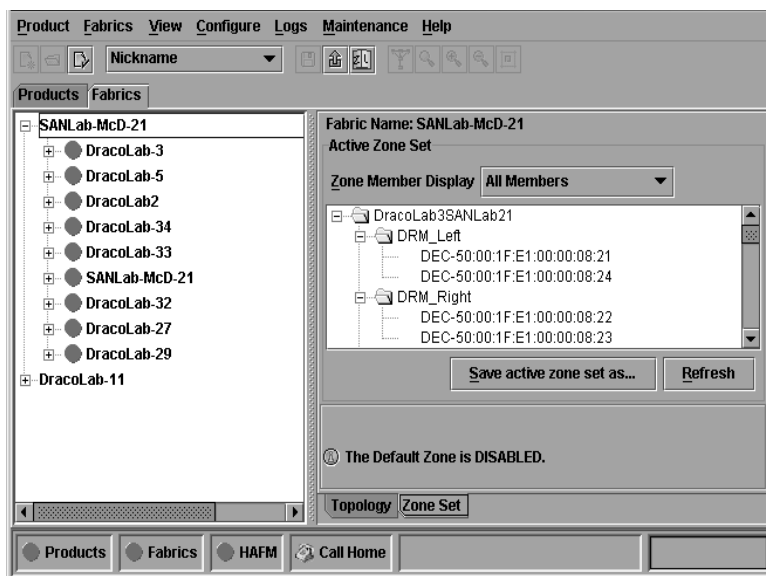


Figure 2–18: Zone Set View

5. Inspect zone names in the active zone set to determine the incompatible name.
6. Modify the incompatible zone name as directed by the customer:
 - a. Click **Configure** and choose **Zoning Library**. The **Zoning Library** dialog box displays.
 - b. Click the **Zones** tab.
 - c. Right click the zone name to be changed and choose **Rename**. The **Rename** dialog box displays. Type the new zone name (specified by the customer) and click **OK**.
 - d. Close the **Zoning Library** dialog box.

- e. 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.”
- f. To activate the zone set, click **Configure** and choose **Active Zone Set**. The **Active Zone Set** dialog box displays. Select the zone to be activated and click **Next**.
- g. 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.
- h. The new display summarizes the directors and switches that will be affected by activating the new zone set. Click **Next** if this reflects the desired zone change.
- i. Click **Start** to activate the zone set.

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

NO **YES**

- ↓ The directors, associated ISL, and multiswitch fabric are operational. **Exit MAP.**

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

17

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

1. Disconnect the fiber-optic jumper cable from the segmented E_Port.
2. Reconnect the cable to the same port.

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

NO **YES**

- ↓ The directors, associated ISL, and multiswitch fabric are operational. **Exit MAP.**

18

Initial program load (IPL) the director ([IPL the Director on page 3–44](#)).

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

NO **YES**

↓ The directors, associated ISL, and multiswitch fabric are operational. **Exit MAP.**

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

19

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

1. Notify the customer the director will set offline. Ensure the system administrator quiets Fibre Channel frame traffic through the director and sets attached devices offline.
2. Set the director offline ([Set Offline State on page 3–47](#)).
3. At the **Hardware View** or **Port Card View** for the director, choose **Configure > Operating Parameters > Switch Parameters**. The **Configure Switch Parameters** dialog box displays.
4. At the **Switch Priority** field, select a switch priority (**Principal**, **Never Principal**, or **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 directors and 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” displays in the **Reason** field of the **Port Properties** dialog box.

5. Set the director online ([Set Online State on page 3–46](#)).

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

NO **YES**

- ↓ The directors, associated ISL, and multiswitch fabric are operational. **Exit MAP.**

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

20

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

1. Perform the data collection procedure at the operational director and return the Zip disk to HP for analysis by third-level support personnel.
2. Go to [MAP 0000: Start MAP on page 2–12](#) and perform fault isolation for the failed director.

Exit MAP.

21

A director E_Port segmented because the director 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 director's inability to receive responses is caused by a hardware or link failure. Port segmentation occurs after five ELP transmissions, and prevents the failed director from joining an operational Fibre Channel fabric.

The director 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 2–12](#) and perform fault isolation for the failed director.

Exit MAP.

22

Is the Embedded Web Server interface operational?

YES **NO**

- ↓ Analysis for an Ethernet link, AC power distribution, or CTP card failure is not described in this MAP. Go to [MAP 0000: Start MAP on page 2–12](#). 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 Embedded Web Server interface.

1. At the **View** panel, click the **Port Properties** tab. The **View** panel (**Port Properties** tab) displays.
2. Click the port number (**0** through **143**) of the segmented port.
3. 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 director ISL is operational. **Exit MAP.**

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

Table 2–17: MAP 700: 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 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.

1. At the **Products View**, click **Logout/Exit** and choose **Exit**. The *HAFM* application closes.
2. Close any other applications that are running.

Continue.

2

Inspect the available random access memory (RAM). The computer must have a minimum of 128 megabytes (MB) of memory to run the Windows 2000 operating system and *HAFM* application.

1. Right-click anywhere in the **Windows 2000** task bar at the bottom of the desktop. A menu displays.
2. Choose **Task Manager**. The **Windows 2000 Task Manager** dialog box displays with the **Applications** page open. Click **Performance** to open the **Performance** page.
3. At the **Physical Memory (K)** portion of the dialog box, inspect the total amount of physical memory.
4. Close the dialog box.

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. **Exit MAP.**

3

Reboot the HAFM server PC and perform system diagnostics.

1. Choose **Start > Shut Down**. The **Shut Down Windows** dialog box displays.
2. At the **Shut Down Windows** dialog box, choose **Shut Down The Computer** and click **Yes** to power off the PC.
3. Wait approximately 30 seconds and power on the PC. After POSTs complete, the **Begin Logon** dialog box displays.
4. Simultaneously press **Ctrl + Alt + Delete** to display the **Logon Information** dialog box. Type a user name and password (obtained in [MAP 0000: Start MAP on page 2–12](#)) and click **OK**. The **Windows 2000** 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. **Exit MAP.**

4

After rebooting the PC, the HAFM Services and *HAFM* applications start, 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 2–12](#), and all are case sensitive), and click **Login**. The application opens and the **Products View** displays.

Did the **Products View** display and is the *HAFM* application operational?

NO **YES**

- ↓ The PC is operational. **Exit MAP.**

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. **Exit MAP.**

7

Reboot the HAFM server PC.

1. Choose **Start > Shut Down**. The **Shut Down Windows** dialog box displays.
2. At the **Shut Down Windows** dialog box, choose **Shut Down The Computer** and click **Yes** to power off the PC.
3. Wait approximately 30 seconds and power on the PC. After POSTs complete, the **Begin Logon** dialog box displays.
4. Simultaneously press **Ctrl + Alt + Delete** to display the **Logon Information** dialog box. Type a user name and password (obtained in [MAP 0000: Start MAP on page 2–12](#)) and click **OK**. The HAFM Services and *HAFM* applications start, and the **HAFM Login** dialog box displays.
5. At the **HAFM Login** dialog box, type a user name, password, and HAFM server name (obtained in [MAP 0000: Start MAP on page 2–12](#), and all are case sensitive), and click **Login**. The application opens and the **Products View** displays.

Did the **Products View** display and is the *HAFM* application operational?

NO **YES**

- ↓ The PC is operational. **Exit MAP.**

8

Re-install the *HAFM* application (“[Install or Upgrade Software](#)” on [page 3–62](#)).

Did the *HAFM* application install and open successfully?

NO **YES**

↓ The PC is operational. **Exit MAP.**

9

Advise the customer and next level of support that the PC hard drive should be restored to its original factory configuration. If the customer and support personnel do not concur, go to [step 10](#).

1. Restore the PC hard drive using the *HAFM Server Restore/Boot CD* shipped with the PC. Refer to the *readme.txt* file on the CD for instructions.
2. Install the *HAFM* application.

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

NO **YES**

↓ The PC is operational. **Exit MAP.**

10

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

Repair Information

This chapter describes repair and repair-related procedures used by service representatives for the Director 2/140 and associated field-replaceable units (FRUs). The following procedures are described:

- Obtaining log information at the HAFM server.
- Displaying and using HAFM server views.
- Obtaining and interpreting port diagnostic and performance data, and performing port diagnostic loopback tests.
- Channel wrap tests.
- Swapping ports.
- Collecting maintenance data.
- Cleaning fiber-optic components.
- Powering the director on and off.
- Performing a director initial program load (IPL).
- Setting the director online or offline.
- Blocking or unblocking Fibre Channel ports.
- Managing firmware versions.
- Managing configuration data.
- Installing or upgrading software.

S/390 Only

S/390 Only

Do not perform repairs until a failure is isolated to a FRU. If fault isolation was not performed, go to [MAP 0000: Start MAP on page 2-12](#).

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, follow all electrostatic discharge (ESD) procedures, **WARNING** and **CAUTION** statements, and 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.
4. After completing a FRU replacement procedure, extinguish the amber system error light-emitting diode (LED) on the bezel at the top front of the director.

Using Log Information

The HAFM and *Product Manager* applications 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 displays 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:

- Director 2/140 Audit Log.
- Director 2/140 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 from the *HAFM* application, click Logs and select Audit.

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

HAFM Event Log

The HAFM Event Log as shown in [Figure 3–1](#), displays events or error conditions recorded by the HAFM Management Services application. Entries reflect the status of the application and managed directors.

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

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.

To open the **HAFM Event Log** from the *HAFM* application, click **Logs** and choose **Event Log**. The 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 *Product Manager* application. In the latter case, the product (Director 2/140) 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. Include the information when reporting an event to third-level customer support.

Session Log

The Session Log displays 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** from the *HAFM* application, click **Logs** and choose **Session Log**.

- 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 as shown in [Figure 3–2](#), records an entry when the status of a director changes. The log reflects the previous status and current status of the director, 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.

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

To open the **Product Status Log** from the *HAFM* application, click **Logs** and choose **Product Status Log**. The log contains the following columns:

- Date/Time**—The date and time the director status change occurred.
- Network Address**—The IP address or configured name of the director. This address or name corresponds to the address or name displayed under the director icon at the **Products View**.
- Previous Status**—The status of the director prior to the reported status change (Operational, Degraded, Failed, or Unknown). An Unknown status indicates the *HAFM* application cannot communicate with the director.
- New Status**—The status of the director after the reported status change (Operational, Degraded, Failed, or Unknown).

Fabric Log

The Fabric Log reflects the time and nature of significant changes in the managed fabric.

To display the **Fabric Log** from the *Product Manager* application, click **Logs** and choose **Fabric Log**.

- **Date/Time**—The column displays the date and time of the change in the fabric.
- **Fabric Status Changed**—The 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).
- **Description**—The column displays a description of the change in the fabric.

Director 2/140 Audit Log

The Director 2/140 Audit Log displays a history of all configuration changes made to a director from the *Product Manager* application, a simple network management protocol (SNMP) management workstation open systems host, or the maintenance port. This information is useful for administrators and users. To open the Director 2/140 **Audit Log** from the *Product Manager* application, click **Logs** and choose **Audit Log**.

- For a description of the Director 2/140 Audit Log and an explanation of button functions at the bottom of the log window, refer to the *hp StorageWorks director product manager user guide*.

Director 2/140 Event Log

The Director 2/140 Event Log as shown in [Figure 3-3](#), displays a history of events for the director, such as system events, degraded operation, FRU failures, FRU removals and replacements, port problems, Fibre Channel link incidents, and HAFM server-to-director communication problems. All detected software and hardware failures are recorded in the Director 2/140 Event Log. The information is useful to maintenance personnel for fault isolation and repair verification.

Date/Time	Event	Description	Severity	FRU-Position
11/21/02 10:56:53 AM	430	Excessive Ethernet transmit errors.	Informational	CTP-0
11/21/02 9:51:14 AM	430	Excessive Ethernet transmit errors.	Informational	CTP-0
11/21/02 8:50:22 AM	430	Excessive Ethernet transmit errors.	Informational	CTP-0
11/21/02 7:58:03 AM	430	Excessive Ethernet transmit errors.	Informational	CTP-0
11/21/02 7:13:26 AM	430	Excessive Ethernet transmit errors.	Informational	CTP-0
11/21/02 6:29:17 AM	430	Excessive Ethernet transmit errors.	Informational	CTP-0
11/21/02 5:42:50 AM	506	Fibre Channel port failure.	Major	GSF2-7
11/21/02 5:42:50 AM	508	Fibre Channel port anomaly detected.	Informational	GSF2-7
11/21/02 5:42:48 AM	508	Fibre Channel port anomaly detected.	Informational	GSF2-7
11/21/02 5:42:46 AM	508	Fibre Channel port anomaly detected.	Informational	GSF2-7
11/21/02 5:28:27 AM	430	Excessive Ethernet transmit errors.	Informational	CTP-0
11/21/02 4:17:43 AM	430	Excessive Ethernet transmit errors.	Informational	CTP-0
11/21/02 3:16:45 AM	430	Excessive Ethernet transmit errors.	Informational	CTP-0
11/21/02 2:15:23 AM	430	Excessive Ethernet transmit errors.	Informational	CTP-0
11/21/02 1:27:06 AM	430	Excessive Ethernet transmit errors.	Informational	CTP-0
11/21/02 12:35:51 AM	430	Excessive Ethernet transmit errors.	Informational	CTP-0
11/20/02 11:34:57 PM	430	Excessive Ethernet transmit errors.	Informational	CTP-0

Export... Clear Refresh Close

Figure 3–3: Director 2/140 Event Log

To open the Director 2/140 **Event Log** from the *Product Manager* application, click **Logs** and choose **Event Log**. The log contains the following columns:

- **Date/Time**—The date and time the director event occurred.
- **Event**—The three-digit event code associated with the event. See Appendix B, [Event Code Tables](#) 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 type, followed by a number representing the FRU chassis position. FRU acronyms are:
 - **BKPLNE**—Backplane.
 - **CTP**—Control processor (CTP) card.
 - **SBAR**—Serial crossbar (SBAR) card.
 - **UPM**—Universal port module (UPM) card.

- **PM**—Port module (designation before a port module is identified as an FPM or UPM type)
- **FAN**—Fan module.
- **PWR**—Power supply.

The chassis (slot) position for a nonredundant FRU is **0**. The chassis positions for redundant FRUs are **0**, **1**, and **2**. The chassis positions for UPM cards are **0** through **35**, slot **32** is for internal use only.

- **Event Data**—Up to 32 bytes of supplementary event data (if available for the event) in hexadecimal format. See Appendix B, [Event Code Tables](#) for an explanation of the supplementary event data.

Refresh the Director 2/140 Event Log

To ensure recently-created events display in the Director 2/140 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 Director 2/140 Event Log

To ensure the Director 2/140 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 as shown in [Figure 3-4](#), displays a history of FRU removals and replacements (insertions) for the director. The information is useful to maintenance personnel for fault isolation and repair verification.

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

▲

▼

Figure 3–4: Hardware Log

To open the **Hardware Log** from the *Product Manager* application, click **Logs** and select **Hardware Log**. 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. FRU acronyms are:
 - **BKPLNE**—Backplane.
 - **CTP**—CTP card.
 - **SBAR**—SBAR card.
 - **UPM**—UPM card.
 - **PM**—Port module
 - **FAN**—Fan module.
 - **PWR**—Power supply.
- **Position**—A number representing the FRU chassis position. The chassis (slot) position for a nonredundant FRU is **0**. The chassis positions for redundant FRUs are **0**, **1**, and **2**. The chassis positions for UPM cards are **0** through **35**, slot **32** is for internal use only.
- **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 as shown in [Figure 3–5](#), displays a history of Fibre Channel link incidents (with associated port numbers) for the director. The information is useful to maintenance personnel for isolating port problems (particularly expansion port (E_Port) segmentation problems) and repair verification.

Date/Time	Port	Link Incident
11/25/02 1:50:34 PM	43	Loss-of-Signal or Loss-of-Synchronization.
11/25/02 1:45:05 PM	43	Loss-of-Signal or Loss-of-Synchronization.
11/21/02 4:12:17 PM	43	Loss-of-Signal or Loss-of-Synchronization.
11/21/02 4:09:30 PM	43	Loss-of-Signal or Loss-of-Synchronization.
11/21/02 3:59:31 PM	43	Loss-of-Signal or Loss-of-Synchronization.
11/21/02 3:55:25 PM	43	Loss-of-Signal or Loss-of-Synchronization.
11/21/02 3:48:23 PM	43	Loss-of-Signal or Loss-of-Synchronization.
11/21/02 3:14:55 PM	43	Loss-of-Signal or Loss-of-Synchronization.
11/21/02 3:12:36 PM	0	Loss-of-Signal or Loss-of-Synchronization.
11/21/02 3:12:36 PM	26	Loss-of-Signal or Loss-of-Synchronization.
11/21/02 3:06:02 PM	43	Loss-of-Signal or Loss-of-Synchronization.
11/21/02 2:58:20 PM	8	Loss-of-Signal or Loss-of-Synchronization.
11/21/02 2:40:56 PM	8	Loss-of-Signal or Loss-of-Synchronization.
11/21/02 2:40:27 PM	26	Not Operational primitive sequence (NOS) received.
11/21/02 2:40:01 PM	43	Loss-of-Signal or Loss-of-Synchronization.
11/21/02 2:01:30 PM	43	Loss-of-Signal or Loss-of-Synchronization.

Buttons: **Export...** **Clear** **Refresh** **Close**

Figure 3–5: Link Incident Log

To open the **Link Incident Log** from the *Product Manager* application, click **Logs** and choose **Link Incident Log**. The log contains the following columns:

- **Date/Time**—The date and time the link incident occurred.
- **Port**—The port number (**0** through **143** inclusive) that reported the link incident.
- **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.

See [MAP 0600: UPM Card Failure and Link Incident Analysis on page 2–79](#) or [MAP 0700: Fabric, ISL, and Segmented Port Problem Determination on page 2–99](#) for corrective actions in response to these link incident messages.

Refresh the Link Incident Log

To ensure recently-created link incidents display 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

The Threshold Alert Log as shown in [Figure 3–6](#), provides details of the threshold alert notifications. Besides the date and time that the alert occurred, the log also displays details about the alert as configured through the **Configure Threshold Alert(s)** option under the **Configure** menu.

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

Export... Clear Refresh Close

Figure 3–6: Threshold Alert Log

To open the **Threshold Alert Log** from the *Product Manager* application, click **Logs** and choose **Threshold Alert Log**. The log contains the following columns:

- **Date/Time**—The date and time stamp for when the alert occurred.
- **Name**—The name for the alert as configured through the **Configure Threshold Alerts** dialog box.

- **Port**—The port number where the alert occurred.
- **Type**—The type of alert: transmit (Tx) or receive (Rx).
- **Utilization %**—The 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.

Using Views

In addition to the **Hardware View**, the *Product Manager* application provides access to a series of views (windows) that provide information for administrators, users, and maintenance personnel. These views are accessed through the **Hardware View** or **Fabrics View**, and include the:

- Port List View.
- FRU List View.
- Node List View.
- Performance View.
- Topology View.
- Zone Set View.

Port List View

The Port List View as shown in [Figure 3–7](#), provides status information for all director ports. The information is useful to maintenance personnel for isolating port problems. To open the **Port List View** from the **Hardware View**, click the **Port List** tab.

Product Configure Logs Maintenance Help						
Hardware Port List Node List Performance FRU List						
#	Name	Block Config	State	Type	Operating Speed	Alert
0		Unblocked	No Light	G Port	2 Gb/sec	
1		Unblocked	No Light	G Port	Not Established	
2		Unblocked	No Light	G Port	Not Established	
3		Unblocked	No Light	G Port	Not Established	
4		Unblocked	No Light	G Port	Not Established	
5		Unblocked	No Light	G Port	Not Established	
6		Unblocked	No Light	G Port	Not Established	
7		Unblocked	No Light	G Port	Not Established	
8		Unblocked	Not Installed	G Port	Not Established	
9		Unblocked	Not Installed	G Port	Not Established	
10		Unblocked	Not Installed	G Port	Not Established	
11		Unblocked	Not Installed	G Port	Not Established	
12		Unblocked	Not Installed	G Port	Not Established	
13		Unblocked	Not Installed	G Port	Not Established	
14		Unblocked	Not Installed	G Port	Not Established	
15		Unblocked	Not Installed	G Port	Not Established	
16		Unblocked	Not Installed	G Port	Not Established	
17		Unblocked	Not Installed	G Port	Not Established	
18		Unblocked	Not Installed	G Port	Not Established	
19		Unblocked	Not Installed	G Port	Not Established	
20		Unblocked	Not Installed	G Port	Not Established	
21		Unblocked	Not Installed	G Port	Not Established	
22		Unblocked	Not Installed	G Port	Not Established	
23		Unblocked	Not Installed	G Port	Not Established	
24		Unblocked	No Light	G Port	Not Established	
25		Unblocked	No Light	G Port	Not Established	
26		Unblocked	No Light	G Port	Not Established	
27		Unblocked	No Light	G Port	Not Established	
28		Unblocked	No Light	G Port	Not Established	

Figure 3–7: Port List View

The **Port List View** provides status information in the following columns:

- **#**–The director port number (inclusive).
- **Addr**–The director logical port address (**04** through **8F** inclusive) in hexadecimal format (S/390 operating mode only).
- **Name**–The port name configured through the **Configure Ports** dialog box.
- **Block Config**–The port status (Blocked or Unblocked).
- **State**–The operating state of the port. Valid states are:
 - Online, offline, or testing.
 - Beaconing.
 - Invalid attachment.
 - Link incident or link reset.

S/390 Only

- No light, not operational, or port failure.
- Segmented E_Port.
- **Type**—The type of port. Valid port types are a generic port (G_Port) not connected to a Fibre Channel device, director, or switch (therefore light is not transmitted); a fabric port (F_Port) connected to a device; or an expansion port (E_Port) connected to a director or switch to form an interswitch link (ISL).
- **Operating Speed**—The operating speed of the port (1 or 2 Gb/sec.).
- **Alert**—If Link Incident (LIN) alerts are configured for the port through the **Configure Ports** dialog box, a yellow triangle displays in the column when a link incident occurs. A yellow triangle also displays if beaconing is enabled for the port. A red and yellow diamond displays if the port fails.

Double-click anywhere in a row for an installed port to open the **Port Properties** dialog box. Right-click anywhere in a row for an installed port to open a menu to:

- Open the **Port Properties**, **Node Properties**, or **Port Technology** dialog boxes.
- Block or unblock the port.
- Enable or disable port beaconing.
- Perform port diagnostics.
- Enable or disable port channel wrapping. This menu option displays only when the director is configured for S/390 operating mode.
- Swap one Fibre Channel port address with another. This menu option displays only when the director is configured for S/390 operating mode.
- Clear link incident alerts.
- Reset the port.
- Configure port binding.
- Clear threshold alerts.




FRU List View

The FRU List View as shown in [Figure 3–8](#), displays a list of all director FRUs. The information is useful to maintenance personnel for fault isolation and repair verification.

Product Configure Logs Maintenance Help						
Hardware Port List Node List Performance FRU List						
FRU	Port List	Node List	Performance	FRU List	Part Number	Serial Number
BKPLNE	0		Active		470-000435-300	T2374878
CTP	0		Active		470-000437-401	82372257
CTP	1		Backup		470-000437-401	82372253
SBAR	0		Active		002-002487-201	82380004
SBAR	1		Backup		002-002487-201	82202000
FAN	0		Active			
FAN	1		Active			
FAN	2		Active			
PWR	0		Active		721-000058-000	52074128
PWR	1		Active		721-000058-000	52074155
UPM	0		Active		470-000453-410	82301030
UPM	1		Active		470-000453-410	82300772
UPM	6		Active		470-000453-410	82301895
UPM	7		Active		470-000453-400	82250602
UPM	8		Active		470-000453-410	32320072
UPM	9		Active		470-000453-410	82342010
UPM	14		Active		470-000453-400	82270485
UPM	15		Active		470-000453-410	82300773
UPM	16		Active		470-000453-410	82321780
UPM	17		Active		470-000453-410	82230786
UPM	22		Active		470-000453-410	82201012
UPM	23		Active		470-000453-410	82221024
UPM	24		Active		470-000453-410	82192979
UPM	25		Active		470-000453-410	82222273
UPM	30		Active		470-000453-410	82151832
UPM	31		Active		470-000453-410	82220907
UPM	33		Active		470-000453-410	82370367
UPM	34		Active		470-000453-410	82341868
UPM	35		Active		470-000453-410	82321410

Figure 3–8: FRU List View

To open the **FRU List View** from the **Hardware View**, click **View** and choose **FRU List**. The **FRU List View** contains the following columns:

- **FRU**—An acronym representing the FRU type. FRU acronyms are:
 - **BKPLNE**—Backplane.
 - **CTP**—CTP card.
 - **SBAR**—SBAR card.
 - **UPM**—UPM card.
 - **PM**—Port module
 - **FAN**—Fan module.
 - **PWR**—Power supply.
- **Position**—A number representing the FRU chassis position. The chassis (slot) position for a nonredundant FRU is **0**. The chassis positions for redundant FRUs are **0**, **1**, and **2**. The chassis positions for UPM cards are **0** through **35**, slot **32** is for internal use only.
- **Status**—The FRU status (Active or Backup).

- **Part Number**—The FRU part number.
- **Serial Number**—The FRU serial number.

Node List View

The Node List View as shown in [Figure 3-9](#), displays information about all devices attached to the director through node ports (N_Ports). The information is useful to maintenance personnel for fault isolation and repair verification.

To open the **Node List View**, choose the **Node List** tab. The **Node List View** contains the following columns:

- **Port #**—The director port number (inclusive). Only ports attached to a device are displayed.
- **Addr**—The director logical port address (**04** through **8F** inclusive) in hexadecimal format (S/390 operating mode only).
- **Node Type**—The type of attached device. This information is supplied by the device (if supported). Node types include:
 - Unknown or other.
 - Hub, switch, gateway, or converter.
 - Host or host bus adapter (HBA).
 - Proxy agent.
 - Storage device or storage subsystem.
 - Module.
 - Software driver.
 - Reserved.

S/390 Only

Product Configure Logs Maintenance Help				
Hardware Port List Node List Performance FRU List				
Port #	Address	Port WWN	Unit Type	BB_Credit
29	752113	XP128 6213	Unspecified	7
32	752413	XP128 6202	Unspecified	7

Figure 3–9: Node List View

- **Port WWN**—The eight-byte (16-digit) world-wide name (WWN) assigned to the port or Fibre Channel interface installed on the attached device.
 - If a 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, the nickname displays in place of the WWN.
- **BB_Credit**—The buffer-to-buffer credit (BB_Credit) value assigned to a port attached to a device. The value (normally **1** through **16** inclusive) determines the frame buffers available for the port. Ports configured for extended distance operation are assigned a BB_Credit value of **60**.

Performance View

The Performance View displays statistical information about the performance of ports. The information is useful to maintenance personnel for fault isolating port problems. For information about the **Performance View**, see [Performing Port Diagnostics on page 3–21](#).

Topology View

To open the **Topology View** from the main HAFM or **Products View**, choose the **Fabrics** tab. In the left pane of the **Fabrics View** window, select the fabric of which the director is a member. The **Topology View** as shown in [Figure 3–10](#), displays with the default **Topology** tab active.

The left panel displays an expandable fabrics tree that lists managed fabrics, director, and switch elements in each fabric, and nodes (Fibre Channel devices) connected to fabric elements. The right panel displays directors, switches, and ISLs for the selected fabric. Information associated with each fabric element icon is identical to that associated with icons in the **Products View**.

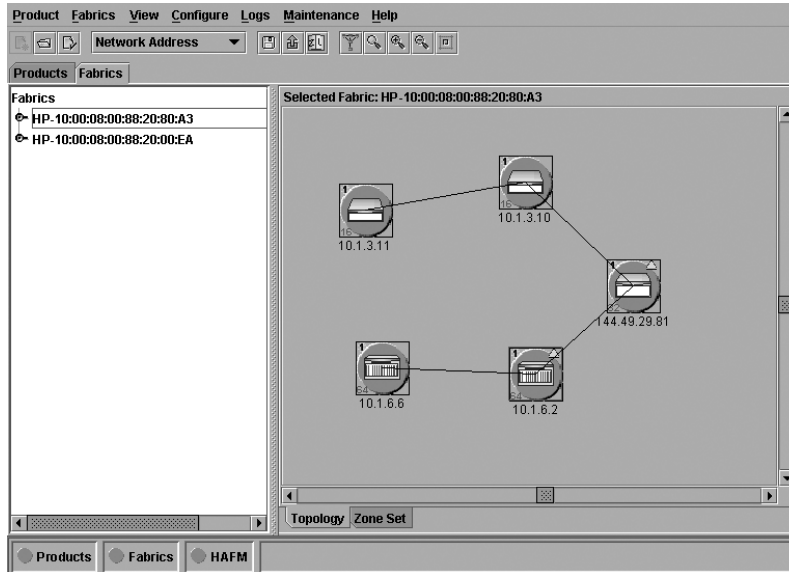


Figure 3–10: Topology View

A menu bar at the top of the **Fabrics View** provides **Product**, **Fabrics**, **View**, **Configure**, **Logs**, **Maintenance**, and **Help** options (with associated menus) that allow users to perform *HAFM* application tasks.

An HAFM status bar at the bottom left corner of the view window displays colored icons (green circle, yellow triangle, red and yellow diamond, or grey square) that indicate the most degraded or critical status of any managed product, fabric, or the HAFM server. Messages display as required to the right of the colored icons.

By double-clicking a fabric icon or right-clicking a fabric icon and selecting from menu options, a user opens the *Product Manager* application for the element.

Zone Set View

To open the **Zone Set View** from the main HAFM or **Products View**, choose the **Fabrics** tab. In the left pane of the **Fabrics View** window, select the fabric of which the director is a member. The **Fabrics View** (Topology) displays with the default **Topology** tab active. choose the **Zone Set** tab at the bottom of the window. The **Zone Set View** displays with the active zone set shown, as shown in [Figure 3–11](#).

The view displays an expanded (or collapsed) list of the active zone set, including all zones and zone members. The active zone set name of the fabric selected in the fabrics window on the left displays at the top of the list, followed by zone names, followed by zone members for each zone name. The table at the top of the view indicates if the default zone is enabled or disabled.

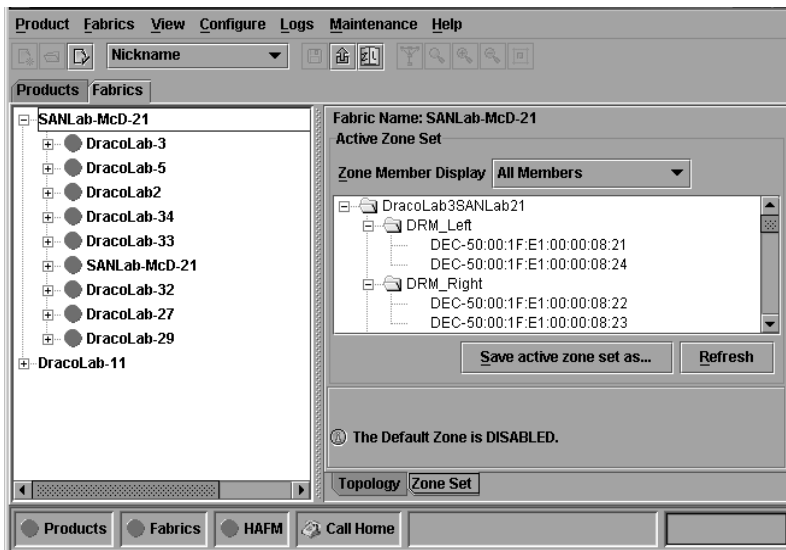


Figure 3–11: Zone Set View

Zone members display as:

- The unique 16-digit WWN identifying the device attached to the port. If a nickname is configured, the nickname displays instead. For example:
10:00:02:06:77:43:B0:1C
- A unique domain ID (**1** through **31** inclusive) and port number (inclusive) if zoned by port number. For example:
Domain 1, Port 7

The information is also useful to maintenance personnel for fault isolating E_Port segmentation problems caused by incompatible zone sets.

When forming a multiswitch fabric by connecting directors with active zone sets, zone names within the active zone sets should not be duplicated. Zone names can be duplicated only if the member WWNs of each zone are identical. If two directors have a zone name conflict (duplicate zone names exist), the zone sets cannot merge, the connecting E_Port at each director segments to prevent the creation of an ISL, and the directors do not form a multiswitch fabric.

- For a description of how to expand or collapse the active zone set list, and an explanation of button functions at the bottom of the **Zone Set View**, refer to the *hp StorageWorks ha-fabric manager user guide*.

Performing Port Diagnostics

Port and UPM card diagnostics are performed at the director or HAFM server (*Product Manager* application). These diagnostics include:

- Inspecting port and UPM card LEDs at the director.
- Obtaining port degradation or failure information at the *Product Manager* application's **Port Card View**.
- Obtaining statistical performance information for ports at the *Product Manager* application's **Performance View**.
- Performing internal or external port loopback tests.
- Performing channel wrap tests. The tests apply only to a director configured for S/390 operating mode.

S/390 Only

UPM card LEDs

To obtain port or UPM card operational information, inspect the UPM card LEDs. The card faceplate contains:

- An amber LED (at the top of the card) that illuminates if any port fails or blinks if FRU beaconing is enabled.
- A bank of amber and green LEDs above the ports. One amber LED and one green LED are associated with each port and indicate port status as follows:
 - The green LED illuminates (or blinks if there is active traffic) and the amber LED extinguishes to indicate normal port operation.
 - The amber LED illuminates and the green LED extinguishes to indicate a port failure.
 - Both LEDs extinguish to indicate a port is operational but not communicating with an N_Port (no cable attached, loss of light, port blocked, or link recovery in process).
 - The amber LED flashes and the green LED either remains on, extinguishes, or flashes to indicate a port is beaconing or running online diagnostics.

Port Card View

The Port Card View as shown in [Figure 3–12](#), shows a representation and associated information about a specified director UPM card. The information is useful to maintenance personnel for fault isolation and repair verification of UPM card degradation, UPM card failures, link incidents, and E_Port segmentation problems.

To open an instance of the **Port Card View** from the **Hardware View**, double-click the desired UPM card graphic on the front view of the director.

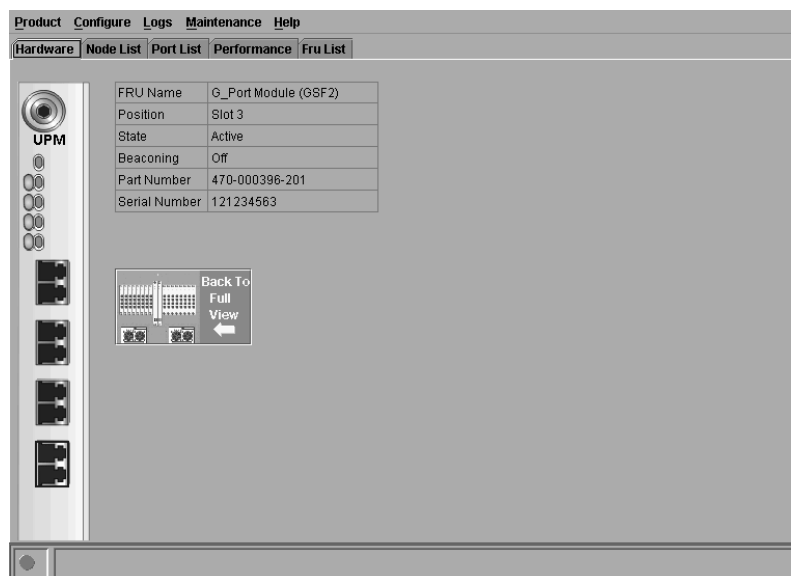


Figure 3–12: Port Card View

The status of the selected UPM card and operational states for all ports are visible on the **Port Card View**. These port operational states are defined in [Table 3–2](#).

Table 3–2: Port Operational States

Port State	Green LED	Amber LED	Alert Symbol	Description
Online	On	Off	None	An attached device is connected to the director and ready to communicate, or is communicating with other attached devices. If the port remains online, the green port LED remains illuminated. At the director UPM card, the green LED blinks when there is Fibre Channel traffic through the port.
Offline	Off	Off	None	The director port is blocked and transmitting the offline sequence (OLS) to the attached device.
	Off	Off	Yellow Triangle	The director port is unblocked and receiving the OLS, indicating the attached device is offline.
Beaconing	Off or On	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 director port has an invalid attachment state if: (1) a loopback plug is connected to the port with no diagnostic test running, or (2) the port is cabled to another port on the same director, or (3) the port connection conflicts with the configured port type.
Link Incident	Off	Off	Yellow Triangle	A link incident occurred on the port. The alert symbol displays at the Port Card View , Port List View , and Hardware View .

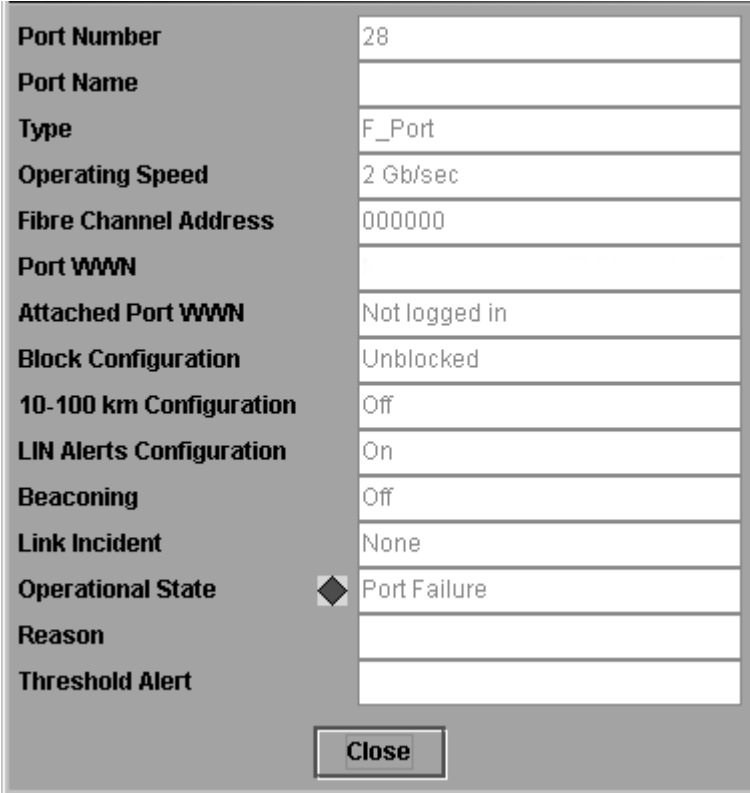
Table 3–2: Port Operational States (Continued)

Port State	Green LED	Amber LED	Alert Symbol	Description
Link Reset	Off	Off	Yellow Triangle	The director 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 by the director port. This is a normal condition when there is no cable attached to the port or when the attached device is powered off.
Not Operational	Off	Off	Yellow Triangle	The director port is receiving the not operational sequence (NOS) from an attached device.
Port Failure	Off	On	Red and Yellow Blinking Diamond	The director port failed and requires service.
Segmented E_Port	On	Off	Yellow Triangle	The E_Port is segmented, preventing two connected directors from joining and forming a multiswitch fabric.
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.

Right-click the faceplate of the UPM card (away from a port connector) to access a menu to:

- Block all ports ([Block a UPM Card on page 3–49](#)).
- Unblock all ports ([Unblock a UPM Card on page 3–50](#)).
- Perform port diagnostics ([Perform Loopback Tests on page 3–32](#)).

Double-click a port connector to display the **Port Properties** dialog box, as shown in [Figure 3–13](#).



Port Number	28
Port Name	
Type	F_Port
Operating Speed	2 Gb/sec
Fibre Channel Address	000000
Port WWN	
Attached Port WWN	Not logged in
Block Configuration	Unblocked
10-100 km Configuration	Off
LIN Alerts Configuration	On
Beaconing	Off
Link Incident	None
Operational State	<input checked="" type="checkbox"/> Port Failure
Reason	
Threshold Alert	

Close

Figure 3–13: Port Properties dialog box

The dialog box provides the following information:

- **Port Number**—The director port number (inclusive).
- **Port Name**—The user-defined name or description for the port.
- **Type**—The type of port (G_Port if nothing is attached to the port, F_Port if a device is attached to the port, and E_Port if the port is connected to another director or switch as part of an ISL).
- **Operating Speed**—The operating speed of the port (1 or 2 Gb/sec.).
- **Fibre Channel Address**—The Fibre Channel address identifier for the port.
- **Port WWN**—The Fibre Channel WWN for the director port.

- **Attached Port WWN**—The Fibre Channel WWN for the port of the attached device.
- **Block Configuration**—A user-configured state for the port (Blocked or Unblocked).
- **10-100 km Configuration**—A user-specified state for the port (On or Off), configured through the **Configure Ports** dialog box.
- **LIN Alerts Configuration**—A user-specified state for the port (On or Off), configured through the **Configure Ports** dialog box.
- **Beaconing**—User-specified for the port (On or Off). When beaconing is enabled, a yellow triangle displays adjacent to the status field.
- **Link Incident**—If no link incidents are recorded, *None* displays in the status field. If a link incident is recorded, a summary displays describing the incident, and a yellow triangle displays adjacent to the status field. Valid summaries are:
 - 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 the current link state.
- **Operational State**—The state of the port (Online, Offline, Beaconing, Invalid Attachment, Link Incident, Link Reset, No Light, Not Operational, Port Failure, Segmented E_Port, or Testing). A yellow triangle displays adjacent to the status field if the port is in a non-standard state that requires attention. A red and yellow diamond displays adjacent to the status field if the port fails.
- **Reason**—The following messages display in the **Reason** field of the **Port Properties** dialog box if an Invalid Attachment or Segmented E_Port state occurs for the port. Invalid Attachment Messages are explained in [Table 3-3](#).

Table 3-3: Invalid Attachment Messages and Explanations

Message	Explanation
01 Unknown.	Invalid attachment reason cannot be determined.
02 ISL connection not allowed on this port.	Port is configured as an F_Port, but connected to switch or director.

Table 3-3: Invalid Attachment Messages and Explanations (Continued)

Message	Explanation
03 ELP rejected by the attached switch.	This director or switch transmitted an exchange link protocol (ELP) frame that was rejected by the switch at the other end of the ISL (Invalid Attachment only).
04 Incompatible switch at the other end of the ISL.	Interop mode for this switch is set to Open Fabric mode and the switch at the other end of the ISL is a switch configured for Homogeneous Fabric mode.
05 External loopback adapter connected to the port.	A loopback plug is connected to the port and there is no diagnostic test running.
06 N_Port connection not allowed on this port.	The port type configuration does not match the actual port use. Port is configured as an E_Port, but attaches to a node device.
07 Non-homogeneous switch at other end of the ISL.	The cable is connected to a non-homogeneous switch and interop mode is set to homogeneous fabric mode.
08 ISL connection not allowed on this port.	This port type configuration does not match the actual port use (the port is configured as an F_Port, but attaches to a switch or director).
10 Port binding violation - unauthorized WWN.	The WWN entered to configure port binding is not valid or a nickname was used that is not configured through the Product Manager for the attached device.
11 Unresponsive node connected to port.	<p>Possible causes are:</p> <ul style="list-style-type: none"> • Hardware problem on switch or on a connected node where ELP frames are not delivered, the response is not received, or a fabric login in (FLOGI) cannot be received. There may be problems in switch SBAR. • Faulty or dirty cable connection. • Faulty host bus adapters that do not send out FLOGI within reasonable time frame.

Segmented E_Port Messages:

- Incompatible operating parameters, such as resource allocation time-out values (R_A_TOV) or error-detect time-out values (E_D_TOV), are inconsistent. Refer to the *hp StorageWorks director 2/140 installation guide* for more information.
- Duplicate domain IDs. Refer to the *hp StorageWorks director 2/140 installation guide* for more information.
- Incompatible zoning configurations. See [MAP 0700: Fabric, ISL, and Segmented Port Problem Determination on page 2–99](#) for details.
- Build fabric protocol error.
- No principal switch (no switch in fabric is capable of being principal switch).
- No response from an attached switch.
- **Threshold Alert**—If a threshold alert exists for the port, an alert indicator (yellow triangle) displays by the **Threshold Alert** field, and the configured name for the last alert received displays in the field.

Right-click a port connector to access a menu to:

- Open the **Port Properties**, **Node Properties**, or **Port Technology** dialog boxes.
- Block or unblock the port.
- Enable or disable port beaconing.
- Perform port diagnostics.
- Enable or disable port channel wrapping. This menu option displays only when the director is configured for S/390 operating mode.
- Swap one Fibre Channel port address with another. This menu option displays only when the director is configured for S/390 operating mode.
- Clear link incident alerts.
- Reset the port.
- Configure port binding.
- Clear threshold alerts.

A blue oval icon with the text "S/390 Only" in white.A blue oval icon with the text "S/390 Only" in white.

Performance View

The Performance View as shown in [Figure 3–14](#), displays statistical information about the performance of ports. The information is useful to maintenance personnel for isolating port problems. To open the **Performance View** from the **Hardware View**, choose the **Performance** tab.

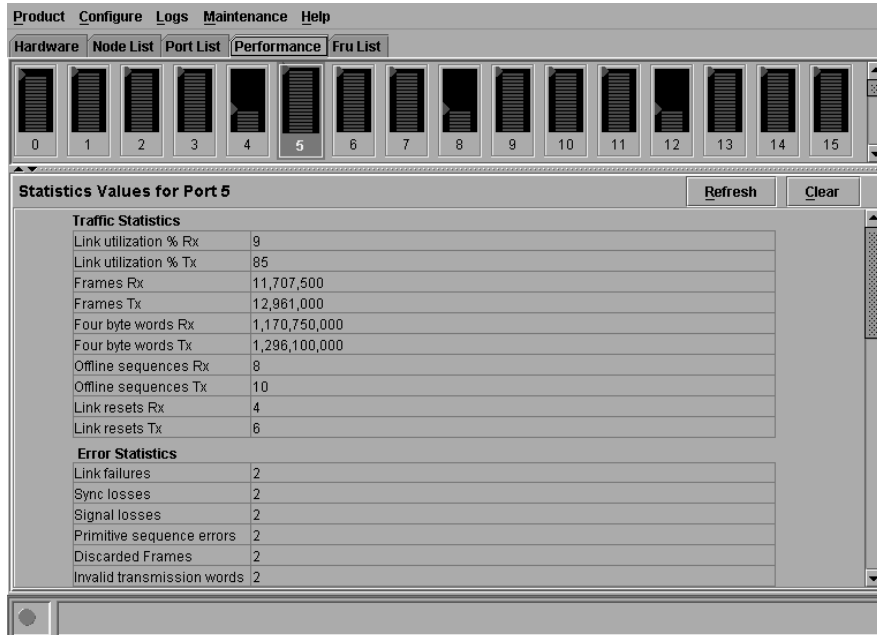


Figure 3–14: Performance View

When the **Performance View** opens, no port statistics or errors display. Each port bar graph in the upper portion of the view displays the instantaneous transmit or receive activity level for the port, and is updated every five seconds. The relative value displayed is the greater of either the transmit or receive activity (whichever value is greatest when sampled). Each port's graph has multiple green-bar level indicators that correspond to a percentage of the maximum Fibre Channel throughput for the port (either transmit or receive). If any activity is detected for a port, at least one green bar displays.

A red indicator on each port bar graph (high-water mark) remains at the highest level the graph has reached since the **Performance View** was opened. The indicator does not display if the port is offline, and is reset to the bottom of the graph if the port detects a loss of light.

When the mouse cursor is passed over a port bar graph, the graph highlights with a blue border and an information pop-up displays adjacent to the port as follows:

- If a device is not attached to the port, the pop-up displays the port's current state.
- If a device is attached to the port, the pop-up displays the WWN of the attached device.
- If the port is an E_Port, the pop-up displays **E_Port**.
- If the port is segmented, the pop-up displays **Segmented E_Port**.

Click a port bar graph to display statistics values for the port (bottom half of the **Performance View**). Right-click a port bar graph to display statistics values for the port (bottom half of the **Performance View**) and access a menu to:

- Open the **Port Properties**, **Node Properties**, or **Port Technology** dialog boxes.
- Block or unblock the port.
- Enable or disable port beaconing.
- Perform port diagnostics.
- Enable or disable port channel wrapping. This menu option displays only when the director is configured for S/390 operating mode.
- Swap one Fibre Channel port address with another. This menu option displays only when the director is configured for S/390 operating mode.
- Clear link incident alerts.
- Reset the port.
- Configure port binding.
- Clear threshold alerts.

A blue oval icon with white text that reads "S/390 Only".A blue oval icon with white text that reads "S/390 Only".

When a port is selected, the bottom half of the **Performance View** displays the following tables of cumulative port statistics and error count values. These statistics correspond to values defined in the Fabric Element management information base (MIB).

- Traffic statistics.
- Class 2 statistics.
- Class 3 statistics.
- Error statistics.

Click **Refresh** to update statistical information displayed on the **Performance View** for the selected port. Click **Clear** to reset the cumulative value counts to zero on the **Performance View** for the selected port. A confirmation dialog box displays before the values are cleared.

Perform Loopback Tests

This section describes the procedures to perform an:

- **Internal loopback test**—An internal loopback test checks UPM card circuitry, but does not check fiber-optic components of a port transceiver. The test is performed with a device attached to the port, but the test momentarily blocks the port and is disruptive to the attached device.
- **External loopback test**—An external loopback test checks UPM card circuitry, including fiber-optic components of a port transceiver. To perform the test, the attached device must be quiesced and disconnected from the port, and a multimode or singlemode loopback plug must be inserted in the port receptacle.

Internal Loopback Test

To perform an internal loopback test for a single port or a UPM card (four ports):

1. Notify the customer a disruptive internal loopback test will be performed on a port or UPM card. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the port or UPM card, and sets attached devices offline.

NOTE: At the start of the loopback test, the port or UPM card can be online, offline, blocked, or unblocked.

2. At the HAFM server, open the *HAFM* application. The **Products View** displays.
3. Double-click the icon representing the director for which the loopback test will be performed. The **Hardware View** for the selected director displays.
4. At the **Hardware View**, verify the location of the port or UPM card to be tested. When the mouse pointer is passed over a graphical UPM card on the front view of the director, the card highlights with a blue border and a pop-up displays with the following information:
 - Port card type (UPM).
 - Chassis slot number (**0** through **35**, slot **32** is for internal use only).
 - The four consecutive port numbers on the selected card. Valid port numbers are in the range of inclusive.

5. Reset each port to be tested:
 - a. At the **Hardware View**, double-click the UPM card for which ports are to be tested. The **Port Card View** displays.
 - b. At the **Port Card View**, right-click the tested port. A menu displays.
 - c. Choose **Reset Port**. A reset warning message box displays.
 - d. Click **OK**. The port resets.
 - e. Click **Back To Full View** to return to the **Hardware View**.
6. Click **Maintenance** and choose **Port Diagnostics**. The **Port Diagnostics** dialog box displays, as shown in [Figure 3–15](#).

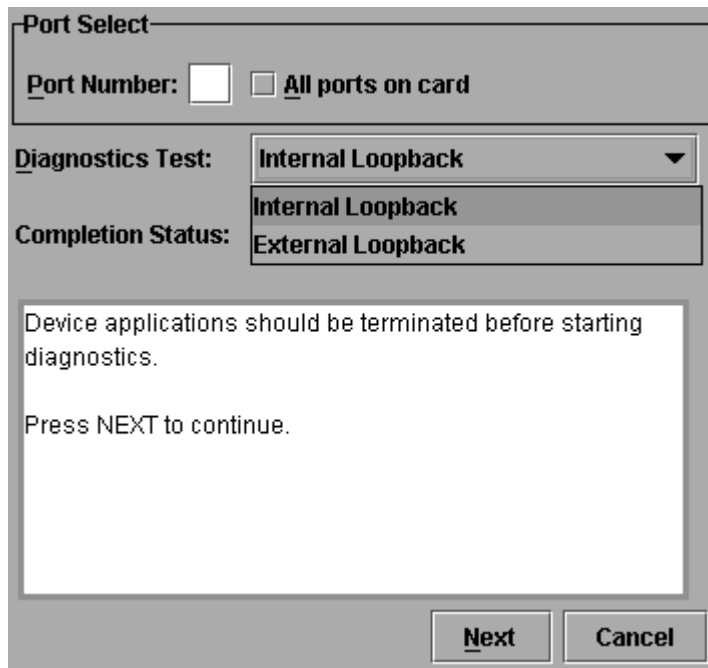


Figure 3–15: Port Diagnostics dialog box

7. Select a port or UPM card for test:
 - To select an individual port for test, type the port number in the **Port Number** field.

- To select a UPM card for test, type the port number of any of the four ports on the card in the **Port Number** field, then choose **All Ports On Card** option.
- 8. At the **Diagnostics Test** list box, choose **Internal Loopback**.
- 9. Click **Next**. Beaconing initiates for the port or UPM card selected for test. At the **Hardware View**, a yellow triangle displays at the top of the UPM card. At the **Port Diagnostics** dialog box, the message `Verify selected ports are beaoning` displays.
- 10. Verify beaoning is enabled, then click **Next**. The message `Press START TEST to begin diagnostics` displays, and **Next** changes to **Start Test**.
- 11. Click **Start Test**. The test begins and:
 - **Start Test** changes to **Stop Test**.
 - The message `Port xx: TEST RUNNING` displays, where `xx` is the port number. If a UPM card is tested, the message displays for all four ports.
 - A red progress bar (indicating percent completion) travels from left to right across the **Completion Status** field.

As a port is tested, the amber LED flashes (beacons) and the green LED extinguishes (indicating the port is blocked).

NOTE: Click **Stop Test** at any time to abort the loopback test.
- 12. When the test completes, test results display (for each port tested) as `Port xx: Passed!` or `Port xx: Failed!` in the message area of the dialog box. If a port fails the test, the amber LED for the port remains illuminated.
- 13. When finished, click **Cancel** to close the **Port Diagnostics** dialog box and return to the **Hardware View**. Beaconing is disabled for the port or UPM card.
- 14. Reset each tested port:
 - a. At the **Hardware View**, double-click the UPM card for which ports were tested. The **Port Card View** displays.
 - b. At the **Port Card View**, right-click the tested port. A menu displays.
 - c. Choose **Reset Port**. A reset warning box displays.
 - d. Click **OK**. The port resets.

External Loopback Test

To perform an external loopback test for a single port or a UPM card (four ports):

1. Notify the customer a disruptive external loopback test will be performed on a port or UPM card, and the fiber-optic cable or cables will be disconnected. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the port or UPM card and sets attached devices offline.

NOTE: At the start of the loopback test, the port or UPM card can be online, offline, blocked, or unblocked.

2. At the HAFM server, open the *HAFM* application. The **Products View** displays.
3. Double-click the icon representing the director for which the loopback test will be performed. The **Hardware View** for the selected director displays.
4. At the **Hardware View**, verify the location of the port or UPM card to be tested. When the mouse cursor is passed over a graphical UPM card on the front view of the director, the card highlights with a blue border and a pop-up displays with the following information:
 - Port card type (UPM).
 - Chassis slot number (**0** through **35**, slot **32** is for internal use only).
 - The four consecutive port numbers on the selected card. Valid port numbers are in the range of inclusive.
5. Reset each port to be tested:
 - a. At the **Hardware View**, double-click the UPM card for which ports are to be tested. The **Port Card View** displays.
 - b. At the **Port Card View**, right-click the tested port. A menu displays.
 - c. Choose **Reset Port**. A reset warning box displays.
 - d. Click **OK**. The port resets.
 - e. Click **Back To Full View** to return to the **Hardware View**.
6. Disconnect the fiber-optic jumper cable from the port to be tested. If a UPM card will be tested, disconnect all four fiber-optic jumper cables.



CAUTION: If name server zoning is implemented by port number, ensure fiber-optic cables that are disconnected to perform the loopback test are reconnected properly. A cable configuration change disrupts zone operation and may incorrectly include or exclude a device from a zone.

7. If the port to be tested is shortwave laser, insert a multimode loopback plug into the port receptacle. If the port to be tested is longwave laser, insert a singlemode loopback plug into the port receptacle. If an entire UPM card will be tested, insert an appropriate loopback plug in all four port receptacles.
8. Click **Maintenance** and choose **Port Diagnostics**. The **Port Diagnostics** dialog box displays, as shown in [Figure 3–15](#).
9. Select a port or UPM card for test:
 - To select an individual port for test, type the port number in the **Port Number** field.
 - To select a UPM card for test, type the port number of any of the four ports on the card in the **Port Number** field, then choose **All Ports On Card**.
10. At the **Diagnostics Test** list box, choose **External Loopback**.
11. Click **Next**. Beaconing initiates for the port or UPM card selected for test. At the **Hardware View**, a yellow triangle displays at the top of the UPM card. At the **Port Diagnostics** dialog box, the message `Loopback plugs must be installed on ports being diagnosed` displays.
12. Verify loopback plugs are installed and click **Next**. The message `Verify selected ports are beaconing` displays.
13. Verify beaconing is enabled, then click the **Next** button. The message `Press START TEST to begin diagnostics` displays, and **Next** changes to **Start Test**.
14. Click **Start Test**. The test begins and:
 - **Start Test** changes to **Stop Test**.
 - The message `Port xx: TEST RUNNING` displays, where `xx` is the port number. If a UPM card is tested, the message displays for all four ports.
 - A red progress bar (indicating percent completion) travels from left to right across the **Completion Status** field.

As an individual port is tested, the amber LED flashes (beacons) and the green LED illuminates (indicating loopback traffic through the port).

NOTE: Click **Stop Test** at any time to abort the loopback test.

15. When the test completes, test results display (for each port tested) as `Port xx: Passed!` or `Port xx: Failed!` in the message area of the dialog box. If a port fails the test, the amber LED for the port remains illuminated.
16. When finished, click **Cancel** to close the **Port Diagnostics** dialog box and return to the **Hardware View**. Beaconing is disabled for the port or UPM card.
17. Reset each tested port:
 - a. At the **Hardware View**, double-click the UPM card for which ports were tested. The **Port Card View** displays.
 - b. At the **Port Card View**, right-click the tested port. A menu displays.
 - c. Choose **Reset Port**. A reset warning message box displays.
 - d. Click **OK**. The port resets.
18. Remove loopback plugs from the tested ports.
19. Reconnect fiber-optic jumper cables from devices to tested ports.

Channel Wrap Test (S/390 only)

A channel wrap test is a diagnostic procedure that checks S/390 host-to-director link connectivity by returning the output of the host as input. The test is host-initiated, and transmits **ECHO** extended link service (ELS) command frames to a director port enabled for channel wrapping. The director port echoes the frames back to the host.

S/390 Only

To perform a channel wrap test for a director-attached host:

1. Notify the customer a disruptive channel wrap test will be performed on the host-to-director FICON link.
2. At the HAFM server, open the *HAFM* application. The **Products View** displays.
 - a. Double-click the icon representing the director for which the channel wrap test will be configured. The **Hardware View** for the selected director displays.

- b. At the **Hardware View**, verify the location of the port to be configured for the channel wrap test. When the mouse cursor is passed over a graphical UPM card on the front view of the director, the card highlights with a blue border and a pop-up displays with the following information:
 - Port card type (UPM).
 - Chassis slot number (**0** through **35**, slot **32** is for internal use only).
 - The four consecutive port numbers on the selected card. Valid port numbers are in the range of inclusive.
- c. Double-click the UPM card with the port to be configured. The **Port Card View** for the selected card displays.
- d. Right-click the port to be configured, then choose **Channel Wrap** from the menu. The **Channel Wrap On for Port n** (where **n** is the port number) window displays, as shown in [Figure 3–16](#).
- e. Click **OK** to enable channel wrapping for the port.



Figure 3–16: Channel Wrap On for Port *n* dialog box

3. Perform the Fibre Channel link test at the S/390 host attached to the configured port. For test instructions, refer to the service documentation delivered with the S/390 system.

Swapping Ports (S/390 only)

Use the port swap procedure to swap a device connection and logical port address from a failed Fibre Channel port to an operational port. Because both ports are blocked during the procedure, director communication with the attached device is momentarily disrupted.

S/390 Only

To perform the port swap procedure for a pair of director ports:

1. Notify the customer a port swap procedure will be performed and a fiber-optic cable or cables will be disconnected. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the ports and sets attached devices offline.
2. At the HAFM server, open the *HAFM* application. The **Products View** displays.
3. Double-click the icon representing the director for which the loopback test will be performed. The **Hardware View** for the selected director displays.
4. Click **Maintenance** and choose **Swap Ports**. The **Swap Ports** dialog box displays, as shown in [Figure 3–17](#).

Port Addresses

First address: (Hex) **U**nblock after swap

Second address: (Hex) **U**nblock after swap

Instructions

Enter the port addresses to be swapped, then press Next.

Figure 3–17: Swap Ports dialog box

5. At the **First address** and **Second address** fields, type the logical port addresses (in hexadecimal format) of the pair of ports to be swapped. The ports are automatically blocked during the procedure.
6. Choose the **Unblock after swap** check boxes to unblock the ports when the procedure completes.

7. Click **Next**. At the **Swap Ports** dialog box, the message Continuing this procedure requires varying the selected ports offline. Ask the system operator to vary the link(s) offline, then press **Next**. displays.
8. Click **Next**. At the **Swap Ports** dialog box, the message Move the port cable(s). Then press **Next**. displays.
9. Swap the fiber-optic jumper cables between the selected ports, then click **Next**.
10. At the **Swap Ports** dialog box, the message Ports swapped successfully. displays. Click **Next** to close the window and return to the **Hardware View**.

Collecting Maintenance Data

When director operational firmware detects a critical error or FRU failure, the director automatically copies the contents of dynamic random access memory (DRAM) to a dump area in FLASH memory on the active CTP card, then initiates a failover to the operational FRU. The director 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 **Products View** displays.
2. Double-click the icon representing the director for which the data collection procedure will be performed. The **Hardware View** for the selected director displays.
3. Click **Maintenance** and choose **Data Collection**. The **Save Data Collection** dialog box displays, as shown in [Figure 3-18](#).

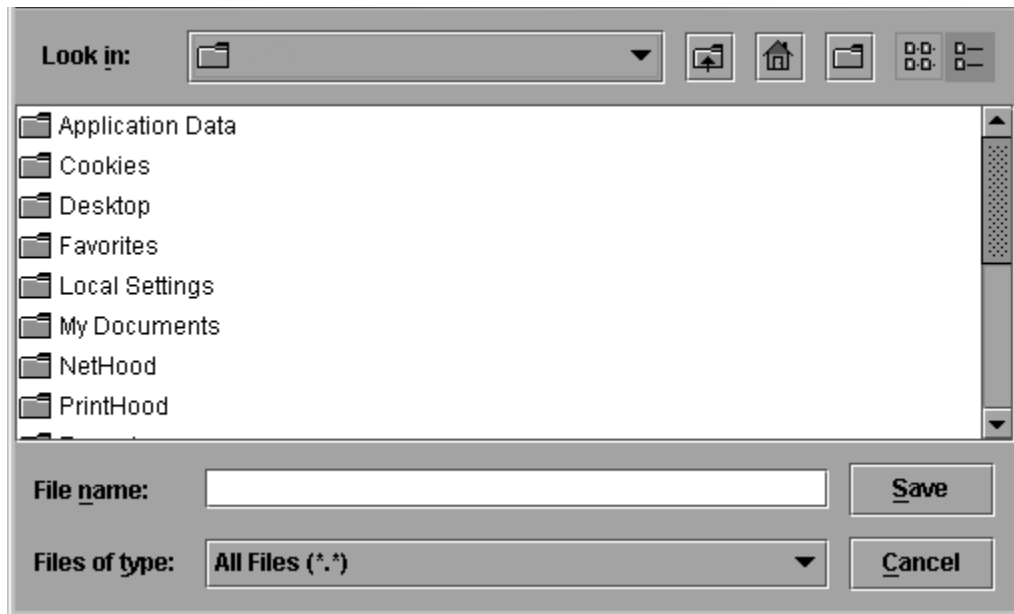


Figure 3-18: Save Data Collection dialog box

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 from the **Look in:** drop-down menu, then type a descriptive name for the collected maintenance data in the **File name** field. Ensure the file name has a *.zip* extension, then click **Save**.
6. A dialog box displays as shown in [Figure 3-19](#), with a progress bar that shows percent completion of the data collection process. When the process reaches 100%, **Cancel** changes to **Close**.

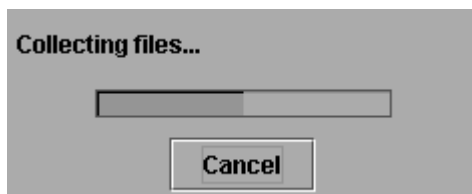


Figure 3-19: Data Collection dialog box

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 with the failed FRU to HP for failure analysis.
9. To ensure the *QuikSync* backup application operates normally, replace the original backup disk in the HAFM server Zip drive.

Clean Fiber-Optic Components

Perform this procedure as directed in this publication and when connecting or disconnecting fiber-optic cables from director UPM card connectors (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 port. Use compressed air to blow any contaminants from the connector, as shown in ❶ on [Figure 3–20](#).
 - a. Keep the air nozzle approximately 50 millimeters (two inches) from the end of the connector and hold the can upright.
 - b. Blow compressed air on the surfaces and end of the connector continuously for approximately five seconds.

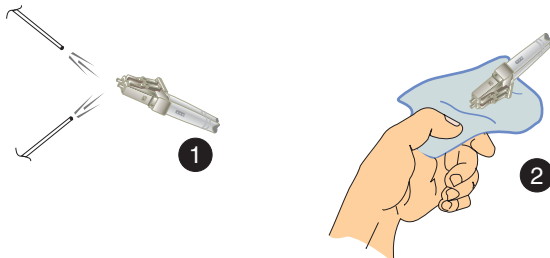


Figure 3–20: Clean Fiber-Optic components

3. Gently wipe the end-face and other surfaces of the connector with an alcohol pad, as shown in ❷ on [Figure 3–20](#). Ensure the pad makes full contact with the surface to be cleaned. Wait approximately five seconds for cleaned 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 director:

1. One alternating current (AC) power cord is required for each power supply installed. Ensure power cords connect facility power to the input power module at the bottom rear of the director. If two power cords are installed for high availability, plug the cords into separate facility power circuits.



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

2. At the bottom rear of the director, set the power switch (circuit breaker) to the up position. The director powers on and performs power-on self-tests (POSTs). During POSTs:
 - a. Amber LEDs on both CTP cards and all UPM cards illuminate momentarily.
 - b. The green LED on each CTP card (active and backup) illuminates as the card is tested and UPM cards are tested.
 - c. Green LEDs associated with Fibre Channel ports sequentially illuminate as the ports are tested.
3. After successful POST completion, the green power LED on the front bezel, green LED on the active CTP card, and green **PWR OK** LEDs on both power supplies remain illuminated.
4. If a POST error or other malfunction occurs, go to [MAP 0000: Start MAP on page 2-12](#) to isolate the problem.

NOTE: When powering on the director after removing and replacing a faulty FRU, the amber system error LED may remain illuminated. Clear the system error LED as part of the replacement procedure.

Power-Off Procedure

Powering the director off and on (performing a power cycle) resets all logic cards and executes POSTs. When performing a power cycle, wait approximately 30 seconds before switching power on.

NOTE: When the director is powered off, the operation of attached Fibre Channel devices is disrupted. Do not power off the director unless directed to do so by a procedural step or the next level of support.

To power-off the director:

1. Notify the customer the director will be powered off. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the director and sets attached devices offline.
2. Set the director offline ([Set Offline State on page 3–47](#)).
3. At the bottom rear of the director, set the power switch (circuit breaker) to the down position. The director powers off.
4. If servicing the director, disconnect power cords from the input power module at the bottom rear of the director. This step is not required when performing a power cycle.

IPL the Director

A director IPL should only be performed if failure of a CTP card is indicated. Do not IPL the director unless directed to do so by a procedural step or the next level of support. A director IPL performs the following functions:

- Resets the functional logic for the active CTP card only. An IPL does not reset the backup CTP card, SBAR cards, or UPM cards. All director switching operations continue unaffected.

NOTE: An initial machine load (IML) performs essentially the same functions, but resets both CTP cards. A director IML is initiated by pressing and holding the white IML button (on the faceplate of either CTP card) for three seconds.

- Loads firmware from the CTP card FLASH memory without cycling director power.
- Resets the Ethernet local area network (LAN) interface on the active CTP card, causing the connection to the HAFM server to drop momentarily until the connection automatically recovers.
- Automatically enables changes to an active zone configuration.
- Keeps all fabric logins, name server registrations, and operating parameters intact.
- Automatically sets the director online. The blocked or unblocked state of each port remains intact.

To IPL the director:

1. At the HAFM server, open the *HAFM* application. The **Products View** displays.
2. Double-click the icon representing the director to be IPLed. The **Hardware View** for the selected director displays.
3. Click **Maintenance** and choose **IPL**. The **Information** dialog box displays, as shown in [Figure 3–21](#).

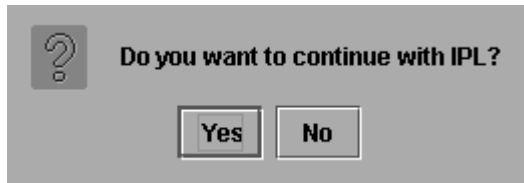


Figure 3–21: Information dialog box

4. Click **Yes** to IPL the director. During the IPL, the director-to-HAFM server Ethernet link drops momentarily and the following occur at the *Product Manager* application:
 - As the network connection drops, the Director 2/140 Status table turns yellow, the **Status** field displays **No Link**, and the **State** field displays a reason message.
 - In the **Products View**, the director icon displays a grey square, indicating director status is unknown.
 - Illustrated FRUs in the **Hardware View** disappear, and display again as the connection is reestablished.

Set the Director Online or Offline

This section describes procedures to set the director online or offline. These operating states are described as follows:

- **Online**—When the director is set online, an attached device can log in to the director if the port is not blocked. Attached devices can communicate with each other if they are configured in the same zone.
- **Offline**—When the director is set offline, all ports are set offline. The director transmits the offline sequence (OLS) to attached devices, and the devices cannot log in to the director.

NOTE: When the director is set offline, the operation of attached Fibre Channel devices is disrupted. Do not set the director offline unless directed to do so by a procedural step or the next level of support.

Set Online State

To set the director online:

1. At the HAFM server, open the *HAFM* application. The **Products View** displays.
2. Double-click the icon representing the director to be set online. The **Hardware View** for the selected director displays.
3. Click **Maintenance** and choose **Set Online State**. If the director is offline, the **Set Online State** dialog box displays, as shown in [Figure 3–22](#) indicating the state is **OFFLINE**.



Figure 3–22: Set Online State dialog box (offline)

4. Click **Set Online**. A **Warning** dialog box displays, indicating the director will be set online.
5. Click **OK**. As the director comes online, observe the *Product Manager* application. The **State** field of the Director 2/140 Status table displays **Online**.

Set Offline State

To set the director offline:

1. Notify the customer the director will be set offline. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the director and sets attached devices offline.
2. At the HAFM server, open the *HAFM* application. The **Products View** displays.
3. Double-click the icon representing the director to be set offline. The **Hardware View** for the selected director displays.
4. Click **Maintenance** and choose **Set Online State**. If the director is online, the **Set Online State** dialog box displays, as shown in [Figure 3–23](#) indicating the state is **ONLINE**.



Figure 3–23: Set Online State dialog box (online)

5. Click **Set Offline**. A **Warning** dialog box displays, indicating the director will be set offline.
6. Click **OK**. As the director goes offline:
 - The OLS sequence is transmitted to all attached devices.
 - At the *Product Manager* application, the **State** field of the Director 2/140 Status table displays **OFFLINE**.

Block and Unblock Ports

This section describes procedures to block or unblock director ports. An entire UPM card (four ports) can be blocked or unblocked, or ports can be blocked or unblocked on an individual basis. When a port is blocked, the port is automatically set offline. When a port is unblocked, the port is automatically set online.

NOTE: When a director port is blocked, the operation of an attached Fibre Channel device is disrupted. Do not block director ports unless directed to do so by a procedural step or the next level of support.

Block a Port

To block an individual director port:

1. 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.
2. At the HAFM server, open the *HAFM* application. The **Products View** displays.
3. Double-click the icon representing the director for which a port will be blocked. The **Hardware View** for the selected director displays.
4. Double-click the UPM card for which a port will be blocked. The **Port Card View** for the selected card displays.
5. Move the cursor over the port to be blocked and right-click the mouse to open a list of menu options.
6. Choose **Block Port**. The **Blocking Port** warning box displays, as shown in [Figure 3-24](#).



Figure 3-24: Blocking Port warning box

7. Click **OK**. The following occur to indicate the port is blocked (and offline):
 - The emulated green LED associated with the port extinguishes at the **Port Card View**.
 - The green LED associated with the port extinguishes at the director.
 - A check mark displays in the check box adjacent to the **Block Port** menu option.
8. Click **Back to Full View** to return to the **Hardware View**.

Block a UPM Card

To block all four ports on a director UPM card:

1. Notify the customer the UPM card will be blocked. Ensure the customer's system administrator quiets Fibre Channel frame traffic through the ports and sets attached devices offline.
2. At the HAFM server, open the *HAFM* application. The **Products View** displays.
3. Double-click the icon representing the director for which a UPM card will be blocked. The **Hardware View** for the selected director displays.
4. Double-click the UPM card to be blocked. The **Port Card View** for the selected card displays.
5. Move the cursor over the UPM card to be blocked (but not over an individual port) and right-click the mouse to open a list of menu options.
6. Choose **Block All Ports**. The **Block All Ports** dialog box displays, as shown in [Figure 3–25](#).

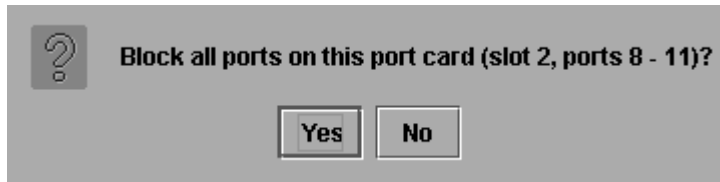


Figure 3–25: Block All Ports dialog box

7. Click **Yes**. The following occur to indicate the UPM card is blocked (and offline):
 - Emulated green LEDs associated with all four ports extinguish at the **Port Card View**.
 - Green LEDs associated with all four ports extinguish at the director.
8. Click **Back to Full View** to return to the **Hardware View**.

Unblock a Port

To unblock an individual director port:

1. At the HAFM server, open the *HAFM* application. The **Products View** displays.

2. Double-click the icon representing the director for which a port will be unblocked. The **Hardware View** for the selected director displays.
3. Double-click the UPM card for which a port will be unblocked. The **Port Card View** for the selected card displays.
4. Move the cursor over the port to be unblocked and right-click the mouse to open a list of menu options.
5. Choose **Block Port**. Note the check mark in the box adjacent to the menu item, indicating the port is blocked. The **Unblocking Port** warning box displays, as shown in [Figure 3–26](#).

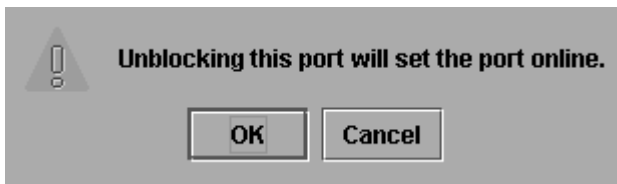


Figure 3–26: Unblocking Port warning box

6. Click **OK**. The following occur to indicate the port is unblocked (and online):
 - The emulated green LED associated with the port illuminates at the **Port Card View**.
 - The green LED associated with the port illuminates at the director.
 - The check box adjacent to the **Block Port** option becomes blank.
7. Click **Back to Full View** to return to the **Hardware View**.

Unblock a UPM Card

To unblock all four ports on a director UPM card:

1. At the HAFM server, open the *HAFM* application. The **Products View** displays.
2. Double-click the icon representing the director for which an UPM card will be unblocked. The **Hardware View** for the selected director displays.
3. Double-click the UPM card to be unblocked. The **Port Card View** for the selected card displays.
4. Move the cursor over the UPM card to be unblocked (but not over an individual port) and right-click the mouse to open a list of menu options.

5. Choose **Unlock All Ports**. The **Unlock All Ports** dialog box displays, as shown in [Figure 3-27](#).



Figure 3-27: Unlock All Ports dialog box

6. Click **Yes**. The following occur to indicate the UPM card is unblocked (and online):
 - Emulated green LEDs associated with all four ports illuminate at the **Port Card View**.
 - Green LEDs associated with all four ports illuminate at the director.
7. Click **Back to Full View** to return to the **Hardware View**.

Manage Firmware Versions

Firmware is the director's internal operating code that is downloaded from the HAFM server and stored on a CTP card. Up to eight versions can be stored on the HAFM server hard drive and made available for download to a director. Service personnel can perform the following firmware management tasks:

- Determine the firmware version active on a director.
- Add to and maintain a library of up to eight firmware versions on the HAFM server hard drive.
- Modify a firmware description stored on the HAFM server hard drive.
- Delete a firmware version from the HAFM server hard drive.
- Concurrently download a firmware version to a selected director.

Determine a Director Firmware Version

To determine a director firmware version:

1. At the HAFM server, open the *HAFM* application. The **Products View** displays.

2. Double-click the icon representing the switch to be inspected for firmware version. The **Hardware View** for the selected switch displays.
3. Click **Maintenance** and choose **Firmware Library**. The **Director 2/140 Firmware Library** dialog box displays, as shown in [Figure 3–28](#).

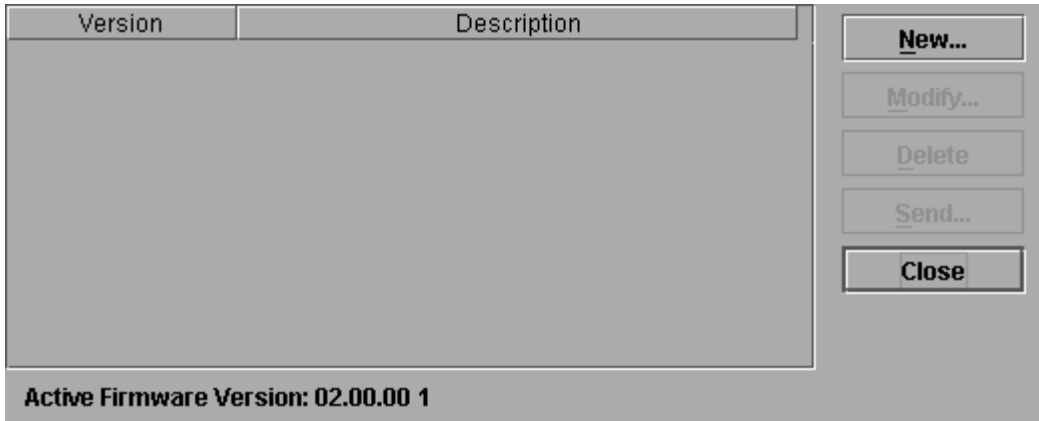


Figure 3–28: Firmware Library dialog box

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 director is provided on the *hp Director 2/140 documentation kit CD*. Subsequent firmware versions to upgrade the director are provided to customers through the HP website.

NOTE: When adding a firmware version, follow procedural information in Release Notes that accompany the firmware version. This information supplements information provided in this general procedure.

To add a director 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://h18006.www1.hp.com/storage/saninfrastructure.html>

NOTE: If required, obtain the customer-specific member name and password from the customer or next level of support.

- b. Follow links to HAFM software.
 - c. Click the **Director 2/140 Firmware Version XX.YY.ZZ** entry, where **XX.YY.ZZ** is the desired version. The **Windows 2000 Save As** dialog box displays.
 - 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 Zip disk, CD-ROM, or other electronic means.
2. At the HAFM server, open the *HAFM* application. The **Products View** displays.
 3. Double-click the icon representing the director to which the firmware version will be added. The **Hardware View** for the selected director displays.
 4. Click **Maintenance** and choose **Firmware Library**. The **Director 2/140 Firmware Library** dialog box displays.
 5. Click **New**. The **New Firmware Version** dialog box displays, as shown in [Figure 3–29](#).



Figure 3–29: 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 display in the **File name** field and click **Save**. The **New Firmware Description** dialog box displays, as shown in [Figure 3–30](#).



Figure 3–30: New Firmware Description dialog box

7. Enter a description (up to 24 characters in length) for the new firmware version and click **OK**. It is recommended the description include the installation date and text that uniquely identifies the firmware version.
8. A **Transfer Complete** message box displays 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 display in the **Director 2/140 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 director, see [Download a Firmware Version to a Director on page 3–56](#).

Modify a Firmware Version Description

To modify the description of a director firmware version in the library stored on the HAFM server hard drive:

1. At the HAFM server, open the *HAFM* application. The **Products View** displays.
2. Double-click the icon representing the director for which the firmware version description will be modified. The **Hardware View** for the selected director displays.
3. Click **Maintenance** and choose **Firmware Library**. The **Director 2/140 Firmware Library** dialog box displays.
4. Select the firmware version to be modified and click **Modify**. The **Modify Firmware Description** dialog box displays, as shown in [Figure 3–31](#).



Figure 3–31: Modify Firmware Description dialog box

5. Enter a modified description (up to 24 characters in length) for the firmware version and click **OK**. It is recommended the description include the installation date and text that uniquely identifies the firmware version.
6. The new description for the firmware version displays in the **Director 2/140 Firmware Library** dialog box. Click **Close** to close the dialog box and return to the *Product Manager* application.

Delete a Firmware Version

To delete a director firmware version from the library stored on the HAFM server hard drive:

1. At the HAFM server, open the *HAFM* application. The **Products View** displays.
2. Double-click the icon representing the director from which the firmware version will be deleted. The **Hardware View** for the selected director displays.
3. Click **Maintenance** and choose **Firmware Library**. The **Director 2/140 Firmware Library** dialog box displays.
4. Select the firmware version to be deleted and click **Delete**. A confirmation dialog box displays.
5. Click **OK**. The selected firmware version is deleted from the **Director 2/140 Firmware Library** dialog box.
6. Click **Close** to close the dialog box and return to the *Product Manager* application.

Download a Firmware Version to a Director

This procedure downloads a selected firmware version from the HAFM server library to a director managed by the open instance of the *Product Manager* application. The procedure applies to a director with two (redundant) CTP cards. The process occurs concurrently without taking the director offline or disrupting operation. The new firmware version takes effect when control is passed from the active to the backup CTP card. Although director operation is not affected, name server, alias server, and login server functions are momentarily unavailable during CTP card switchover.

NOTE: When downloading a firmware version, follow procedural information in release notes or EC instructions that accompany the firmware version. This information supplements information provided in this general procedure.

To download a firmware version to a director:

1. At the HAFM server, open the *HAFM* application. The **Products View** displays.
2. Before downloading firmware version **XX.YY.ZZ** to a director, ensure that the required version of the *HAFM* application as described in the firmware release notes is running on the HAFM server.
 - a. Select **About** from the **Help** menu. The **About** dialog box displays and lists 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 3–62](#)).
3. Double-click the icon representing the director to which the firmware version will be downloaded. The **Hardware View** for the selected director displays.
4. As a precaution to preserve director configuration information, perform the data collection procedure ([Collecting Maintenance Data on page 3–40](#)).
5. Click **Maintenance** and choose **Firmware Library**. The **Director 2/140 Firmware Library** dialog box displays.
6. Select the firmware version to be downloaded and click **Send**. The send function verifies existence of certain director conditions before the download process begins. If an error occurs, a message displays indicating the problem must be fixed before firmware is downloaded. Conditions that terminate the process include:
 - A redundant CTP card failure.
 - The firmware version is being installed to the director by another user.
 - The director-to-HAFM server link is down.

If a problem occurs and a corresponding message displays, go to [MAP 0000: Start MAP on page 2–12](#) to isolate the problem. If no error occurs, the **Send Firmware** confirmation box displays, as shown in [Figure 3–32](#).



Figure 3–32: Send Firmware dialog box

7. Click **Yes**. The **Send Firmware** dialog box displays.

As the download begins, a `Writing data to FLASH` message displays at the top of the dialog box, followed by a `Sending Files` message. This message remains as a progress bar travels across the dialog box to show percent completion of the download. The bar progresses to 50% when the last file is transmitted to the

first CTP card. The bar remains at the 50% point until the director performs an IPL (indicated by an IPLing message). During the IPL, the director-to-HAFM server link drops momentarily and the following occur at the Product Manager:

- As the network connection drops, the Director 2/140 Status table turns yellow, the **Status** field displays `No Link`, and the **State** field displays a reason message.
- In the **Products View**, the director icon displays a grey square, indicating director status is unknown.
- Illustrated FRUs in the **Hardware View** disappear, and display again as the connection is reestablished.

After the IPL, a `Synchronizing CTPs` message displays. This message remains as files are transmitted to the second CTP card and the progress bar travels across the dialog box to 100%. When the download reaches 100%, a `Send Firmware Complete` message displays, as shown in [Figure 3–33](#).

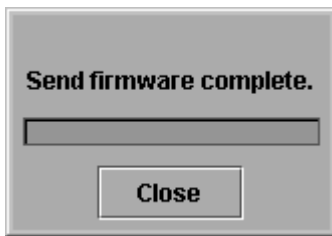


Figure 3–33: Send Firmware Complete dialog box

8. Click **Close** to close the dialog box.
9. Click **Close** to close the **Director 2/140 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 files stored in nonvolatile random-access memory (NV-RAM) on both director CTP cards. Configuration data in the file include:

- Identification data (director name, description, and location).
- Port configuration data (port names, blocked states, extended distance settings).

- Operating parameters (buffer-to-buffer credit (BB_Credit) value, error-detect time-out value (E_D_TOV), resource allocation time-out value (R_A_TOV), switch priority, and preferred domain ID).
- Simple network management protocol (SNMP) configuration information, including trap recipients, community names, and write authorizations.
- Zoning configuration information, including the active zone set and default zone state.

The backup file is not required in a redundant director, however the feature is available and may be useful to save a special-purpose configuration for test. The director must be set offline prior to restoring or resetting the configuration file.

Backup the Configuration

To backup the director configuration file to the HAFM server:

1. At the HAFM server, open the *HAFM* application. The **Products View** displays.
2. Double-click the icon representing the director for which the configuration file will be backed up. The **Hardware View** for the selected director displays.
3. Click **Maintenance** and choose **Backup & Restore Configuration**. The **Backup and Restore Configuration** dialog box displays, as shown in [Figure 3-34](#).



Figure 3-34: Backup and Restore Configuration dialog box

4. Click **Backup**. When the backup process finishes, the **Backup Complete** dialog box displays, as shown in [Figure 3-35](#).



Figure 3–35: Backup Complete dialog box

5. Click **OK** to close the dialog box and return to the **Hardware View**.

Restore the Configuration

To restore the director configuration file from the HAFM server:

1. Notify the customer the director will be set offline. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the director and sets attached devices offline.
2. Set the director offline ([Set Offline State on page 3–47](#)).
3. At the HAFM server, open the *HAFM* application. The **Products View** displays.
4. Double-click the icon representing the director for which the configuration file will be restored. The **Hardware View** for the selected director displays.
5. Click **Maintenance** and choose **Backup & Restore Configuration**. The **Backup and Restore Configuration** dialog box displays, as shown in [Figure 3–36](#).



Figure 3–36: Backup and Restore Configuration dialog box

6. Click **Restore**. A **Warning** message box displays, as shown in [Figure 3–37](#).

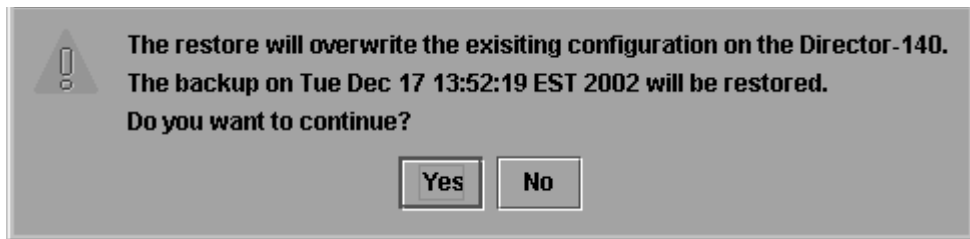


Figure 3–37: Warning dialog box

7. Click **Yes**. When the restore process finishes, the **Restore Complete** dialog box displays, as shown in [Figure 3–38](#).

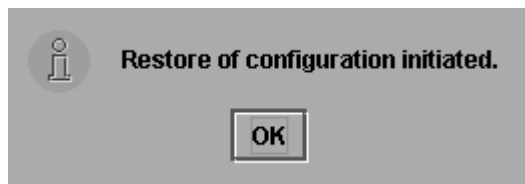


Figure 3–38: Restore Complete dialog box

8. Click **OK** to close the dialog box and return to the **Hardware View**.

Reset Configuration Data

NOTE: This procedure resets the director IP address to the default value of **10.1.1.10** and may disrupt HAFM server-to-director communication. All configured feature (PFE) keys must be re-entered.

To reset director data to the factory default settings:

1. Notify the customer the director will be set offline. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the director and sets attached devices offline.
2. Set the director offline ([Set Offline State on page 3–47](#)).
3. At the HAFM server, open the *HAFM* application. The **Products View** displays.
4. Double-click the icon representing the director for which the configuration file will be reset to factory default settings. The **Hardware View** for the selected director displays.
5. Click **Maintenance** and choose **Reset Configuration**. The **Reset Configuration** dialog box displays, as shown in [Figure 3–39](#).



Figure 3–39: Reset Configuration dialog box

6. Click **Reset**. When the process completes, the dialog box closes and the application returns to the **Hardware View**.

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 Director 2/140 Product Manager and HAFM Services applications.

The *HAFM* application shipped with the director is provided on the HAFM Applications CD-ROM. Subsequent software versions for upgrading the director are provided to customers through the HAFM Applications CD-ROM or through the HP website.

NOTE: When installing or upgrading a software version, follow all procedural information in Release Notes that accompany the software version. This information supplements information provided 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).
2. Obtain the new software 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://h18006.www1.hp.com/storage/saninfrastructure.html>

NOTE: If required, obtain the customer-specific member name and password from the customer or next level of support.

- b. Follow links to HAFM software.

- c. Click the **HAFM Software Version XX.YY.ZZ** entry, where **XX.YY.ZZ** is the desired version. The **Windows 2000 Save As** dialog box displays.
 - 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 HAFM version is downloaded and saved to the HAFM server or PC hard drive.
 - e. If the new HAFM version was downloaded to a PC (not the HAFM server), transfer the HAFM software version file to the HAFM server by CD-ROM or other electronic means.
3. Choose **Start > Run**. The **Run** dialog box displays, as shown in [Figure 3–40](#).

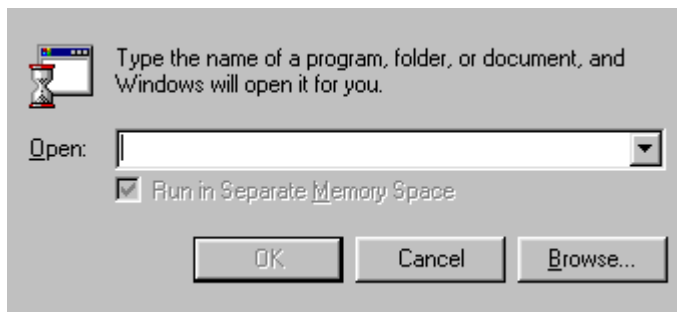


Figure 3–40: Run dialog box

4. At the **Run** dialog box, select the directory path (hard drive or CD-ROM drive) and filename of the executable file (*HAFM_SERVERINSTALL.EXE*) using **Browse**. The directory path and filename display in the **Open** field.
5. Click **OK**. A series of message boxes display as the *InstallAnywhere* application as shown in [Figure 3–41](#), prepares to install the *HAFM* application software, followed by the **HP StorageWorks HA-Fabric Manager** dialog box.



Figure 3–41: InstallAnywhere dialog box (Introduction)

6. Follow the online instructions for the *InstallAnywhere* program. Click **Next**, **Install**, or **Done** as appropriate.
7. Power off and reboot the HAFM server.
 - a. Simultaneously press **Ctrl + Alt + Delete** to display the **Windows 2000 Logon Information** dialog box.
 - b. Type the user name and password and click **OK**. The **Windows 2000** desktop displays.

NOTE: If required, obtain the user name and password from the customer or next level of support.
8. The *HAFM* application automatically opens. At the **HAFM Login** window, enter a user name, password, and HAFM server name (all are case sensitive), and click **Login**. The application opens and the **Products View** displays.

NOTE: If required, obtain the user name, password, and HAFM server name from the customer or next level of support.

FRU Removal and Replacement

This chapter describes removal and replacement procedures (RRPs) used by authorized service representatives for all director field-replaceable units (FRUs). Do not perform a procedure in this chapter until a failure is isolated to a FRU. If fault isolation was not performed, go to [MAP 0000: Start MAP on page 2–12](#).

Factory Defaults

[Table 4–1](#) lists the defaults for the passwords, and IP, subnet, and gateway addresses.

Table 4–1: 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 as applicable. The notes do not necessarily apply to all procedures in the chapter.

1. Before performing a FRU repair, read the removal and replacement procedures for that FRU carefully and thoroughly to familiarize yourself with the procedures and reduce the possibility of problems or customer down time.
2. When performing procedures described in this chapter, follow all electrostatic discharge (ESD) procedures, **WARNING** and **CAUTION** statements, and statements listed in the preface of this manual.

3. After completing the 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.
4. After completing a replacement procedure, clear the event code reporting the failure and the event code reporting the recovery from the Director 2/140 Event Log (at the HAFM server), and extinguish the amber system error light-emitting diode (LED) at the director front bezel.

Removing and Replacing FRUs

This section describes procedures to remove and replace director FRUs, along with a list of tools required to perform each procedure. In addition, the section provides:

- ESD information.
- A list of concurrent FRUs.
- A list of nonconcurrent FRUs.

See Chapter 5, [Illustrated Parts Breakdown](#) for FRU locations and part numbers.

ESD Information

When performing procedures described in this section, follow all ESD procedures, **WARNING** statements, and **CAUTION** statements. When removing and replacing FRUs, connect a grounding cable to the director chassis and wear an ESD wrist strap.



CAUTION: To avoid causing machine errors or damage while working on the director, follow ESD procedures by connecting a grounding cable to the director chassis and wearing an ESD wrist strap.

The ESD grounding points for the front of the chassis (ⓘ) are located at the right and left sides of the chassis, as shown in [Figure 4-1](#). Touch the chassis once before performing any maintenance action, and once each minute while removing or replacing FRUs. If the director is not connected to facility power (and therefore not grounded), connect the ESD wrist strap to an approved bench grounding point instead of the chassis. The ESD grounding point for the rear of the chassis (ⓘ) is located next to the maintenance port, as shown in [Figure 4-1](#). Touch the chassis once before performing any maintenance action, and once each minute while removing or replacing FRUs.

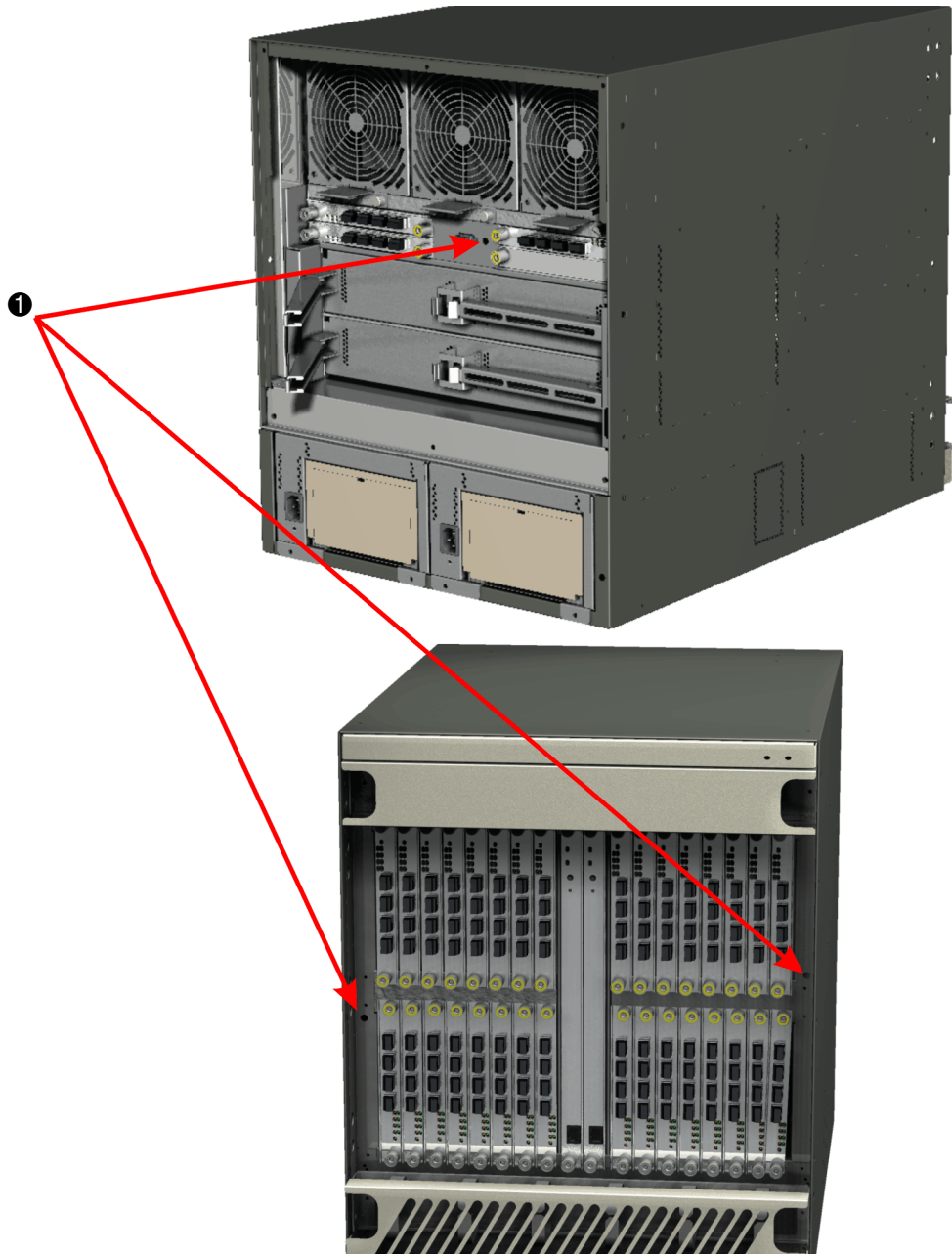


Figure 4-1: ESD grounding points

Concurrent FRUs

Table 4–2 lists concurrent FRUs. Concurrent FRUs are removed and replaced while the director is powered on and operational. The table also lists ESD precautions (yes or no) for each FRU and provides hyperlinks to the removal and replacement procedure.

Table 4–2: Concurrent FRU Names and ESD Requirements

Concurrent FRU Name	ESD Precaution Requirement
Control processor card (RRP: Redundant CTP Card on page 4-5)	Yes
Universal port module card (RRP: UPM Card on page 4-9)	Yes
Small form factor pluggable (SFP) optical transceiver (RRP: SFP Optical Transceiver on page 4-14)	No
UPM filler blank (RRP: UPM Filler Blank on page 4-17)	No
Power supply (RRP: Redundant Power Supply on page 4-19)	Yes
AC module (RRP: AC Module on page 4-21)	Yes
Power/System Error LED assembly (RRP: Power Module Assembly on page 4-30)	Yes
Serial crossbar assembly (RRP: Redundant SBAR Assembly on page 4-24)	Yes
Fan module (RRP: Redundant Fan Module on page 4-27)	Yes

Nonconcurrent FRUs

[Table 4–3](#) lists nonconcurrent FRUs. Nonconcurrent FRUs are removed and replaced after the director is powered off. The table also lists ESD precautions (yes or no) for each FRU, and references the page number of the removal and replacement procedure.

Table 4–3: Nonconcurrent FRU Names and ESD Precautions

Nonconcurrent FRU Name	ESD Precaution Requirement
Power module assembly (RRP: Power Module Assembly on page 4-30)	Yes
Backplane (RRP: Backplane on page 4-32)	Yes

RRP: Redundant CTP Card

Use the following procedures to remove or replace a redundant CTP card (two cards in the director) with the backup CTP card operational. A list of tools required is provided.



CAUTION: Do not remove and replace a redundant CTP card if the backup CTP card is not fully operational and director power is on. The director IP address, configuration data, and other operating parameters will be lost.

Tools Required

The following tools are required to perform these procedures.

- ESD grounding cable and wrist strap.
- Torque tool and hex adapter (provided with the director).

Removing the CTP Card

To remove a redundant CTP card:

1. If the director is installed in a stand-alone configuration, go to [step 2](#). If the director is rack-mounted, unlock and open the cabinet front door as directed by the HP authorized service provider.
2. Follow ESD procedures by attaching a wrist strap to the director chassis and your wrist, as shown in [Figure 4–1](#).



CAUTION: To avoid causing machine errors or damage while working on the director, follow ESD procedures by connecting a grounding cable to the director chassis and wearing an ESD wrist strap.

3. Identify the defective CTP card from the amber LED on the card or failure information at the HAFM server's **Hardware View**.
 4. Disconnect the Ethernet local area network (LAN) cable from the RJ-45 connector on the card faceplate.
 5. The CTP card is secured to the director chassis with two captive Allen screws. The bottom screw is spring-loaded and locks the CTP card in place. The top screw cams the CTP card into and out of the backplane.
-



CAUTION: The torque tool supplied with the director is designed to tighten director logic cards and is set to release at a torque value of six inch-pounds. Do not use an Allen wrench or torque tool designed for use with another HP product. Use of the wrong tool may overtighten and damage logic cards.

- a. Insert the torque tool into the locking Allen screw at the bottom of the card. Turn the screw counterclockwise until the spring releases and the tool turns freely.
- b. Insert the torque tool(❶) into the cam Allen screw at the top of the card(❷). To unseat the CTP card and cam it out of the backplane, turn the screw counterclockwise until the tool turns freely, as shown in [Figure 4-2](#).

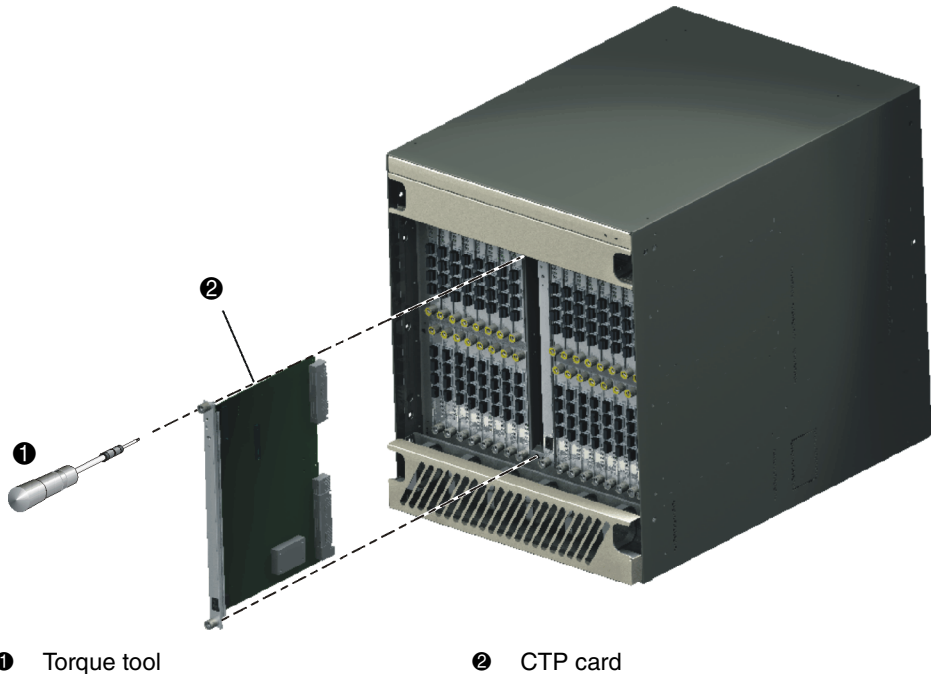


Figure 4–2: CTP card removal and replacement

6. Pull the CTP card from its card track and remove it from the director chassis. Place the card in an antistatic bag to provide ESD protection.

Replacing the CTP Card

To replace a redundant CTP card:

1. Wait approximately 20 seconds after removal of the failed CTP card to begin this replacement procedure.
2. Remove the replacement card from its protective antistatic bag.
3. Hold the card by its stiffener and insert it in the chassis card track, as shown in [Figure 4–2](#). The label identifying the card should be at the top. Verify the card is aligned in the card tracks, then slide it forward until it makes contact with the backplane.

4. Secure the CTP card:
 - a. Insert the torque tool into the cam Allen screw at the top of the card. Turn the torque tool clockwise until you feel it release and hear a clicking sound. As the screw turns clockwise, the card cams into the backplane connector.
 - b. Insert the torque tool into the locking Allen screw at the bottom of the card. Turn the torque tool clockwise until you feel it release and hear a clicking sound. As the screw turns clockwise, the card locks into place.
 - c. Verify the card stiffener is flush with the front of the card cage and even with other director logic cards.
5. After the replacement CTP card is installed, note the following:
 - When a CTP card with a different firmware version is installed in a director with an active CTP card, a synchronization process occurs. This process causes firmware from the active CTP card to be downloaded to the replacement CTP card. The process does not occur if both CTP cards have the same firmware version.
 - The synchronization process may take up to ten minutes (depending on director activity).



CAUTION: Allow the synchronization process to complete. If the process is interrupted by a director power cycle or initial program load (IPL), or by removing the replacement CTP card, the card may be unusable due to partially-loaded firmware.

- If after ten minutes the replacement CTP card is not operational, perform the data collection procedure and return the failed replacement card to HP ([Collecting Maintenance Data on page 3–40](#)).
 - Do not reinstall the failed replacement CTP card because this can corrupt director firmware. Obtain a new CTP card and perform this replacement procedure.
6. Verify that synchronization is complete by viewing the **Event Log**.
 7. Connect the Ethernet LAN cable to the RJ-45 connector on the faceplate of the replacement CTP card.
 8. Disconnect the ESD wrist strap from the director chassis and your wrist.
 9. Inspect the CTP card to ensure the amber LED is extinguished. If the amber LED is illuminated, go to [MAP 0000: Start MAP on page 2–12](#) to isolate the problem.

10. At the HAFM server's **Hardware View**, click **Logs** and choose **Event Log**. The **Event Log** displays. Ensure the following event codes display in the log:

- **410**-CTP card reset.
- **416**-Backup CTP installed.
- **422**-CTP firmware synchronization complete (only if the firmware versions on the two CTP cards are different).

If the event codes do not display in the log, go to [MAP 0000: Start MAP on page 2–12](#) to isolate the problem.

11. At the **Hardware View**, observe the graphic representing the replacement card and ensure no alert symbols display that indicate a failure (yellow triangle or red diamond). If a problem is indicated, go to [MAP 0000: Start MAP on page 2–12](#) to isolate the problem.

12. At the **Hardware View**, double-click the graphic representing the replacement card to open the **FRU Properties** dialog box. Verify that CTP card information (FRU name, position, and state) is correct. If a problem is indicated, go to [MAP 0000: Start MAP on page 2–12](#) to isolate the problem.

13. If necessary, close and lock the equipment cabinet door.

14. Perform the data collection procedure ([Collecting Maintenance Data on page 3–40](#)).

15. If the customer requests the replacement CTP card be set as the active card, perform a FRU switchover. At the **Hardware View**, right-click the graphic representing the replacement card to open a menu, then choose **Switchover**.

16. Clear the amber system error LED on the director bezel:

- a. At the **Hardware View**, right-click the front panel bezel graphic (away from a FRU) to open a menu.
- b. Click **Clear System Error Light**.

RRP: UPM Card

Use the following procedures to remove or replace a UPM card. A list of tools required is provided.

Tools Required

The following tools are required to perform these procedures.

- ESD grounding cable and wrist strap.
- Torque tool and hex adapter (provided with the director).
- Fiber-optic protective plugs (provided with the director).
- Protective caps (provided with fiber-optic jumper cables).
- Fiber-optic cleaning kit.

Removing the UPM Card

To remove a UPM card:

1. Notify the customer that all ports on the defective UPM card will be blocked. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through any operational ports on the card and sets attached devices offline.
2. If the director is installed in a stand-alone configuration, go to [step 3](#). If the director is rack-mounted, unlock and open the cabinet front door as directed by the HP authorized service provider.
3. Follow ESD procedures by attaching a wrist strap to the director chassis and your wrist, as shown in [Figure 4-1](#).



CAUTION: To avoid causing machine errors or damage while working on the director, follow ESD procedures by connecting a grounding cable to the director chassis and wearing an ESD wrist strap.

4. Identify the defective UPM card from the amber LED on the card or failure information at the HAFM server's **Hardware View**.
5. Block communication to the defective UPM card ([Block a UPM Card on page 3-49](#)).
6. Disconnect the fiber-optic jumper cable from each port on the defective card. Repeat this step for all four ports.
 - a. Pull the keyed LC connector free from the port's optical transceiver.
 - b. Place a protective cap over the cable connector. If required, label jumper cables to ensure correct connections when the UPM card is replaced.

NOTE: If name server zoning is implemented by port number, a change to the director fiber-optic cable configuration disrupts zone operation and may incorrectly include or exclude a device from a zone.

- c. Insert a protective plug into the optical transceiver.



CAUTION: When fiber-optic cables are disconnected from UPM card optical transceivers, ensure protective plugs are inserted into the receptacles. This prevents damage to sensitive components and prevents injury to the eye if the laser is viewed directly.

7. The UPM card is secured to the director chassis with two captive Allen screws. One screw (yellow) is spring-loaded and locks the UPM card in place. The other screw (uncolored) cams the UPM card into and out of the backplane.



CAUTION: The torque tool supplied with the Director 2/140 is designed to tighten director logic cards and is set to release at a torque value of six inch-pounds. Do not use an Allen wrench or torque tool designed for use with another HP product. Use of the wrong tool may overtighten and damage logic cards.

- a. Insert the torque tool into the locking Allen screw (yellow). Turn the screw counter-clockwise until the spring releases and the tool turns freely.
 - b. Insert the torque tool (❶) into the cam Allen screw (❷ uncolored). To unseat the UPM card and cam it out of the backplane, turn the screw counterclockwise until the tool turns freely, as shown in [Figure 4-3](#).
8. Pull the UPM card from its card track and remove it from the director chassis. Place the card in an antistatic bag to provide ESD protection.

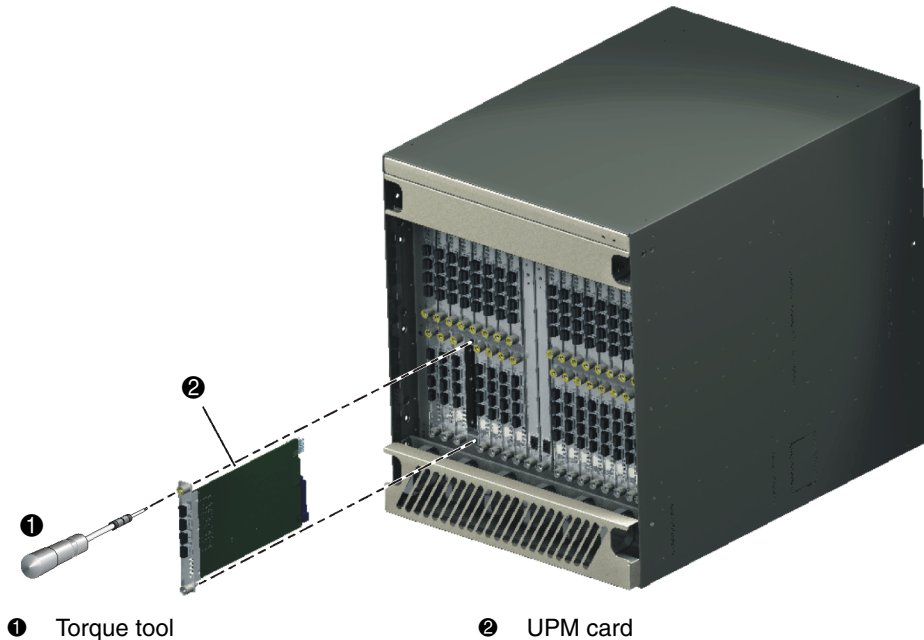


Figure 4-3: UPM card removal and replacement

Replacing the UPM Card

To replace a UPM card:

1. Remove the replacement card from its protective antistatic bag.
2. Hold the card by its stiffener and insert it in the chassis card track, as shown in [Figure 4-3](#). The label identifying the card should be at the top. Verify the card is aligned in the card tracks, then slide it forward until it makes contact with the backplane.
3. Secure the UPM card:
 - a. Insert the torque tool into the cam Allen screw (uncolored). Turn the torque tool clockwise until you feel it release and hear a clicking sound. As the screw turns clockwise, the card cams into the backplane connector.
 - b. Insert the torque tool into the locking Allen screw (yellow). Turn the torque tool clockwise until you feel it release and hear a clicking sound. As the screw turns clockwise, the card locks into place.

- c. Verify the card stiffener is flush with the front of the card cage and even with other director logic cards.
4. Perform an external loopback test for all ports on the replacement UPM card ([External Loopback Test on page 3–35](#)). If the test fails, go to [MAP 0000: Start MAP on page 2–12](#) to isolate the problem.
5. Reconnect a fiber-optic jumper cable to each port on the card. Inspect the label on the jumper cable to ensure the correct connection. Repeat this step for all four ports.
 - 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 cable and port connectors ([Clean Fiber-Optic Components on page 3–42](#)).
 - c. Insert the keyed LC cable connector into the port's optical transceiver.
6. Disconnect the ESD wrist strap from the director chassis and your wrist.
7. Inspect the UPM card to ensure all amber LEDs are extinguished. If any amber LEDs are illuminated, go to [MAP 0000: Start MAP on page 2–12](#) to isolate the problem.
8. At the HAFM server's **Hardware View**, click **Logs** and choose **Event Log**. The **Event Log** displays. Ensure the following event codes display in the log:
 - **500**-Port card hot-insertion initiated.
 - **501**-Port card has been recognized.If an event code **501** does not display in the log, go to [MAP 0000: Start MAP on page 2–12](#) to isolate the problem.
9. At the **Hardware View**, double-click the graphic representing the replacement card to open the **Port Card View**. At the **Port Card View**:
 - a. Ensure no alert symbols display that indicate a failure (yellow triangle or red diamond).
 - b. Verify UPM card information (FRU name, position, and state) is correct.

If a problem is indicated, go to [MAP 0000: Start MAP on page 2–12](#) to isolate the problem.
10. If necessary, close and lock the equipment cabinet door.

11. Restore communication to the replacement UPM card and set the card online as directed by the customer ([Unblock a UPM Card on page 3–50](#)). Inform the customer the UPM card is available for use.
12. Perform the data collection procedure ([Collecting Maintenance Data on page 3–40](#)).
13. Clear the amber system error LED on the director bezel:
 - a. At the **Hardware View**, right-click the front panel bezel graphic (away from a FRU) to open a menu.
 - b. Click **Clear System Error Light**.

RRP: SFP Optical Transceiver

Use the following procedures to remove or replace an SFP optical transceiver from a UPM card. A list of tools required is provided.

Tools Required

The following tools are required to perform these procedures.

- Fiber-optic protective plug (provided with the director).
- Protective cap (provided with the fiber-optic jumper cable).
- Fiber-optic cleaning kit.

Removing the SFP Optical Transceiver

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. If the director is installed in a stand-alone configuration, go to [step 3](#). If the director is rack-mounted, unlock and open the cabinet front door as directed by the HP authorized service provider.
3. Identify the defective port transceiver from the amber LED on the UPM card or failure information at the HAFM server's **Port Card View**.
4. Block communication to the port ([Block a Port on page 3–48](#)).

5. Disconnect the fiber-optic jumper cable from the port:
 - a. Pull the keyed LC free from the port's optical transceiver.
 - b. Place a protective cap over the cable connector.
6. Depending on the manufacturer, the optical transceiver may have a locking mechanism to secure the transceiver in the port receptacle, or the transceiver may have a pull tab to assist in removal.
 - a. If required, disengage the locking mechanism by squeezing the mechanism or pushing it toward the port receptacle.
 - b. Grasp the pull tab or the optical transceiver frame and pull the transceiver (❶) from the port receptacle, as shown in [Figure 4-4](#).

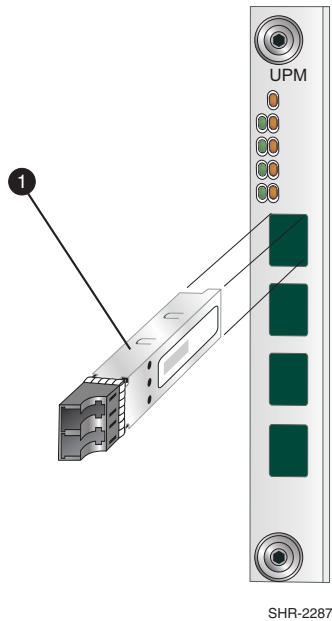


Figure 4-4: SFP optical transceiver removal and replacement

Replacing the SFP Optical Transceiver

To replace an SFP optical transceiver:

1. Remove the transceiver from its packaging.

2. Insert the transceiver into the port receptacle, as shown in [Figure 4-4](#).
3. Perform an external loopback test for the port ([External Loopback Test on page 3-35](#)). If the test fails, go to [MAP 0000: Start MAP on page 2-12](#) 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 cable and port connectors ([Clean Fiber-Optic Components on page 3-42](#)).
 - c. Insert the keyed LC cable connector into port's optical transceiver.
5. Inspect the UPM card with the replacement port transceiver to ensure all amber LEDs are extinguished. If any amber LEDs are illuminated, go to [MAP 0000: Start MAP on page 2-12](#) to isolate the problem.
6. At the HAFM server's **Hardware View**, click **Logs** and choose **Event Log**. The **Event Log** displays. Ensure an event code **510** (SFP optics card hot-insertion initiated) displays in the log.

If an event code **510** does not display in the log, go to [MAP 0000: Start MAP on page 2-12](#) to isolate the problem.
7. At the **Hardware View**, double-click the graphic representing the UPM card with the replacement transceiver to open the **Port Card View**. At the **Port Card View**:
 - a. Ensure no alert symbols display that indicate a port failure (yellow triangle or red diamond).
 - b. Double-click the port with the replacement transceiver to open the **Port Properties** dialog box. Verify port information is correct.
 - c. Right-click the port with the replacement transceiver and choose **Port Technology** option the menu. The **Port Technology** dialog box displays. Verify port technology information is correct.

If a problem is indicated, go to [MAP 0000: Start MAP on page 2-12](#) to isolate the problem.
8. If necessary, close and lock the equipment cabinet door.

9. Restore communication to the port with the replacement transceiver as directed by the customer ([Unblock a Port on page 3–49](#)). Inform the customer the port is available for use.
10. Clear the amber system error LED on the director bezel:
 - a. At the **Hardware View**, right-click the front panel bezel graphic (away from a FRU) to open a menu.
 - b. Click **Clear System Error Light**.

RRP: UPM Filler Blank

Use the following procedures to remove or replace a UPM filler blank. Filler blanks cover and protect unused UPM card slots in the director chassis. A list of tools required is provided.

Tools Required

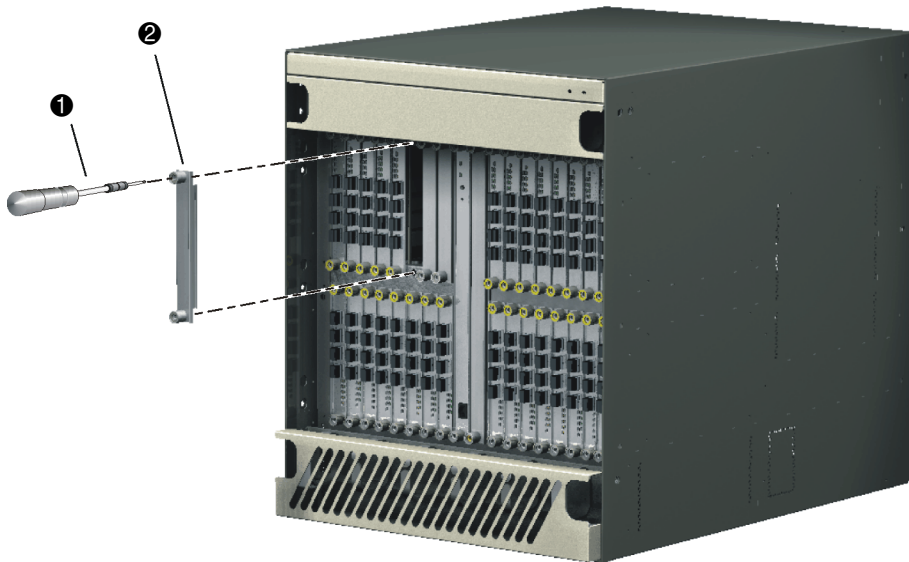
The following tool is required to perform these procedures.

- Torque tool and hex adapter (provided with the director).

Removing the Filler Blank

To remove a filler blank:

1. If the director is installed in a stand-alone configuration, go to [step 2](#). If the director is rack-mounted, unlock and open the cabinet front door as directed by the HP authorized service provider.
2. Identify the filler blank to be removed.
3. The filler blank is secured to the director chassis with two captive Allen screws. Both screws are spring-loaded to lock the filler blank in place.
4. Insert the torque tool (❶) into each locking Allen screw in the filler blank (❷). Turn each screw counterclockwise until the spring releases and the tool turns freely, as shown in [Figure 4–5](#).
5. Pull the filler blank out and remove it from the director chassis.



❶ Torque tool

❷ UPM filler blank

Figure 4-5: UPM filler blank removal and replacement

Replacing the Filler Blank

To replace a filler blank:

1. Remove the filler blank from its packaging.
2. Hold the filler blank by its stiffener and insert it in the chassis card track, as shown in [Figure 4-5](#).
3. To secure the filler blank, sequentially insert the torque tool into each locking Allen screw. Turn each screw clockwise until you feel the torque tool release and hear a clicking sound. As each screw turns clockwise, the filler blank locks into place.
4. Verify the filler blank stiffener is flush with the front of the card cage and even with other director logic cards.
5. If necessary, close and lock the equipment cabinet door.

RRP: Redundant Power Supply

Use the following procedures to remove or replace a redundant power supply. A list of tools required is provided.

Tools Required

The following tool is required to perform these procedures.

- ESD grounding cable and wrist strap.

Removing the Power Supply

To remove a redundant power supply:

1. If the director is installed in a stand-alone configuration, go to [step 2](#). If the director is rack-mounted, unlock and open the cabinet front door as directed by the HP authorized service provider.
2. Follow ESD procedures by attaching a wrist strap to the director chassis and your wrist, as shown in [Figure 4-1](#).



CAUTION: To avoid causing machine errors or damage while working on the director, follow ESD procedures by connecting a grounding cable to the director chassis and wearing an ESD wrist strap.

3. Identify the defective power supply from the extinguished green **PWR OK** LED on the supply or failure information at the HAFM server's **Hardware View**.
4. Use a flat-tip screwdriver to release the handle at the top of the power supply.
5. Pull the power supply (❶) from the director AC module (❷), as shown in [Figure 4-6](#). Support the power supply with one hand.
6. Place the power supply in an anti-static bag to provide ESD protection.

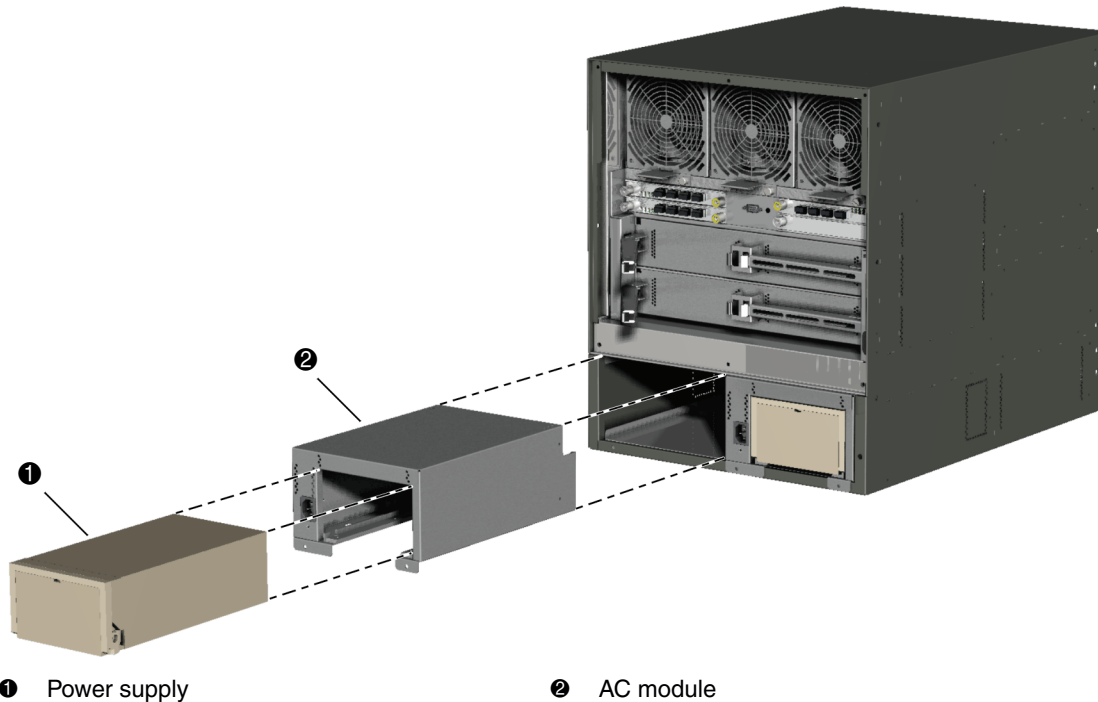


Figure 4–6: Redundant power supply removal and replacement

Replacing the Power Supply

To replace a redundant power supply:

1. Remove the replacement power supply from its protective antistatic bag.
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. Insert the power supply into the chassis guide of the AC module, then push the power supply toward the backplane to engage the connector pins.
4. Disconnect the ESD wrist strap from the director chassis and your wrist.
5. Inspect the power supply to ensure the green **PWR OK** LED is illuminated and all amber LEDs are extinguished. If a problem is indicated, go to [MAP 0000: Start MAP on page 2–12](#) to isolate the problem.

6. At the HAFM server's **Hardware View**, click **Logs** and choose **Event Log**. The **Event Log** displays. Ensure an event code **207** (power supply installed) displays in the log.

If an event code **207** does not display in the log, go to [MAP 0000: Start MAP on page 2–12](#) to isolate the problem.
7. At the **Hardware View**, observe the graphic representing the replacement power supply and ensure no alert symbols display that indicate a failure (yellow triangle or red diamond). If a problem is indicated, go to [MAP 0000: Start MAP on page 2–12](#) to isolate the problem.
8. At the **Hardware View**, double-click the graphic representing the replacement power supply to open the **FRU Properties** dialog box. Verify that information (FRU name, position, and state) is correct. If a problem is indicated, go to [MAP 0000: Start MAP on page 2–12](#) to isolate the problem.
9. Perform the data collection procedure ([Collecting Maintenance Data on page 3–40](#)).
10. Clear the amber system error LED on the director bezel:
 - a. At the **Hardware View**, right-click the front panel bezel graphic (away from a FRU) to open a menu.
 - b. Click **Clear System Error Light**.
11. If necessary, close and lock the equipment cabinet door.

RRP: AC Module

Use the following procedures to remove or replace the AC module. A list of tools required is provided.

Tools Required

The following tools are required to perform these procedures.

- Standard cross-tip (Phillips) screwdriver.
- ESD grounding cable and wrist strap.

Removing the AC Module

To remove the AC module:

1. If the director is installed in a stand-alone configuration, go to [step 2](#). If the director is rack-mounted, unlock and open the cabinet front door as directed by the HP authorized service provider.
2. Follow ESD procedures by attaching a wrist strap to the director chassis and your wrist, as shown in [Figure 4-1](#).



WARNING: Ensure the power cord is disconnected from the defective AC module.



CAUTION: To avoid causing machine errors or damage while working on the director, follow ESD procedures by connecting a grounding cable to the director chassis and wearing an ESD wrist strap.

3. Identify the defective AC module from the extinguished green **PWR OK** LED on the supply or failure information at the HAFM server's **Hardware View**.
4. Remove the power supply from the defective AC module ([RRP: Redundant Power Supply on page 4-19](#)).
5. Remove the two panhead Phillips screws that secure the AC module to the director chassis, as shown in [Figure 4-7](#).
6. Pull the power supply (❶) from the director AC module (❷), as shown in [Figure 4-7](#). Support the AC module with one hand.
7. Place the AC module in an anti-static bag to provide ESD protection.

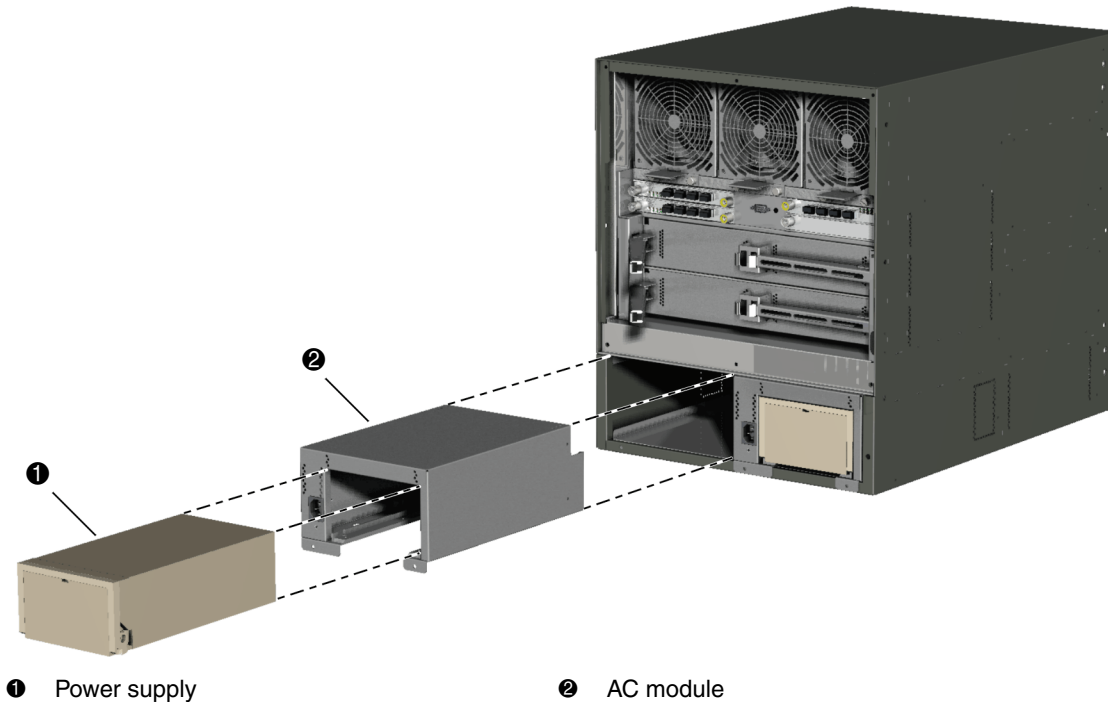


Figure 4-7: AC module removal and replacement

Replacing the AC Module

To replace a AC module:

1. Remove the replacement AC module from its protective antistatic bag.
2. Inspect the PWA side of the AC module for bent or broken connector pins that may have been damaged during shipping. If any pins are damaged, obtain a new assembly.
3. Position the AC module at the rear of the director chassis, as shown in [Figure 4-7](#). Push the module toward the backplane to engage the connector pins.
4. Insert and tighten the two panhead Phillips screws that secure the AC module.
5. Replace the power supply ([RRP: Redundant Power Supply on page 4-19](#)).
6. Disconnect the ESD wrist strap from the director chassis and your wrist.

7. Connect the power cord to the AC module.
8. Verify that power-on self-tests (POSTs) complete and the green power LED on the front bezel, green LED on the active CTP card, and green PWR OK LEDs on both power supplies remain illuminated. If a problem is indicated, go to [MAP 0000: Start MAP on page 2–12](#) to isolate the problem.
9. At the **Hardware View**, observe all FRU graphics and ensure no alert symbols display that indicate a failure (yellow triangle or red diamond). If a problem is indicated, go to [MAP 0000: Start MAP on page 2–12](#) to isolate the problem.
10. Perform the data collection procedure ([Collecting Maintenance Data on page 3–40](#)).
11. Clear the amber system error LED on the director bezel:
 - a. At the **Hardware View**, right-click the front panel bezel graphic (away from a FRU) to open a menu.
 - b. Click **Clear System Error Light**.
12. If necessary, close and lock the equipment cabinet door.

RRP: Redundant SBAR Assembly

Use the following procedures to remove or replace a redundant SBAR assembly (two assemblies in the director) with the backup SBAR assembly operational. A list of tools required is provided.

Tools Required

The following tools are required to perform these procedures.

- Standard flat-tip screwdriver.
- ESD grounding cable and wrist strap.
- Torque tool and hex adapter (provided with the director).

Removing the SBAR Assembly

To remove a redundant SBAR assembly:

1. If the director is installed in a stand-alone configuration, go to [step 2](#). If the director is rack-mounted, unlock and open the cabinet rear door as directed by the HP authorized service provider.

2. Follow ESD procedures by attaching a wrist strap to the director chassis and your wrist, as shown in [Figure 4-2](#).



CAUTION: To avoid causing machine errors or damage while working on the director, follow ESD procedures by connecting a grounding cable to the director chassis and wearing an ESD wrist strap.

3. Remove the RFI shield.
4. Identify the defective SBAR assembly from the amber LED on the assembly or failure information at the HAFM server's **Hardware View**.
5. The SBAR assembly is secured to the director backplane with two handles (extractor levers) that snap lock, as shown in [Figure 4-8](#). Open both handles.



- 1 SBAR assembly

Figure 4-8: SBAR assembly removal and replacement

6. Using the handles, pull the SBAR assembly out of the director chassis. Support the assembly with one hand when performing this step.
7. Place the SBAR assembly in an antistatic bag to provide ESD protection.

Replacing the SBAR Assembly

To replace a redundant SBAR assembly:

1. Remove the replacement SBAR assembly from its protective antistatic bag.

2. Inspect the printed wiring assembly (PWA) side of the SBAR assembly for bent or broken connector pins that may have been damaged during shipping. If any pins are damaged, obtain a new assembly.
3. Orient the SBAR assembly, as shown in [Figure 4–8](#). Insert the assembly into the director chassis guide, then push the assembly toward the backplane to engage the connector pins. Verify the assembly is flush and even with the other SBAR assembly in the director.
4. Close both handles.
5. Disconnect the ESD wrist strap from the director chassis and your wrist.
6. Inspect the assembly to ensure the amber LED is extinguished. If the amber LED is illuminated, go to [MAP 0000: Start MAP on page 2–12](#) to isolate the problem.
7. Replace the RFI shield.
8. At the HAFM server's **Hardware View**, click **Logs** and choose **Event Log**. The **Event Log** displays. Ensure the following event codes display in the log:
 - **600**-SBAR card hot-insertion initiated.
 - **601**-SBAR card hot-insertion completed.If an event code **601** does not display in the log, go to [MAP 0000: Start MAP on page 2–12](#) to isolate the problem.
9. At the **Hardware View**, observe the graphic representing the replacement SBAR assembly and ensure no alert symbols display that indicate a failure (yellow triangle or red diamond). If a problem is indicated, go to [MAP 0000: Start MAP on page 2–12](#) to isolate the problem.
10. At the **Hardware View**, double-click the graphic representing the replacement SBAR assembly to open the **FRU Properties** dialog box. Verify that information (FRU name, position, and state) is correct. If a problem is indicated, go to [MAP 0000: Start MAP on page 2–12](#) to isolate the problem.
11. Perform the data collection procedure ([Collecting Maintenance Data on page 3–40](#)).
12. If the customer requests the replacement SBAR assembly be set as the active SBAR, perform a FRU switchover. At the **Hardware View**, right-click the graphic representing the replacement assembly to open a menu, then choose **Switchover**.

13. Clear the amber system error LED on the director bezel:
 - a. At the **Hardware View**, right-click the front panel bezel graphic (away from a FRU) to open a menu.
 - b. Click **Clear System Error Light**.
14. If necessary, close and lock the equipment cabinet door.

RRP: Redundant Fan Module

Use the following procedures to remove or replace a redundant cooling fan module. A list of tools required is provided.

Tools Required

The following tools are required to perform these procedures.

- Standard flat-tip screwdriver.
- ESD grounding cable and wrist strap.

Removing the Fan Module

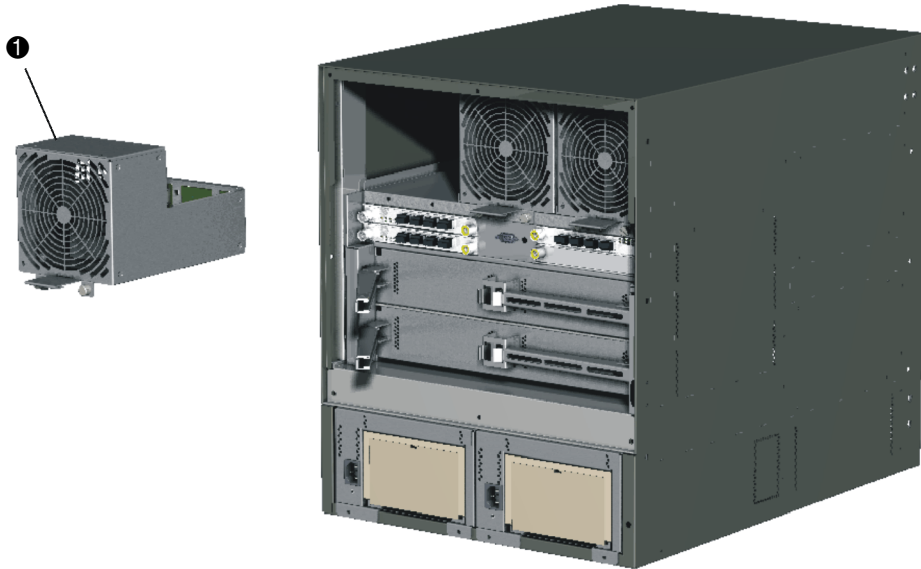
To remove a redundant fan module:

1. If the director is installed in a stand-alone configuration, go to [step 2](#). If the director is rack-mounted, unlock and open the cabinet rear door as directed by the HP authorized service provider.
2. Follow ESD procedures by attaching a wrist strap to the director chassis and your wrist, as shown in [Figure 4-2](#).



CAUTION: To avoid causing machine errors or damage while working on the director, follow ESD procedures by connecting a grounding cable to the director chassis and wearing an ESD wrist strap.

3. Remove the RFI shield.
4. Identify the defective fan module from the amber LED on the module or failure information at the HAFM server's **Hardware View**.
5. Two captive screws secure the fan module (❶) to the director chassis, as shown in [Figure 4-9](#). Using a standard flat-tip screwdriver, loosen the captive screws.



- 1 Fan module

Figure 4-9: Fan module removal and replacement

6. Using the rear of the fan module as a handle, pull the module from the director. Support the fan module with one hand when performing this step.



CAUTION: Do not remove a fan module unless the replacement module is available. Operation of the director with only one fan module for an extended period may cause one or more thermal sensors to post event codes.

7. Place the fan module in an antistatic bag to provide ESD protection.

Replacing the Fan Module

To replace the fan module:

1. Remove the replacement fan module from its protective antistatic bag.
2. Inspect the PWA on the underside of the fan module for bent or broken connector pins that may have been damaged during shipping. If any pins are damaged, obtain a new fan module.

3. Position the fan module at the rear of the director chassis, as shown in [Figure 4–9](#). Using the rear of the fan module as a handle, push the module toward the backplane to engage the connector pins. Support the fan module with one hand when performing this step.
4. Using a standard flat-tip screwdriver, tighten the two captive screws that secure the fan module to the director chassis.
5. Disconnect the ESD wrist strap from the director chassis and your wrist.
6. Inspect the fan module to ensure the amber LED is extinguished. If the LED is illuminated, go to [MAP 0000: Start MAP on page 2–12](#) to isolate the problem.
7. Replace the RFI shield.
8. At the HAFM server's **Hardware View**, click **Logs** and choose **Event Log**. The **Event Log** displays. Ensure an event code **321** (fan FRU inserted) displays in the log.

If an event code **321** does not display in the log, go to [MAP 0000: Start MAP on page 2–12](#) to isolate the problem.
9. At the **Hardware View**, observe the graphic representing the replacement fan module and ensure no alert symbols display that indicate a failure (yellow triangle or red diamond). If a problem is indicated, go to [MAP 0000: Start MAP on page 2–12](#) to isolate the problem.
10. At the **Hardware View**, double-click the graphic representing the replacement fan module to open the **FRU Properties** dialog box. Verify that information (FRU name, position, and state) is correct. If a problem is indicated, go to [MAP 0000: Start MAP on page 2–12](#) to isolate the problem.
11. Perform the data collection procedure ([Collecting Maintenance Data on page 3–40](#)).
12. Clear the amber system error LED on the director bezel:
 - a. At the **Hardware View**, right-click the front panel bezel graphic (away from a FRU) to open a menu.
 - b. Click **Clear System Error Light**.
13. If necessary, close and lock the equipment cabinet door.

RRP: Power Module Assembly

Use the following procedures to remove or replace the power module assembly. A list of tools required is provided.

Tools Required

The following tools are required to perform these procedures.

- Standard flat-tip screwdriver.
- Standard cross-tip (Phillips) screwdriver.
- ESD grounding cable and wrist strap.

Removing the Power Module Assembly

To remove the power module assembly:

1. Notify the customer the director will be powered off. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the director and sets attached devices offline.
2. If the director is installed in a stand-alone configuration, go to [step 3](#). If the director is rack-mounted, unlock and open the cabinet front and rear doors as directed by the HP authorized service provider.
3. Power off and unplug the director ([Power-Off Procedure on page 3–43](#)).



WARNING: Ensure both power cords are disconnected from the power module assembly prior to removal or replacement.

4. Follow ESD procedures by attaching a wrist strap to an approved bench grounding point and your wrist.



CAUTION: To avoid causing machine errors or damage while working on the director, follow ESD procedures by connecting a grounding cable to an approved bench grounding point and wearing an ESD wrist strap.

5. Unseat and disconnect (but do not remove) both power supplies ([RRP: Redundant Power Supply on page 4–19](#)).
6. Remove the RFI shield.

7. Remove only the center and upper left fan modules (❶) (viewed from the rear) (RRP: [Redundant Fan Module on page 4-27](#)).
8. Unplug the power module assembly cable from the backplane.
9. Remove the power module assembly (❷), as shown in [Figure 4–10](#).
10. Place the LED assembly in an anti-static bag to provide ESD protection.

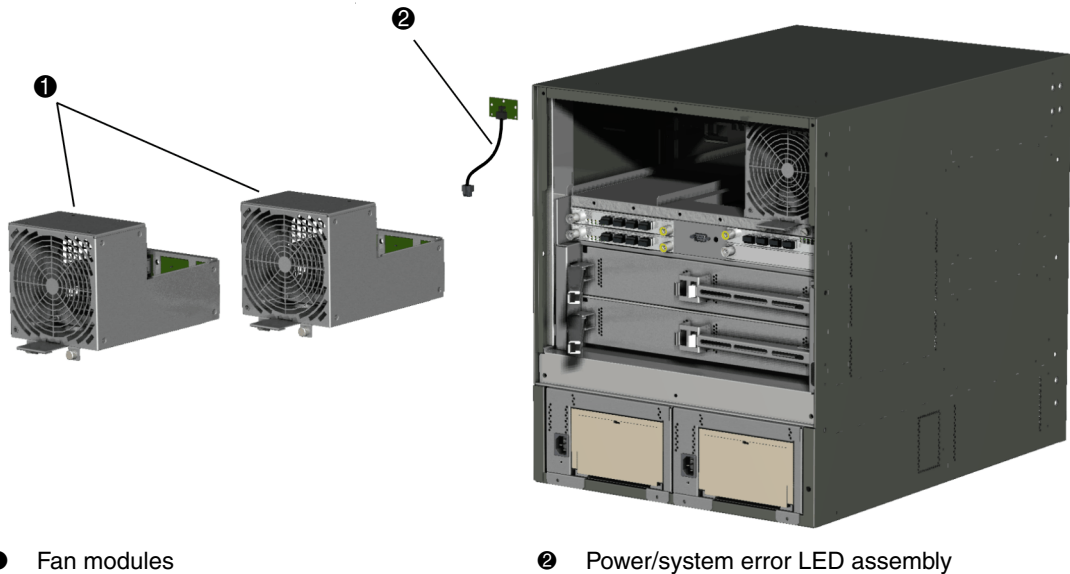


Figure 4–10: Power module assembly removal and replacement

Replacing the Power Module Assembly

To replace the power module assembly:

1. Remove the replacement power module assembly from its protective anti-static bag.
2. Replace the power module assembly.
3. Plug the power module assembly cable into the backplane.
4. Replace the center and upper left fan modules (viewed from the rear) (RRP: [Redundant Fan Module on page 4-27](#)).

5. Disconnect the ESD wrist strap from the director chassis and your wrist.
6. Replace the RFI shield.
7. Seat and connect both power supplies ([RRP: Redundant Power Supply on page 4–19](#)).
8. Disconnect the ESD wrist strap from the director chassis and your wrist.
9. Power on the director ([Power-On Procedure on page 3–43](#)).
10. Verify that power-on self-tests (POSTs) complete and the green power LED on the front bezel, green LED on the active CTP card, and green **PWR OK** LEDs on both power supplies remain illuminated. If a problem is indicated, go to [MAP 0000: Start MAP on page 2–12](#) to isolate the problem.
11. At the HAFM server's **Hardware View**, observe all FRU graphics and ensure no alert symbols display that indicate a failure (yellow triangle or red diamond). If a problem is indicated, go to [MAP 0000: Start MAP on page 2–12](#) to isolate the problem.
12. Perform the data collection procedure ([Collecting Maintenance Data on page 3–40](#)).
13. If required, clear the amber system error LED on the director bezel:
 - a. At the **Hardware View**, right-click the front panel bezel graphic (away from a FRU) to open a menu.
 - b. Click **Clear System Error Light**.
14. If necessary, close and lock the equipment cabinet doors.

RRP: Backplane

Use the following procedures to remove or replace the backplane. A list of tools required is provided.

Tools Required

The following tools are required to perform these procedures.

- Torque tool and hex adapter (provided with the director).
- Standard flat-tip screwdriver.
- Standard cross-tip (Phillips) screwdriver.

- ESD grounding cable and wrist strap.
- Maintenance terminal (desktop or notebook PC) with:
 - The Microsoft Windows 98, Windows 2000, Windows Millennium Edition, or Windows XP.
 - RS-232 serial communication software (such as ProComm Plus or HyperTerminal). HyperTerminal is provided with Windows operating systems.
- Asynchronous RS-232 null modem cable (provided with the director).

Removing the Backplane Assembly

To remove the backplane:

1. At the **Hardware View**, double-click the graphic representing the director bezel (do not click a graphical FRU) to open the **Director Properties** dialog box. Record the director serial number. This number must be programmed into the replacement backplane.

If the director is not communicating with the HAFM server (**Director Properties** dialog box is not available), obtain the serial number while performing [step 5](#).

2. Notify the customer the director will be powered off. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the director and sets attached devices offline.
3. If the director is installed in a stand-alone configuration, go to [step 4](#). If the director is rack-mounted, unlock and open the cabinet front and rear doors as directed by the HP authorized service provider.
4. Power off and unplug the director ([Power-Off Procedure on page 3–43](#)).



WARNING: Ensure both power cords are disconnected from the power module assembly prior to removal or replacement.

5. If necessary, record the director serial number from the silver label at the bottom front of the chassis (under the CTP cards).
6. Remove the RFI shield.
7. Follow ESD procedures by attaching a wrist strap to an approved bench grounding point and your wrist.



CAUTION: To avoid causing machine errors or damage while working on the director, follow ESD procedures by connecting a grounding cable to an approved bench grounding point and wearing an ESD wrist strap.

8. Remove the CTP cards ([RRP: Redundant CTP Card on page 4-5](#)).
9. Remove the UPM cards ([RRP: UPM Card on page 4-9](#)).
10. Remove both power supplies ([RRP: Redundant Power Supply on page 4-19](#)).
11. Remove the AC module ([RRP: AC Module on page 4-21](#)).
12. Remove the fan modules ([RRP: Redundant Fan Module on page 4-27](#)).
13. Remove both SBAR assemblies ([RRP: Redundant SBAR Assembly on page 4-24](#)).
14. Unplug the power module assembly cable from the backplane.
15. The card cage and backplane are secured to the director chassis with 6 panhead Phillips screws, as shown in [Figure 4-11](#). Use a standard Phillips screwdriver to remove these screws.

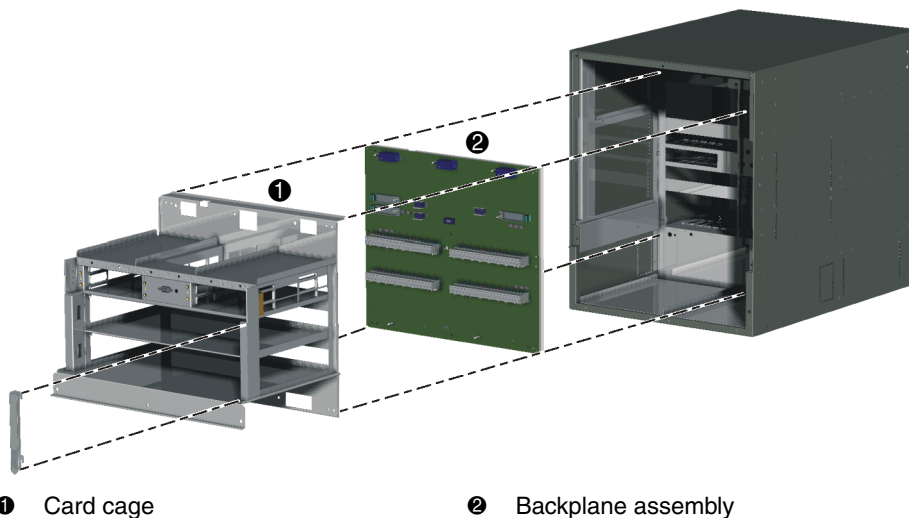


Figure 4-11: Backplane removal and replacement

16. Remove the card cage (❶) and backplane assembly (❷), as shown in [Figure 4-11](#).

17. Disconnect the maintenance port cable from the backplane.
18. The backplane is secured to the card cage with 7 panhead Phillips screws. Use a standard Phillips screwdriver to remove these screws.
19. Remove the backplane (PWA and frame as one FRU) from the card cage. Place the backplane in an anti-static bag to provide ESD protection.

Replacing the Backplane Assembly

To replace the backplane and all FRUs disconnected from the backplane:

1. Remove the replacement backplane from its protective anti-static bag. Inspect the backplane PWA to ensure no connector pins are damaged.
2. Align the guide pins on the back of the backplane with the alignment holes in the card cage.
3. While holding the backplane in place, insert and hand tighten one of the top center panhead Phillips screws.
4. Insert and hand tighten the remaining six panhead Phillips screws.
5. Using a standard Phillips screwdriver, tighten the 7 panhead screws that secure the backplane to the card cage. Tighten the screws alternately from bottom to top and from side to side.
6. Connect the maintenance port cable.
7. Replace the card cage and backplane in the director chassis. with 6 panhead Phillips screws. Use a standard Phillips screwdriver to replace the 6 panhead Phillips screws.
8. Plug the Power/System LED assembly cable into the backplane.
9. Replace the SBAR assemblies ([RRP: Redundant SBAR Assembly on page 4–24](#)).
10. Replace the fan modules ([RRP: Redundant Fan Module on page 4–27](#)).
11. Replace the AC modules ([RRP: AC Module on page 4-21](#)).
12. Replace the power supplies ([RRP: Redundant Power Supply on page 4–19](#)).
13. Replace the UPM cards ([RRP: UPM Card on page 4-9](#)).
14. Replace the CTP cards ([RRP: Redundant CTP Card on page 4-5](#)).
15. Disconnect the ESD wrist strap from the director chassis and your wrist.

16. Replace the RFI shield.
17. Connect the power cords and power on the director ([Power-On Procedure on page 3-43](#)).
18. Verify that POSTs complete and the green power LED on the front bezel, green LED on the active CTP card, and green **PWR OK** LEDs on both power supplies remain illuminated. If a problem is indicated, go to [MAP 0000: Start MAP on page 2-12](#) to isolate the problem.
19. Reprogram the replacement backplane with the original director serial number:
 - a. Remove the protective cap from the 9-pin maintenance port at the rear of the director (a flat-tip screwdriver may be required). Connect the 9-pin end of the RS-232 null modem cable to the 9-pin maintenance port on the director.
 - 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 and establish a hyperterminal connection. Use the following settings:
 - **Kilobits per second—115.2.**
 - **Data bits—8.**
 - **Parity—None.**
 - **Stop bits—1.**
 - **Flow control—Hardware.**When the parameters are set, click **OK**. The **HyperTerminal** window displays.
 - d. At the **C>** prompt, type the maintenance-level password (the default is **level-2**) and press **Enter**. The password is case sensitive. The **HyperTerminal** window displays with an **C>** prompt at the top of the window.
 - e. Type the command **oem nnnnnnnn**, where **nnnnnnnn** is the original director serial number recorded in [step 1](#) or [step 5](#) of the removal procedure.
 - f. Choose **Exit** from the **File** menu to close the *HyperTerminal* application.
20. Initial machine load (IML) the director. At the front of the director, press and hold the white IML button on the faceplate of the active CTP card (green LED illuminated) for three seconds.

21. At the HAFM server's **Hardware View**, observe all FRU graphics and ensure no alert symbols display that indicate a failure (yellow triangle or red diamond). If a problem is indicated, go to [MAP 0000: Start MAP on page 2–12](#) to isolate the problem.
22. Perform the data collection procedure ([Collecting Maintenance Data on page 3–40](#)).
23. If required, clear the amber system error LED on the director bezel:
 - a. At the **Hardware View**, right-click the front panel bezel graphic (away from a FRU) to open a menu.
 - b. Click **Clear System Error Light**.
24. If necessary, close and lock the equipment cabinet doors.

Illustrated Parts Breakdown

This chapter provides an illustrated parts breakdown for all Director 2/140 field-replaceable units (FRUs). Exploded-view assembly drawings are provided for:

- Front-accessible FRUs.
- Rear-accessible FRUs.
- Miscellaneous parts.
- Power plugs and receptacles.

Exploded-view illustrations portray the director disassembly sequence for clarity. Illustrated FRUs are numerically keyed to associated parts lists. The parts lists also include HP part numbers, descriptions, and quantities.

An (*ESD*) symbol precedes the description of a FRU containing electrostatic discharge (ESD) sensitive components. Handle ESD-labelled FRUs in accordance with caution statements in this manual.

Front-Accessible FRUs

[Figure 5-1](#) illustrates front-accessible FRUs, and [Table 5-1](#) is the parts list. The table includes reference numbers to [Figure 5-1](#), part numbers, descriptions, and quantities.

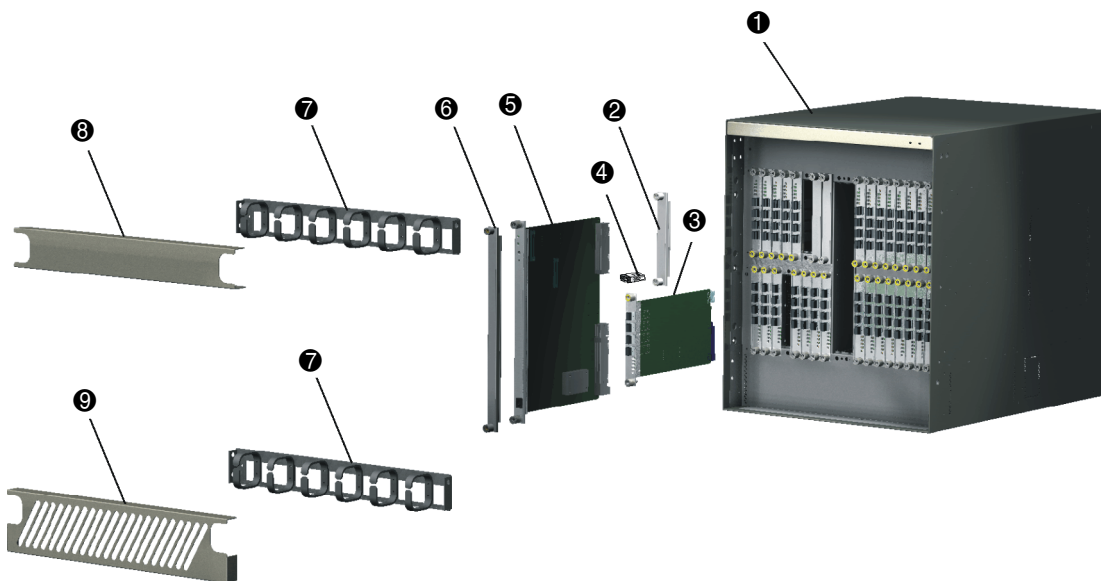


Figure 5–1: Front-accessible FRUs

Table 5–1: Front-Accessible FRU Parts List

Ref.	Part Number	Description	Qty.
①	Reference	Base assembly, ED-6140 Director	1
②	002-002230-100	Filler panel, UPM	1 to 17
③	470-000453-400	(*ESD*) Printed wiring assembly, universal port module (UPM), 4-port, LC (pluggable optics not included)	16 to 35
④	803-000064-386	SFP transceiver, optical, shortwave laser, 2.1250 Gbps, LC	0 to 140
④	803-000065-313	SFP transceiver, optical, longwave laser, 2.1250 Gbps, 10 K, LC	0 to 140
④	803-000066-313	SFP transceiver, optical, longwave laser, 2.1250 Gbps, 20 K, LC	0 to 140
④	803-000067-313	SFP transceiver, optical, longwave laser, 2.1250 Gbps, 35 K, LC	0 to 140
⑤	470-000437-401	(*ESD*) Printed wiring assembly, control processor (CTP)	2
⑥	Reference	Filler panel, CTP	2
⑦	Reference	Bracket, d-ring (cable organizer feature)	2

Table 5-1: Front-Accessible FRU Parts List (Continued)

Ref.	Part Number	Description	Qty.
⑧	Reference	Cover, top cable	1
⑨	Reference	Cover, diagonal cable	1

Rear-Accessible FRUs

Figure 5-2 and Figure 5-3 illustrate rear-accessible FRUs, and Table 5-2 and Table 5-3 are the rear-accessible parts lists. The tables include reference numbers to Figure 5-2 and Figure 5-3, part numbers, descriptions, and quantities.

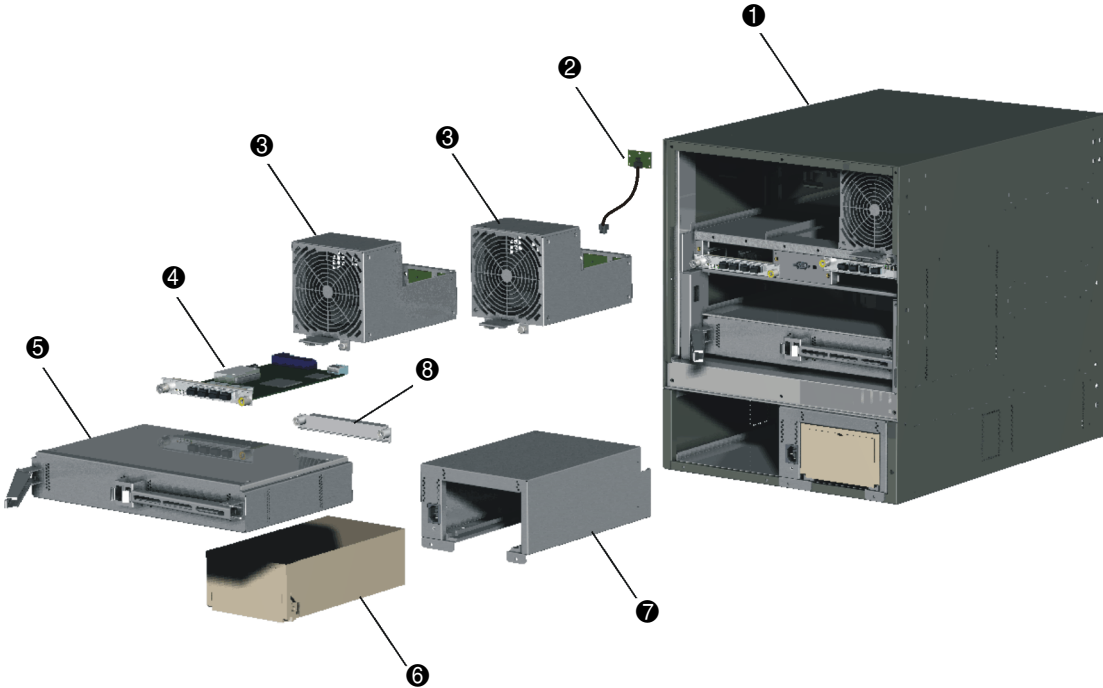


Figure 5-2: Rear-accessible FRUs (part 1)

Table 5–2: Rear-Accessible FRU Parts List (Part 1)

Ref.	Part Number	Description	Qty.
❶	Reference	Base assembly, ED-6140 Director	1
❷	470-000466-100	(*ESD*) LED assembly, power/system error	1
❸	476-000462-102	(*ESD*) Fan module	3
❹	See Table 5–1	(*ESD*) Printed wiring assembly, universal port module (UPM), 4-port, LC (pluggable optics not included)	16 to 35
❺	475-000471-201	(*ESD*) Printed wiring assembly, serial crossbar (SBAR)	2
❻	721-000058-001	(*ESD*) Power supply, 180 - 264 VAC, 48 VDC	2
❼	002-002489-100	(*ESD*) AC module (Power distribution assembly)	2
❽	See Table 5–1	Filler panel, UPM	1 to 17

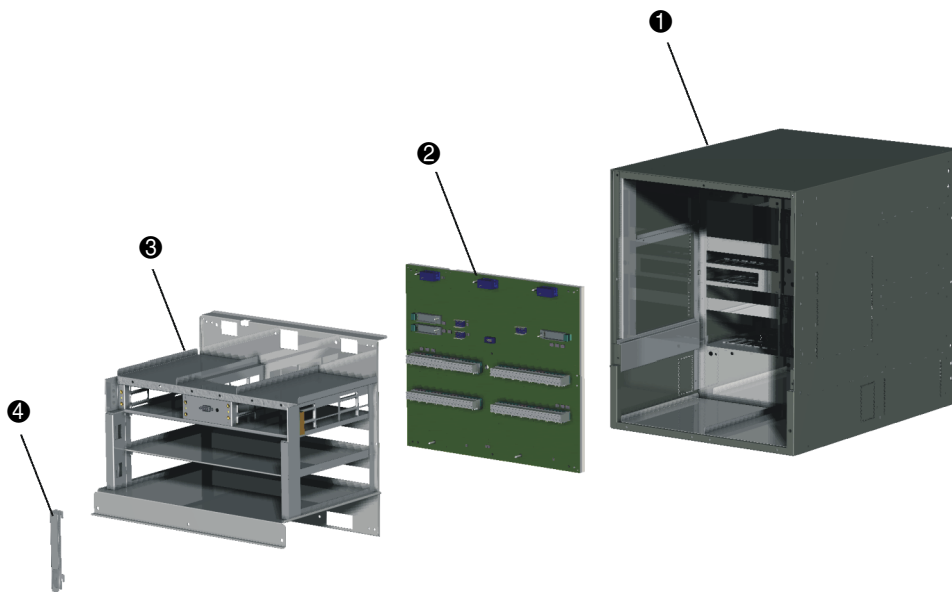


Figure 5–3: Rear-accessible FRUs (part 2)

Table 5–3: Rear-Accessible FRU Parts List (Part 2)

Ref.	Part Number	Description	Qty.
❶	Reference	Base assembly, ED-6140 Director	1
❷	476-000435-300	(*ESD*) Printed wiring assembly, backplane	1
❸	Reference	Cage assembly, rear card	1
❹	Reference	Retainer, rear cable guide	1

Miscellaneous Parts

Table 5–4 is the parts list for miscellaneous parts.

Table 5–4: Miscellaneous Parts

Ref.	Part Number	Description	Qty.
❶	002-002317-000	Torque driver with 5/32 in. bit	1
❷	803-000057-000	Loopback plug, LC, MM (50/125) (#1148)	1
❷	803-000057-001	Loopback plug, LC, SM (9/125) (blue) (#1149)	1
❸	801-000039-000	Null modem cable, DB9F-DB9F	1
❹	801-000035-010	Ethernet cable, 10 ft.	1

Power Plugs and Receptacles

Figure 5–4 illustrates the optional power plugs and receptacles and Table 5–4 is the parts list. The table includes reference numbers to Figure 5–4, feature numbers, and descriptions.

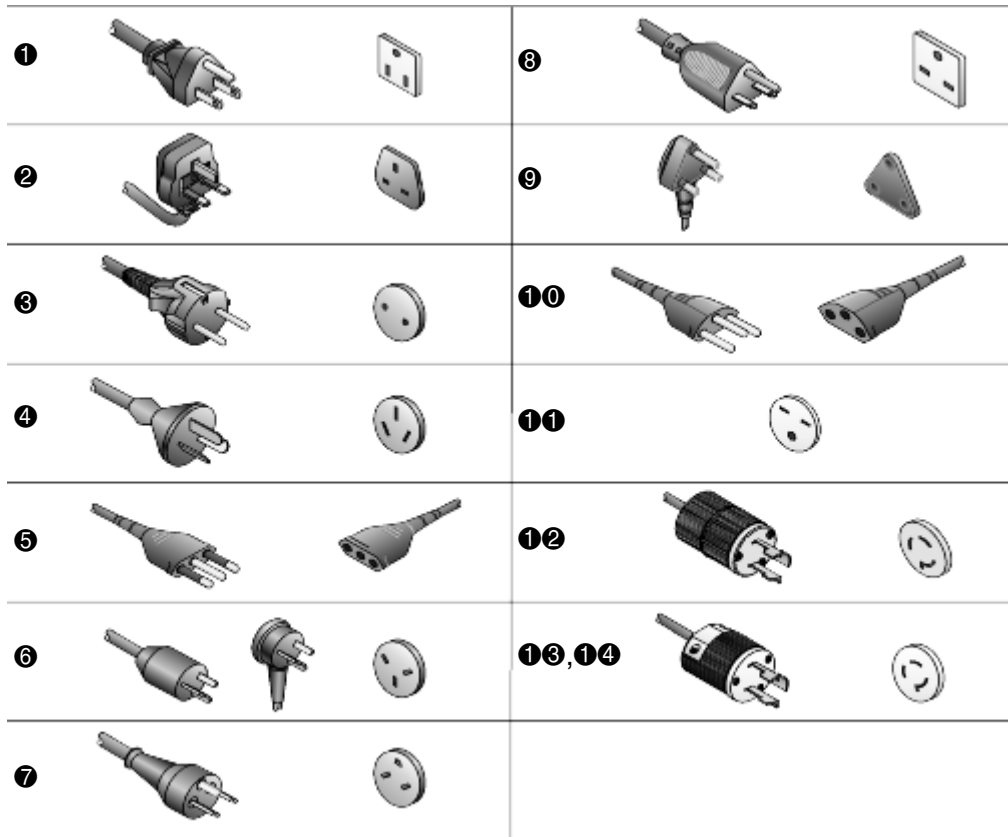


Figure 5-4: Power plugs and receptacles

Table 5-5: Power Plugs and Receptacles

Ref.	Part Number	Description	Qty.
①	806-000001-000	120V, United States NEMA 5-15P straight, 120V, 15A, 15'1" Receptacle: NEMA 5-15R, 125V, 15A	1010
①	806-000058-000	125V, Japan NEMA 5-15P straight, 125V, 12A, 2.5 m. Receptacle: NEMA 5-15R, 125V, 12A	1030
②	806-000004-001	220V, 2.5m United Kingdom, 10A	1012

Table 5-5: Power Plugs and Receptacles (Continued)

Ref.	Part Number	Description	Qty.
③	806-000005-001	220V, 2.5m European Community, 10A	1013
④	806-000006-001	220V, 2.5m Australia, 10A	1014
⑤	806-000027-000	250V, Italy/Chile/Libya/Ethiopia, 10A, 6 to 10 ft.	1021
⑥	806-000029-000	250V, Israel, 10A, 6 to 10 ft.	1022
⑦	806-000030-000	250V, Thailand/Bolivia/Peru NEMA 6-15P, 250V, 10A, 6 to 10 ft. Receptacle: NEMA 6-15R, 250V, 15A	1023
⑧	806-000033-000	250V, Denmark, 10A, 6 to 10 ft.	1024
⑨	806-000034-000	250V, South Africa/Burma/Bangladesh, 10A, 6 to 10 ft.	1025
⑩	806-000037-000	250V, Switzerland/Liechtenstein, 10A, 6 to 10 ft.	1026
⑪	806-000038-000	240V, United States, Non-Locking NEMA 6-15P, 15A, 6 ft. Receptacle: NEMA 6-15R, 250V, 15A	1027
⑫	806-000040-000	240V, 1.8M, United States, Twist Lock NEMA L6-15P, 6A, 6 ft. Receptacle: NEMA 6-15R, 250V, 15A	1028
⑬	806-000042-000	208-240V, 9'10" United States, Twist Lock NEMA L6-15P, 208-240V, 15A Receptacle: NEMA L6-15R, 250V, 15A	1016
⑭	806-000042-000	240V, 2.8M, United States, Twist Lock NEMA L6-15P, 6A, 10 ft. Receptacle: NEMA L6-15R, 250V, 15A	1029

Messages

This appendix lists information and error messages that display in message boxes at the HP StorageWorks *HA-Fabric Manager (HAFM)* and *Director 2/140 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.

Table A-1: HAFM Messages

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 alias, zone, and zone set names must be unique.	When creating a new alias, zone, or zone set, the name must be unique.	Choose a unique name for the new alias, zone, or zone set.

Table A-1: HAFM Messages (Continued)

Message	Description	Action
All zone members are logged.	Attempt was made to display all zone members not logged-in using the Zone Set tab, but all members are currently logged in.	Informational message.
An <i>HAFM</i> application session is already active from this workstation.	Only one instance of the <i>HAFM</i> application is allowed to be open per remote workstation.	Close all but one of the <i>HAFM</i> application sessions.
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 delete this zone set?	The selected zone set will be deleted from the zone library.	Click Yes to delete the zone set 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.

Table A-1: HAFM Messages (Continued)

Message	Description	Action
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.
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 for the device you want to add to the zone.
Cannot connect to HAFM server.	The <i>HAFM</i> 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. <ul style="list-style-type: none"> • 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.	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 in HAFM before disabling Fabric Binding.
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.

Table A-1: HAFM Messages (Continued)

Message	Description	Action
Cannot display route. All switches in route must be managed by the same server.	You cannot show the route between devices that are attached to switches or directors managed by a different HAFM server.	Make sure devices named in Show Routes dialog box are attached to products 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 Edge Switch 2/16s, Edge Switch 2/32s, or Director 2/140s.
Cannot display route. Device is not a member of a zone in the active zone set.	You cannot show the route for a device that is not a member of a zone in the active zone set. The source node that you have selected is not part 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 on one switch fabric.	The user cannot show routes between end devices in a fabric when configuring Show Routes (Configure menu) .	Error displays when attempting to show routes on a fabric with only one switch. Configure Show Routes on a multi-switch fabric.
Cannot display route. error 9.	An internal error has occurred while trying to view routes.	Contact the next level of support to report the problem.
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 .

Table A-1: HAFM Messages (Continued)

Message	Description	Action
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.
Cannot modify product.	The selected product cannot be modified.	Verify the HAFM server-to-product link is up. <ul style="list-style-type: none"> • 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 displays 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 displays 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 has not been configured.	Enter a valid community name in the Configure SNMP dialog box.

Table A-1: HAFM Messages (Continued)

Message	Description	Action
Cannot show zoning library. No fabric exists.	You cannot show the zoning library if no fabric exists. You must have identified a switch or director to HAFM for a fabric to exist.	Identify an existing switch or director to HAFM using 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 has been lost.	Log in to the HAFM server again through the HAFM Manager Login dialog box.
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 product is enabled for Open Fabric mode. Open Fabric mode does not support zone members defined by port numbers.	Redefine zone members by the WWN of attached devices.
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 therefore 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.

Table A–1: HAFM Messages (Continued)

Message	Description	Action
Download complete. Click OK and start the HAFM.	Download of the <i>HAFM</i> and <i>Product Manager</i> applications is complete.	Start the <i>HAFM</i> 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 name in zoning configuration.	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.
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 current active zone set will be replaced.	Click OK to continue or Cancel to end the operation.

Table A-1: HAFM Messages (Continued)

Message	Description	Action
Error connecting to switch.	While viewing routes, the HAFM server was unable to connect to the switch. The switch failed or the switch-to-HAFM server Ethernet link failed.	Try the operation again. If the problem persists, contact the next level of support.
Error creating zone.	The <i>HAFM</i> application encountered an internal error.	Try the operation again. If the problem persists, contact the next level of support.
Error creating zone set.	The <i>HAFM</i> application encountered an internal error.	Try the operation again. If the problem persists, contact the next level of support.
Error deleting zone.	The <i>HAFM</i> application encountered an internal error.	Try the operation again. If the problem persists, contact the next level of support.
Error deleting zone set.	The <i>HAFM</i> application encountered an internal error.	Try the operation again. If the problem persists, contact the next level of support.
Error reading log file.	The <i>HAFM</i> 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 <i>HAFM</i> application encountered an internal error.	Try the operation again. If the problem persists, contact the next level of support.
Error transferring files < <i>message</i> >.	An error occurred while transferring files from the PC hard drive to the <i>HAFM</i> application. The message varies, depending on the problem.	Try the file transfer operation again. If the problem persists, contact the next level of support.

Table A-1: HAFM Messages (Continued)

Message	Description	Action
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 member could not be found.	A fabric member does not exist when the application prepared to find a route, find a route node, or gather route information on that fabric member.	Ensure the product is incorporated into the fabric and retry the operation. If the problem persists, contact the next level of support.
Fabric not persisted.	The user attempted to refresh or clear the Log dialog, after a fabric was unpersisted. When you unpersist a fabric, the corresponding fabric log is deleted.	Clear the log dialog after the fabric is unpersisted.
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 error <error number 1 through 8 >.	The <i>HAFM</i> application encountered an internal error (1 through 8 inclusive) and cannot continue operation.	Contact the next level of support to report the problem.

Table A-1: HAFM Messages (Continued)

Message	Description	Action
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 <i>HAFM</i> application.	Verify the user name and password with the customer's network administrator and retry the operation.
HAFM server is shutting down. Connection will be terminated.	The <i>HAFM</i> 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 session is already active from this workstation.	An HAFM session already exists on the current workstation.	A workstation can have only one active HAFM session.
Invalid character in field.	An invalid character was entered in the data field.	Remove invalid characters from the entry.
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.
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.

Table A-1: HAFM Messages (Continued)

Message	Description	Action
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 1. For example, for a switch with 32 ports, the valid port range is 0–31.
Invalid product selection.	At the New Product dialog box, an invalid product was selected.	Select a valid product and retry the operation.
Invalid request.	<p>Three conditions result in this message:</p> <ul style="list-style-type: none"> • The user tried to add or modify a product from product view and the network 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.) 	<p>Select the action that is appropriate to the activity that caused the error:</p> <ul style="list-style-type: none"> • Network address: Specify a unique network address for the product. • User name: Specify a unique user name for the new user ID. • Do not delete the default Administrator user.

Table A-1: HAFM Messages (Continued)

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.	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 or nickname.	The World Wide Name or nickname that you have specified is invalid. The valid format for the World Wide Name is eight two-digit hexadecimal numbers separated by colons (xx:xx:xx:xx:xx:xx:xx:xx). The valid format for a nickname is non blank characters, up to 32 characters.	Try the operation again using a valid World Wide Name or nickname.
Invalid zone in zone set.	The defined zone no longer exists and is invalid.	Delete the invalid zone from the zone set.

Table A-1: HAFM Messages (Continued)

Message	Description	Action
Limit exceeded.	You cannot add a new product or user to HAFM if the maximum number of that resource already exists on the system.	Delete unneeded products or users from the system, before attempting to add any new ones.
Management session is already active from this workstation.	An instance of the <i>HAFM</i> application is already open at this workstation.	Close the previous session of the <i>HAFM</i> application before starting a new one.
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 HAFM server specified.	An HAFM server is not defined to the <i>HAFM</i> application.	At the HAFM Login screen, type a server name in the HAFM server field and click the Login button.
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 switch <i>Product Manager</i> 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.

Table A-1: HAFM Messages (Continued)

Message	Description	Action
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.
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.

Table A-1: HAFM Messages (Continued)

Message	Description	Action
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 <i>Product Manager</i> application is open.	Close the <i>Product Manager</i> application, then delete the product.
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.
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.
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.
Route data corrupted.	The information for this route is corrupt.	Try the operation again. If the problem persists, contact the next level of support.
Route request timeout.	The Show Route request timed out.	Try the operation again. If the problem persists, contact the next level of support.

Table A-1: HAFM Messages (Continued)

Message	Description	Action
Routing is not supported by the switch.	This switch or director does not support the Show Routes feature.	Select a different switch or director to show the route.
SANtegrity Feature not installed. Please contact your sales representative.	User selected Fabric Binding or Enterprise Fabric Mode from the Fabrics menu, but the SANtegrity feature was not installed.	Install the SANtegrity feature to use Fabric Binding or enable Enterprise Fabric Mode.
Select alias to add to zone.	An alias was not selected before clicking Add.	Select an alias before clicking Add.
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 <i>HAFM</i> 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.
Switch is not managed by HAFM.	The selected switch or director is not managed by the <i>HAFM</i> application.	Select a different switch or director.
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.

Table A-1: HAFM Messages (Continued)

Message	Description	Action
The Domain ID was not accepted. The World Wide Name and Domain ID must be unique in the Fabric Membership List.	User attempted to add a detached switch to the Fabric Membership List through the Fabric Binding option (SANtegrity feature), but a switch 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 <i>Product Manager</i> application and cannot perform the requested operation.	Wait until the process completes, then perform the operation again.
The link to the switch is not available.	The Ethernet connection between the HAFM server and director is down or unavailable.	Establish and verify the network connection.
The maximum number of aliases has already been configured.	The maximum number of aliases allowed was reached.	Delete an existing alias before adding a new alias.
The maximum number of HAFM server network addresses has already been configured.	The number of HAFM server IP addressees has already been configured.	Delete an existing IP address before adding a new address.

Table A-1: HAFM Messages (Continued)

Message	Description	Action
The maximum number of HAFM sessions has been reached.	A maximum of four 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 eight) or terminate a session before attempting to initiate a new session.
The maximum number of members has already been configured.	The maximum number of unique members is 4097. The maximum number of members is 8192.	Delete members that are no longer needed to allow new members to be configured.
The maximum number of nicknames has already been configured.	The maximum number of nicknames that can be defined to the <i>HAFM</i> application was reached.	Delete an existing nickname before adding a new nickname.
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 HP products (48) that can be defined to the <i>HAFM</i> 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 managed HP products of this type (48) that can be defined to the <i>HAFM</i> application was reached.	Delete an existing product of this type before adding a new product.

Table A–1: HAFM Messages (Continued)

Message	Description	Action
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 users has already been configured.	The number of users (32) that can be defined to the <i>HAFM</i> 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.

Table A-1: HAFM Messages (Continued)

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 has been 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.	User attempted to remove a switch from the Fabric Membership List using the Fabric Binding option, but the switch is still part of the fabric.	Remove the switch from the fabric by setting the switch offline or blocking the E_Port where the switch is connected.

Table A-1: HAFM Messages (Continued)

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.	User attempted to add a detached switch to the Fabric Membership List through the Fabric Binding option (SANtegrity feature), but an entry already exists in the Fabric Membership List with the same World Wide Name (WWN).	Enter a unique World Wide Name for the switch in 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.

Table A–1: HAFM Messages (Continued)

Message	Description	Action
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.
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 do not have a compatible version of the HAFM server software. In order for the <i>HAFM</i> application to function properly, a compatible version must be installed on the client machine. Click OK to install a compatible version.	The version of the <i>HAFM</i> application 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 <i>HAFM</i> application to the remote workstation (client) using the web install procedure.
You must download the HAFM client via the web install.	An attempt was made to download the <i>HAFM</i> application to a remote workstation (client) using an improper procedure.	Download a compatible version of the <i>HAFM</i> application to the remote workstation (client) using the web install procedure.

Table A-1: HAFM Messages (Continued)

Message	Description	Action
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 HAFM.	Define zones using the New Zone dialog box.
Zoning by port number is 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.
Zoning by port number is not supported in Open Fabric Mode.	You cannot specify an item for zoning by port number if HAFM is in Open Fabric Mode.	Define zones by WWN of device.
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.

Director 2/140 Product Manager Messages

This section lists Director 2/140 Product Manager information and error messages in alphabetical order.

Table A–2: Product Manager Messages

Message	Description	Action
A Product Manager instance is already open.	Only one instance of the <i>Product Manager</i> application can be open at one time.	Close the open <i>Product Manager</i> application so the desired instance of the <i>Product Manager</i> application can be opened.
All FPM ports will be held inactive while the director is configured to 2 Gb/sec speed. Do you want to continue?	Occurs when FPM cards are installed in the director and director speed is being set to 2Gb/sec in the Configure Operating Parameters dialog box.	Replace FPM cards with UPM cards (UPM cards operate at 1 and 2 Gb/sec) or set the director speed to 1 Gb/sec.
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 <i>Product Manager</i> application can install a firmware version to the 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.

Table A–2: Product Manager Messages (Continued)

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 director.	Click Yes to send the firmware version or No to abort the operation.
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 director with a failed CTP card.	A firmware version cannot be installed on a director with a failed control processor (CTP) card.	Replace the failed CTP card and retry the firmware installation.
Cannot Modify Switch/Director speed.	Port speeds can not be configured at a higher data rate than the director speed. This displays when you set the director speed to 1 Gb/sec through the Configure Operating Parameters dialog box and at least one of the ports is running at 2 Gb/sec.	Either return the director speed to 2 Gb/sec or configure all port data speeds to 1 Gb/sec through the Configure Ports dialog box.
Cannot retrieve current SNMP configuration.	The director SNMP configuration cannot be retrieved by the <i>Product Manager</i> application because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.

Table A-2: Product Manager Messages (Continued)

Message	Description	Action
Cannot retrieve diagnostics results.	director diagnostic results cannot be retrieved by the <i>Product Manager</i> 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 director date and time.	The director date and time cannot be retrieved by the <i>Product Manager</i> 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 director state.	The director state cannot be retrieved by the <i>Product Manager</i> 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 <i>Product Manager</i> 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 information.	Port information cannot be retrieved by the <i>Product Manager</i> application because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.

Table A-2: Product Manager Messages (Continued)

Message	Description	Action
Cannot retrieve port statistics.	Port statistics cannot be retrieved by the <i>Product Manager</i> 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 a port that is not installed.	Port diagnostics (loopback tests) cannot be performed on a port that does not have a small form factor pluggable (SFP) optical transceiver installed.	Install a transceiver in the port and perform diagnostics again.
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.

Table A-2: Product Manager Messages (Continued)

Message	Description	Action
Cannot save port configuration.	The port configuration cannot be saved at the <i>Product Manager</i> 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 director SNMP configuration cannot be saved at the <i>Product Manager</i> 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 all ports to Negotiate due to port speed restriction on some ports.	Displays if you try to set all ports to Negotiate through the Configure Ports dialog box and some ports do not support speed configuration.	Replace ports that do not support speed configuration (FPM cards) with those that do support more than one speed configuration (UPM cards).
Cannot set director date and time.	The director date and time cannot be set at the <i>Product Manager</i> 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 director state.	The director state cannot be set at the <i>Product Manager</i> application because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.

Table A-2: Product Manager Messages (Continued)

Message	Description	Action
Cannot set fibre channel parameters.	Fibre Channel parameters for the director cannot be set at the <i>Product Manager</i> 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 data collection.	The data collection procedure cannot be started by the <i>Product Manager</i> 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 firmware install while CTP synchronization is in progress.	The director's CTP cards are synchronizing and firmware cannot be installed until synchronization is complete.	Install the firmware after CTP card synchronization completes.
Cannot start port diagnostics.	Port diagnostics cannot be started at the <i>Product Manager</i> 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 to cancel the operation.
Connection to HAFM server lost. Click OK to exit application.	The <i>HAFM</i> application at a remote workstation lost the network connection to the HAFM server.	Start the <i>HAFM</i> application to connect to the HAFM server.

Table A-2: Product Manager Messages (Continued)

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 <i>Product Manager</i> 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 <i>Product Manager</i> 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 <i>Product Manager</i> application because the Ethernet link is down or busy, or because the 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 director's CTP card.	Retry the operation again. If the condition persists, contact the next level of support.

Table A-2: Product Manager Messages (Continued)

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.
Director clock alert must be cleared before enabling period synchronization.	Clock alert mode is enabled through the Configure FICON Management Sever dialog box, and user is attempting to enable Periodic Date/Time Synchronization through the Configure Date and Time dialog box.	Disable clock alert mode through the Configure FICON Management Server dialog box.
Director must be offline to configure.	The director must be set offline prior to configuring Fibre Channel operating parameters.	Set the director offline, reconfigure parameters at the Configure Operating Parameters dialog box, and retry the operation.

Table A-2: Product Manager Messages (Continued)

Message	Description	Action
Do you want to continue with IPL?	This message requests confirmation to initial program load (IPL) the director.	Click OK to IPL the 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.
Error retrieving port information.	An error occurred at the <i>Product Manager</i> 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 <i>Product Manager</i> 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 <i>Product Manager</i> 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.

Table A-2: Product Manager Messages (Continued)

Message	Description	Action
Error transferring files < message >.	An error occurred while transferring files from the PC hard drive to the <i>Product Manager</i> 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.
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.
Internal file transfer error received from director.	The director detected an internal file transfer error.	Retry the operation. If the problem persists, contact the next level of support.

Table A–2: Product Manager Messages (Continued)

Message	Description	Action
Invalid character in field.	An invalid character was entered in the data field.	Remove invalid characters from the entry.
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 address.	An invalid port address has been entered.	Verify port address through the Configure Addresses - “Active” dialog box (S/390 mode only) and re-enter.
Invalid port number.	The Fibre Channel number entered is invalid. The port number must be an integer from 0 through 143 inclusive.	Verify and enter a valid port number.
Invalid response received from director.	An error occurred at the director during a firmware download operation.	Retry the firmware download operation. If the problem persists, contact the next level of support.
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.

Table A-2: Product Manager Messages (Continued)

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 value for BB_Credit.	At the Configure Operating Parameters dialog box, the buffer-to-buffer credit (BB_Credit) value must be an integer from 1 through 60 inclusive.	Verify and enter a valid 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.

Table A–2: Product Manager Messages (Continued)

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.

Table A–2: Product Manager Messages (Continued)

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-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 <i>Product Manager</i> 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 <i>HAFM</i> application's firmware library was reached.	Delete an existing firmware version before adding a new version.
No file was selected.	Action requires the selection of a file.	Select a file.
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.

Table A–2: Product Manager Messages (Continued)

Message	Description	Action
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.
Nonredundant director must be offline to install firmware.	If the director has only one CTP card, the director must be set offline to install a firmware version.	Set the director offline and install the firmware.
Performing this action will overwrite the date/time on the director.	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 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 director offline.	Click OK to set the director offline or to cancel the operation.
Performing this operation will change the current state to Online.	This message requests confirmation to set the director online.	Click OK to set the director online or to cancel the operation.
Periodic Date/Time synchronization must be cleared.	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.

Table A-2: Product Manager Messages (Continued)

Message	Description	Action
Port cannot swap to itself.	Port addresses entered in the Swap Ports dialog box are the same.	Ensure that address in the first and second port address fields are different.
Port diagnostics cannot be performed on an inactive port.	This displays when port diagnostics are run on a port that is in an inactive state.	Run the diagnostics on an active port.
Product Manager error < <i>error number 5001 or 5002</i> >.	At the Configure Operating Parameters dialog box, the R_A_TOV entry must be greater than E_D_TOV entry.	Verify and change one of the entries to make the relationship valid.
Product Manager instance is currently open.	A Product Manager window is open.	Informational message only.
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.
Start diagnostics failed. The test is currently running.	Diagnostics for the port was already started from the Port Diagnostics dialog box	Informational message.

Table A–2: Product Manager Messages (Continued)

Message	Description	Action
Stop diagnostics failed. The test is already running.	Diagnostics for the port was not running and the Stop was selected on the Port Diagnostics dialog box. Diagnostics quit for the port, 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.
System diagnostics cannot run. The Operational Status is invalid.	System diagnostics cannot run on directors or switches 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 director did not accept the request.	The director cannot perform the requested action.	Retry the operation. If the condition persists, contact the next level of support.
The director did not respond in the time allowed.	While waiting to perform a requested action, the director timed out.	Retry the operation. If the condition persists, contact the next level of support.

Table A-2: Product Manager Messages (Continued)

Message	Description	Action
The director is busy saving maintenance information.	The 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 director must be offline to configure.	This configuration task requires the director to be offline.	Take the director offline and retry the action.
The Ethernet link dropped.	The Ethernet connection between the HAFM server and the director is down or unavailable.	Establish and verify the network connection.
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 director is not available.	The Ethernet connection between the HAFM server and the 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 <i>Product Manager</i> application, and cannot perform the requested operation.	Wait until the process is completes, then perform the operation again.

Table A-2: Product Manager Messages (Continued)

Message	Description	Action
Threshold alerts are not supported.	Threshold alerts are not supported in firmware releases before 1.03.00.	Informational message.
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.

Event Code Tables

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. Events are reported as event codes.

This appendix lists all three-digit Director 2/140 event codes and provides detailed information about each code. Event codes are listed in numerical order and in tabular format, and are grouped as follows:

- **000** through **199**-system events.
- **200** through **299**-power supply events.
- **300** through **399**-fan module events.
- **400** through **499**-control processor (CTP) card events.
- **500** through **599**-fiber port module (UPM) card events.
- **600** through **699**-serial crossbar (SBAR) assembly events.
- **800** through **899**-thermal events.

Events are recorded in the Director 2/140 Event Log at the HAFM server, in the event log of the Embedded Web Server interface, at a remote workstation if e-mail and call-home features are enabled, at a simple network management protocol (SNMP) workstation, or at a host console if inband management is enabled. An event may also illuminate the system error light-emitting diode (LED) on the director front bezel.

In addition to numerical event codes, the tables in this appendix also provide:

- **Message**-a brief text string that describes the event.
- **Severity**-a severity level that indicates event criticality as follows:
 - Informational.
 - Minor.

- Major.
- 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 displays in the event log in hexadecimal format.
- **Distribution**-check marks in associated fields indicate where the event code is reported (director, HAFM server, or host).

System Events (000 through 199)

Event Code: 001							
Message:	System power-down.						
Severity:	Informational.						
Explanation:	The director was powered off or disconnected from the facility AC power source. The event code is distributed the next time the director 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:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 010							
Message:	Login Server unable to synchronize databases.						
Severity:	Minor.						
Explanation:	Following a CTP card reset or replacement, the Login Server attempted to acquire an up-to-date copy of its databases from the other CTP card, but failed. 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 HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		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 a CTP card failover or replacement, 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 HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓		

Event Code: 020							
Message:	Name Server unable to synchronize databases.						
Severity:	Minor.						
Explanation:	Following a CTP card reset or replacement, the Name Server attempted to acquire an up-to-date copy of its databases from the other CTP card, but failed. 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 HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		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 a CTP card failover or replacement, 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 HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		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 <i>Product Manager</i> application are allowed.						
Action:	Add the community name to the SNMP configuration using the <i>Product Manager</i> application.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 050							
Message:	Management Server unable to synchronize databases.						
Severity:	Minor.						
Explanation:	Following a CTP card reset or replacement, the Management Server attempted to acquire an up-to-date copy of its databases from the other CTP card, but failed. 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 HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		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 a CTP card failover or replacement, 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 HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		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 HP Services 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_ASYNC_STATUS_REPORTING . Mode register update: subcomponent_id is eMS_ELR_MODE_REGISTER_UPDATE .						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓			✓	

Event Code: 060							
Message:	Fabric Controller unable to synchronize databases.						
Severity:	Minor.						
Explanation:	Following a CTP card reset or replacement, the Fabric Controller attempted to acquire an up-to-date copy of its databases from the other CTP card, but failed. 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 HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		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 a CTP card failover or replacement, 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 HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		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 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 directors or switches 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:	Director		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 director. 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:	Director		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 director E_Port recognized an incompatibility with an attached fabric element (director or switch), preventing the director 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 switch). Refer to the event data for the segmentation reason.
Action:	Action depends on the segmentation reason specified in the event data.
Event Data:	<p>The first byte of event data (byte 0) specifies the E_Port number. The fifth byte (byte 4) specifies the segmentation reason as follows:</p> <p>1 = Incompatible operating parameters. Either the resource allocation time out value (R_A_TOV) or error detect time out value (E_D_TOV) is inconsistent between the Director 2/140 and another fabric element (director or switch). Modify the R_A_TOV and E_D_TOV to make the values consistent for all fabric directors and switches.</p> <p>2 = Duplicate domain ID. The Director 2/140 has the same preferred domain ID as another fabric element (director or switch). Modify the director's Domain ID to make it unique.</p> <p>3 = Incompatible zoning configurations. The same name is applied to a zone for the Director 2/140 and another fabric element (director or 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.</p> <p>4 = Build fabric protocol error. A protocol error was detected during incorporation of the Director 2/140 into the fabric. Disconnect the E_Port link, reconnect the link, and initial program load (IPL) the director. If the condition persists, perform the data collection procedure and return the Zip disk to HP support personnel.</p> <p>5 = No principal switch. No director or switch in the fabric can become the principal switch. Modify the switch priority to any value other than 255.</p> <p>6 = No response from attached switch (hello timeout). The Director 2/140 periodically verifies operation of attached fabric elements (directors or switches). The director E_Port (at the operational director) times out and segments if the attached device does not respond. Check the status of the attached director or switch. If the condition persists, perform the data collection procedure (at the attached device) and return the Zip disk to HP support personnel.</p> <p>7 = ELP retransmission failure timeout. A Director 2/140 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 switch). However, because of the problem, the director did not receive responses to the ELP frames, and did not receive a fabric login (FLOGI) frame. After five ELP transmission attempts, the director E_Port (failed director) times out and segments. Go to MAP 0000: Start MAP to perform hardware fault isolation at the failed director.</p>

Event Code: 070 (continued)							
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 071	
Message:	Director is isolated.
Severity:	Informational.
Explanation:	The director is isolated from other fabric elements (directors or switches). 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:	<p>The first byte of event data (byte 0) specifies the E_Port number. The fifth byte (byte 4) specifies the segmentation reason as follows:</p> <p>1 = Incompatible operating parameters. Either the resource allocation time out value (R_A_TOV) or error detect time out value (E_D_TOV) is inconsistent between the Director 2/140 and another fabric element (director or switch). Modify the R_A_TOV and E_D_TOV to make the values consistent for all fabric directors and switches.</p> <p>2 = Duplicate domain ID. The Director 2/140 has the same preferred domain ID as another fabric element (director or switch). Modify the director's Domain ID to make it unique.</p> <p>3 = Incompatible zoning configurations. The same name is applied to a zone for the Director 2/140 and another fabric element (director or 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.</p>

Event Code: 071 (continued)							
Event Data (continued):	<p>4 = Build fabric protocol error. A protocol error was detected during incorporation of the Director 2/140 into the fabric. Disconnect the E_Port link, reconnect the link, and IPL the director. If the condition persists, perform the data collection procedure and return the Zip disk to HP support personnel.</p> <p>5 = No principal switch. No director or switch in the fabric can become the principal switch. Modify the switch priority to any value other than 255.</p> <p>6 = No response from attached switch (hello timeout). The Director 2/140 periodically verifies operation of attached fabric elements (directors or switches). The director E_Port (at the operational director) times out and segments if the attached device does not respond. Check the status of the attached director or switch. If the condition persists, perform the data collection procedure (at the attached device) and return the Zip disk to HP support personnel.</p> <p>7 = ELP retransmission failure timeout. A Director 2/140 that exhibits a hardware or link failure attempted to join a fabric and transmitted multiple ELP frames to a fabric element (director or switch). However, because of the problem, the director did not receive responses to the ELP frames, and did not receive an FLOGI frame. After five ELP transmission attempts, the director E_Port (failed director) times out and segments. Go to MAP 0000: Start MAP to perform hardware fault isolation at the failed director.</p>						
Distribution:	Director		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 director is attached (through an ISL) to an incompatible fabric element (director or switch).						
Action:	Disconnect the ISL.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		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 HP Services 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:	Director		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 HP Services support personnel.						
Event Data:	Byte 0 = E_Port number reporting the problem. Byte 1 = reserved.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 080							
Message:	Unauthorized worldwide name.						
Severity:	Informational.						
Explanation:	The worldwide name of the device or director plugged in the indicated port is not authorized for that port.						
Action:	Change the port binding definition or plug the correct device or director 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:	Director		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 director 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:	<p>The first byte of event data (byte 0) specifies the port number. The fifth byte (byte 4) specifies the isolation reason as follows:</p> <p>1 = Unknown - Isolation reason is unknown, but probably caused by failure of a device attached to the director through an E_Port connection. Fault isolate the failed device or contact support personnel to report the problem.</p> <p>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.</p> <p>3 = Incompatible switch - The director returned a <i>Process ELP Reject - Unable to Process</i> reason code because the attached fabric element is not compatible. Set the director operating mode to Open Fabric 1.0 if connected to an open-fabric compliant product manufactured by a different vendor.</p> <p>4 = Incompatible switch - The director returned a <i>Process ELP Reject - Invalid Revision Level</i> reason code because the attached fabric element is not compatible. Set the director operating mode to Open Fabric 1.0 if connected to an open-fabric compliant product manufactured by a different vendor.</p> <p>5 = Loopback plug connected - A loopback plug is connected to the port with no diagnostic test running. Remove the loopback plug.</p> <p>6 = N_Port connection not allowed - The director is connected to a fabric element through a port configured as an F_port. Change the port type to E_Port.</p> <p>7 = Non-HP switch at other end - The attached fabric element is not an HP product. Set the director operating mode to Open Fabric 1.0 if connected to an open-fabric compliant product manufactured by a different vendor.</p> <p>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.</p>						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 090							
Message:	Database replication time out.						
Severity:	Minor						
Explanation:	Replication of a Fabric Services database from master CTP to backup has timed out. The backup CTP has been dumped and IPLed. After the backup CTP completes the IPL, its databases will be brought up to date and replication will resume.						
Action:	Perform a data collection for this switch using the <i>HAFM</i> application, saving the data file to the HAFM server Zip drive, and return the Zip disk to HP support personnel.						
Event Data:	Bytes 0-3 : Type of replication operation that timed out.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error Light	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	4	✓	✓	4		

Event Code: 091							
Message:	Database replication discontinued.						
Severity:	Informational						
Explanation:	Replication of Fabric Services databases from master CTP to backup has been discontinued because the backup CTP has failed or been removed.						
Action:	<p>This Event will occur any time the backup CTP fails or is removed and does not require any additional action; when the backup CTP is recovered/replaced, its databases will be brought up to date and replication will resume.</p> <p>If this Event occurs without the backup CTP failing or being removed, perform a data collection operation for this switch using the <i>HAFM</i> application, saving the data file to the HAFM server Zip drive, and return the Zip disk to HP support personnel.</p>						
Event Data:	None						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 120							
Message:	Error detected while processing system management command.						
Severity:	Informational.						
Explanation:	This event occurs when the director receives an HAFM Management command that violates specified boundary conditions, typically as a result of a network error. The director rejects the command, drops the director-to-HAFM server Ethernet link, and forces error recovery processing. When the link recovers, the command can be retried.						
Action:	No action is required for an isolated event. If this event persists, perform a data collection for this director using the <i>HAFM</i> application, save the data file to the HAFM server Zip drive, and return the Zip drive to HP Services support personnel.						
Event Data:	No supplementary data included with the event.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 121							
Message:	Zone set activation failed - zone set too large.						
Severity:	Informational.						
Explanation:	This event occurs when the director receives a zone set activation command that exceeds the size supported by the director. The director rejects the command, drops the director-to-HAFM server Ethernet link, and forces error recovery processing. When the link recovers, the command can be modified and retried.						
Action:	Reduce the size of the zone set to conform to the limit specified, then retry the activation command.						
Event Data:	No supplementary data included with the event.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

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 director.						
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 HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		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 director.						
Action:	Replace the failed power supply. Perform the data collection procedure and return the Zip disk and failed power supply to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 202							
Message:	Power supply thermal failure.						
Severity:	Major.						
Explanation:	The thermal sensor associated with a power supply indicates an overheat condition that shut down the power supply. The second power supply assumes the full operating load for the director.						
Action:	Replace the failed power supply. Perform the data collection procedure and return the Zip disk and failed power supply to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		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 director.						
Action:	No action required.						
Event Data:	No supplementary data included with the event.						
Distribution:	Director		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 director.						
Action:	No action required.						
Event Data:	No supplementary data included with the event.						
Distribution:	Director		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 director was powered on and operational. The second power supply assumes the full operating load for the director.						
Action:	No action required or install an operational power supply.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		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 director powered on and operational. Both power supplies adjust to share operating load for the director.						
Action:	No action required.						
Event Data:	No supplementary data included with the event.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 208							
Message:	Power supply false shutdown.						
Severity:	Major.						
Explanation:	Director operational firmware nearly shut down the indicated power supply as a result of failure or facility power loss or voltage fluctuation.						
Action:	Confirm operation of facility power. If subsequent power loss events occur, replace the failed power supply. Perform the data collection procedure and return the Zip disk and failed power supply to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		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 three) failed or is rotating at insufficient angular velocity. The remaining fans are operational. The amber LED illuminates at the rear of the fan module associated with the failed fan.						
Action:	Replace the indicated fan module.						
Event Data:	The first byte of event data (byte 0) specifies the failed fan number.						
Distribution:	Director		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 three) failed or are rotating at insufficient angular velocity. The remaining fans are operational. The amber LED illuminates at the rear of the fan modules associated with the failed fans.						
Action:	Replace the indicated fan modules.						
Event Data:	The first byte of event data (byte 0) specifies the failed fan numbers.						
Distribution:	Director		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 three) failed or are rotating at insufficient angular velocity. The remaining fans are operational. The amber LED illuminates at the rear of the fan modules associated with the failed fans.						
Action:	Replace the indicated fan modules.						
Event Data:	The first byte of event data (byte 0) specifies the failed fan numbers.						
Distribution:	Director		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 three) failed or are rotating at insufficient angular velocity. The remaining fans are operational. The amber LED illuminates at the rear of both fan modules.						
Action:	Replace the indicated fan modules.						
Event Data:	The first byte of event data (byte 0) specifies the failed fan numbers.						
Distribution:	Director		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 three) failed or are rotating at insufficient angular velocity. The remaining fan is operational. The amber LED illuminates at the rear of both fan modules.						
Action:	Replace the indicated fan modules.						
Event Data:	The first byte of event data (byte 0) specifies the failed fan numbers.						
Distribution:	Director		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 three cooling fans failed or are rotating at insufficient angular velocity. The amber LED illuminates at the rear of both fan modules.						
Action:	Replace the indicated fan modules.						
Event Data:	The first byte of event data (byte 0) specifies the failed fan numbers.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 310							
Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	One cooling fan (out of three) recovered or the associated fan module was replaced. All fans are operational.						
Action:	No action required.						
Event Data:	The first byte of event data (byte 0) specifies the recovered fan number.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 311							
Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	Two cooling fans (out of three) recovered or the associated fan modules 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.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error Indicator	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 312							
Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	Three cooling fans (out of three) recovered or the associated fan modules 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.						
Distribution:	Director		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 three) recovered or the associated fan modules 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.						
Distribution:	Director		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 three) recovered or the associated fan modules 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.						
Distribution:	Director		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 three cooling fans recovered or the associated fan modules 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.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 320							
Message:	Fan module removed.						
Severity:	Major.						
Explanation:	A fan module was removed with the director powered on and operational.						
Action:	Replace the indicated fan module.						
Event Data:	No supplementary data included with the event.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓				

Event Code: 321							
Message:	Fan module installed.						
Severity:	Informational.						
Explanation:	A fan module was installed with the director powered on and operational.						
Action:	No action required.						
Event Data:	No supplementary data included with the event.						
Distribution:	Director		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:	Replace the failed FRU with a functional FRU. Perform the data collection procedure and return the Zip disk and faulty FRU to HP support personnel.						
Event Data:	Byte 0 = FRU code as follows: 01 = backplane, 02 = CTP card, 03 = SBAR assembly, 05 = fan module, 06 = power supply, and 08 through 22 = UPM cards. Byte 1 = FRU slot number.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 410							
Message:	CTP card reset.						
Severity:	Informational.						
Explanation:	The indicated CTP card reset after a director power-on, CTP card installation, hardware IML (CTP card faceplate), or software IPL. An IPL can be user-initiated at the <i>Product Manager</i> application, or occur automatically after a firmware fault (event code 411). The event data indicates the type of reset.						
Action:	No action required.						
Event Data:	Byte 0 = reset type as follows: 00 = power-on hot-insert, 02 = IML, 04 = IPL, 08 = reset by other CTP card, 40 = partition switch, or 80 = dual CTP card hot-insert.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 411							
Message:	Firmware fault.						
Severity:	Major.						
Explanation:	Firmware executing on the indicated CTP card encountered an unexpected operating condition and dumped the operating state to FLASH memory for retrieval and analysis. The dump file is automatically transferred from the director to the HAFM server, where it is stored for retrieval through the data collection procedure. A non-disruptive failover to the backup CTP card occurs. When the dump and subsequent IPL complete, the faulty CTP card reinitializes to become a the backup.						
Action:	Perform the data collection procedure and return the Zip disk to HP support personnel.						
Event Data:	Bytes 0 through 3 = fault identifier, least significant byte first.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 413								
Message:	Backup CTP card POST failure.							
Severity:	Major.							
Explanation:	A backup CTP card was installed in the director and failed POSTs.							
Action:	Replace the indicated CTP card with a functional card. Perform the data collection procedure and return the Zip disk and faulty card to HP support personnel.							
Event Data:	No supplementary data included with this event.							
Distribution:	Director		HAFM Server			Host		
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident	
	✓	✓	✓	✓	✓	✓		

Event Code: 414								
Message:	Backup CTP card failure.							
Severity:	Major.							
Explanation:	The backup CTP card failed.							
Action:	Replace the indicated CTP card with a functional card. Perform the data collection procedure and return the Zip disk and faulty card to HP support personnel.							
Event Data:	No supplementary data included with this event.							
Distribution:	Director		HAFM Server			Host		
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident	
	✓	✓	✓	✓	✓	✓		

Event Code: 415							
Message:	Backup CTP card removed.						
Severity:	Informational.						
Explanation:	The backup CTP card was removed while the director was powered on and operational.						
Action:	No action required or install an operational backup CTP card.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 416							
Message:	Backup CTP card installed.						
Severity:	Informational.						
Explanation:	A backup CTP card was installed while the director was powered on and operational.						
Action:	No action required.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 417							
Message:	CTP card firmware synchronization initiated.						
Severity:	Informational.						
Explanation:	The active CTP card initiated a firmware synchronization with the backup CTP card.						
Action:	No action required.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 418							
Message:	User-initiated CTP card switchover.						
Severity:	Informational.						
Explanation:	The backup CTP card became the active CTP card after a user-initiated switchover. The previously active CTP card is now the backup CTP card.						
Action:	No action required.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 420							
Message:	Backup CTP card non-volatile memory failure.						
Severity:	Major.						
Explanation:	The backup CTP card detected a non-volatile memory failure. The failure has no impact on the active CTP card.						
Action:	Replace the indicated CTP card with a functional card. Perform the data collection procedure and return the Zip disk and faulty card to HP support personnel.						
Event Data:	Byte 0 = non-volatile memory area identifier.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 421							
Message:	Firmware download complete.						
Severity:	Informational.						
Explanation:	A director firmware version was downloaded from the HAFM server or Embedded Web Server interface. 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 - 12 = build ID (bbbb).						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 422							
Message:	CTP firmware synchronization complete.						
Severity:	Informational.						
Explanation:	Active CTP card synchronization with the backup CTP card complete.						
Action:	No action required.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		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 director.						
Action:	No action required.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 430							
Message:	Excessive Ethernet transmit errors.						
Severity:	Informational.						
Explanation:	Transmit error counters for the active CTP card Ethernet adapter (sum of all counters) exceeded a threshold. This does not indicate a CTP card failure; it indicates a problem with the Ethernet cable, hub, or device on the same Ethernet segment. Event data counters are represented in hexadecimal format with the least significant byte first.						
Action:	Verify the Ethernet cable, hub, and other devices are properly connected and operational.						
Event Data:	<p>Bytes 0 through 3 = sum of all transmit errors (total_xmit_error).</p> <p>Bytes 4 through 7 = frame count where Ethernet adapter does not detect carrier sense at preamble end (loss_of_CRSS_cnt).</p> <p>Bytes 8 through 11 = frame count where Ethernet adapter does not detect a collision within 64 bit times at transmission end (SQE_error_cnt).</p> <p>Bytes 12 through 15 = frame count where Ethernet adapter detects a collision more than 512 bit times after first preamble bit (out_of_window_cnt). Frame not transmitted.</p> <p>Bytes 16 through 19 = frame count where transmission is more than 26 ms (jabber_cnt). Frame not transmitted.</p> <p>Bytes 20 through 23 = frame count where Ethernet adapter encounters 16 collisions while attempting to transmit a frame (16coll_cnt). Frame not transmitted.</p>						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 431							
Message:	Excessive Ethernet receive errors.						
Severity:	Informational.						
Explanation:	Receive error counters for the active CTP card Ethernet adapter (sum of all counters) exceeded a threshold. This does not indicate a CTP card failure; it indicates a problem with the Ethernet cable, hub, or device on the same Ethernet segment. Event data counters are represented in hexadecimal format with the least significant byte first.						
Action:	Verify the Ethernet cable, hub, and other devices are properly connected and operational.						
Event Data:	<p>Bytes 0 through 3 = sum of all receive errors (total_recv_error).</p> <p>Bytes 4 through 7 = frame count where received frame had from 1 to 7 bits after last received full byte (dribble_bits_cnt). CRC error counter updated but frame not processed.</p> <p>Bytes 8 through 11 = frame count where received frame had bad CRC (CRC_error_cnt). Frame not processed.</p> <p>Bytes 12 through 15 = frame count received with less than 64 bytes (runt_cnt). Broadcast frames count but do not contribute to threshold. Frame not processed.</p> <p>Bytes 16 through 19 = frame count received with more than 1518 bytes (extra_data_cnt). Broadcast frames count but do not contribute to threshold. Frame not processed.</p>						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 432							
Message:	Ethernet adapter reset.						
Severity:	Minor.						
Explanation:	The active CTP card Ethernet adapter was reset in response to an internally detected error. A card failure is not indicated. The director-to-HAFM server connection terminates, but automatically recovers after the reset.						
Action:	Perform the data collection procedure and return the Zip disk to HP support personnel.						
Event Data:	Bytes 0 through 3 = reason for adapter reset, least significant byte first (reset_error_type) 1 = completion notification for timed-out frame transmission.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 433							
Message:	Nonrecoverable Ethernet fault.						
Severity:	Major.						
Explanation:	A nonrecoverable error was detected on the CTP card Ethernet adapter and the LAN connection to the HAFM server or Internet terminated. All Fibre Channel switching functions remain unaffected. This event only occurs on a director with a single CTP card. Because Ethernet communication is lost, no failure indication is externally reported.						
Action:	Replace the CTP card with a functional card. Perform the data collection procedure and return the Zip disk and faulty card to HP Services support personnel.						
Event Data:	Byte 0 = LAN error type, where 01 = hard failure and 04 = registered fault. Byte 1 = LAN error subtype (internally defined). Byte 2 = LAN fault identifier (internally defined).						
Distribution:	Director		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 card error.						
Action:	Replace the indicated CTP card with a functional card. Perform the data collection procedure and return the Zip disk and faulty card to HP support personnel.						
Event Data:	Byte 0 = CTP slot position (00 or 01). Byte 1 = engineering reason code Bytes 4 through 7 = elapsed millisecond tick count.						
Distribution:	Director		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 CTP card 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. Byte 14 = participating SBAR assembly. Bytes 16 and 17 = high-availability error callout #3. Bytes 18 and 19 = high-availability error callout #4.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 450							
Message:	Serial number mismatch detected.						
Severity:	Informational						
Explanation:	This event occurs when the sequence number or OEM serial number in the system VPD (read from the backplane) does not match the sequence number and serial Number that was saved in NVRAM the last time the switch was IPLed. This event will occur normally when a CTP is moved from one switch to the master position of another switch. This event may occur abnormally when a hardware problem is causing a problem reading the system VPD from the backplane.						
Action:	None. Any configured feature keys will be cleared, configuration information will be synched with the backplane VPD, and the CTP will automatically be IPLed.						
Event Data:	Bytes 0-12 are the sequence number from the system VPD. Bytes 13-31 are the OEM serial number obtained from the system VPD.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 451							
Message:	Switch speed incompatibility detected.						
Severity:	Informational						
Explanation:	The event occurs when the configured switch speed saved in NVRAM conflicts with the speed capability of the switch. This event may occur when backup CTP hardware running an early version of software (below 1.3) is improperly synchronized with a CTP operating at greater than 1Gb/s.						
Action:	None. Switch speed configuration and port speed configuration data will be set to a level that is compatible with the CTP and the CTP will automatically be IPLed.						
Event Data:	None						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 452							
Message:	Backup CTP incompatible with configured systems settings.						
Severity:	Informational						
Explanation:	This event occurs when the backup CTP is failed as a result of being incompatible with current system settings. Normally this event will be generated following a hot-plug or power on reset. (This event usually occurs when a CTP is installed into a system operating at a switch speed not supported by the CTP). This event should be followed by a 414 event.						
Action:	Replace the backup CTP with a version of hardware capable of supporting the user-configured settings or adjust the user settings to be compatible with the backup CTP and reseal the backup CTP.						
Event Data:	None						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 453							
Message:	New feature key installed.						
Severity:	Informational.						
Explanation:	This event occurs when a new feature key is installed from the HAFM server or Embedded Web Server interface. The director performs an IPL when the feature key is enabled. Event data indicates which feature or features are installed.						
Action:	No action required.						
Event Data:	Byte 0 = feature description as follows: 00 through 04 = Flexport, 06 = open-system management server. Byte 1 = feature description as follows: 06 = SANtegrity.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 460							
Message:	Management request out of range.						
Severity:	Informational						
Explanation:	This event occurs when requests passed from the managing tool (generally HAFM) to the switch do not meet data boundary specifications. This event is most likely to be triggered if a user attempt to activate a zone set that is larger than the maximum defined zone set size.						
Action:	The director found request data from the management tool to be larger or smaller than expected. The connection to the management tool will be temporarily lost. After the link is re-established, verify that all information changed in the managing tool is within the specified ranges. For example, verify that the zones and zone members in a zone set fall within the limits stated in the user manual. Try sending the request again.						
Event Data:	None						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

UPM Card Events (500 through 599)

Event Code: 500							
Message:	UPM card hot-insertion initiated.						
Severity:	Informational						
Explanation:	Installation of an UPM card was initiated with the director powered on and operational. The event indicates that operational firmware detected the presence of the UPM card, but the card is not seated. When the card is seated in the director chassis and identified by firmware, an event code 501 is generated.						
Action:	If event code 501 follows this event and the amber LED on the UPM card extinguishes, the replacement card is installed and no additional action is required. If event code 501 does not follow this event, re-seat the UPM card. If event code 501 still does not display, replace the UPM card.						
Event Data:	Byte 0 = UPM slot position (00 through 22). Bytes 4 through 7 = elapsed millisecond tick count.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 501							
Message:	UPM card recognized.						
Severity:	Informational.						
Explanation:	An UPM card is installed and recognized by director operational firmware.						
Action:	No action required.						
Event Data:	Byte 0 = UPM slot position (00 through 22). Bytes 4 through 7 = elapsed millisecond tick count.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 502							
Message:	UPM card anomaly detected.						
Severity:	Informational.						
Explanation:	The CTP card detected a deviation in the normal operating mode or status of the indicated four-port UPM card.						
Action:	No action required. An event code 504 is generated if the UPM card fails.						
Event Data:	<p>Byte 0 = UPM slot position (00 through 22).</p> <p>Byte 1 = engineering reason code.</p> <p>Bytes 4 through 7 = elapsed millisecond tick count.</p> <p>Bytes 8 and 9 = high-availability error callout #1</p> <p>Bytes 10 and 11 = high-availability error callout #2.</p> <p>Byte 12 = detecting port.</p> <p>Byte 13 = connected port.</p> <p>Byte 14 = participating SBAR assembly.</p> <p>Bytes 16 and 17 = high-availability error callout #3.</p> <p>Bytes 18 and 19 = high-availability error callout #4.</p>						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 503							
Message:	UPM card hot-removal completed.						
Severity:	Informational.						
Explanation:	An UPM card was removed with the director powered on and operational.						
Action:	No action required.						
Event Data:	Byte 0 = UPM slot position (00 through 22). Bytes 4 through 7 = elapsed millisecond tick count.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 504							
Message:	UPM card failure.						
Severity:	Major.						
Explanation:	The indicated UPM card failed.						
Action:	Replace the indicated UPM card with a functional UPM card of the same type. Perform the data collection procedure and return the Zip disk and faulty card to HP support personnel.						
Event Data:	Byte 0 = UPM slot position (00 through 22). Byte 1 = engineering reason code. Bytes 4 through 7 = elapsed millisecond tick count. Bytes 8 through 11 = reason code specific data.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 505							
Message:	UPM card revision not supported.						
Severity:	Minor.						
Explanation:	The indicated UPM card is not recognized and the four ports display uninstalled to the director firmware.						
Action:	Ensure the director model supports the operating firmware version. If the firmware version is supported, replace the UPM card with a functional card. Perform the data collection procedure and return the Zip disk and faulty card to HP support personnel.						
Event Data:	Byte 0 = UPM slot position (00 through 22). Bytes 4 through 7 = elapsed millisecond tick count. Bytes 8 and 9 = detected module identifier.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 506							
Message:	Fibre Channel port failure.						
Severity:	Major.						
Explanation:	A Fibre channel port on an UPM card failed. The amber LED corresponding to the port illuminates to indicate the failure. Other ports remain operational if their LEDs are extinguished.						
Action:	Replace the indicated UPM card with a functional UPM card of the same type. Perform the data collection procedure and return the Zip disk and faulty card to HP support personnel.						
Event Data:	Byte 0 = port number (00 through 143). 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 = speed capabilities.						
Distribution:	Director		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 143). 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:	Director		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 card 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 143). 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. Byte 14 = participating SBAR assembly. Bytes 16 and 17 = high-availability error callout #3. Bytes 18 and 19 = high-availability error callout #4.						
Distribution:	Director		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 director 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 143). Bytes 4 through 7 = elapsed millisecond tick count.						
Distribution:	Director		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:	Director firmware detected a 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 143). Byte 1 = engineering reason code. Bytes 4 through 7 = elapsed millisecond tick count.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 513							
Message:	SFP optical transceiver hot-removal completed.						
Severity:	Informational.						
Explanation:	A SFP optical transceiver was removed while the director was powered on and operational.						
Action:	No action required.						
Event Data:	Byte 0 = port number (00 through 143). Bytes 4 through 7 = elapsed millisecond tick count.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 514							
Message:	SFP optical transceiver failure.						
Severity:	Major.						
Explanation:	A SFP optical transceiver in an UPM card failed. The amber LED corresponding to the port illuminates to indicate the failure. Other ports remain operational if their LEDs are extinguished.						
Action:	Replace the failed transceiver with a functional transceiver of the same type.						
Event Data:	Byte 0 = port number (00 through 143). Byte 1 = engineering reason code. Bytes 4 through 7 = elapsed millisecond tick count.						
Distribution:	Director		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) or Fibre Connection (FICON) 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) or the FICON architecture document (FICON). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. See MAP 0000: Start MAP on page 2-12 for instructions.						
Event Data:	Refer to the T11/99-017v0 or FICON architecture document for the specific link incident record format.						
Distribution:	Director		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 or FICON 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) or the FICON architecture document (FICON). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. See MAP 0000: Start MAP on page 2-12 for instructions.						
Event Data:	Refer to the T11/99-017v0 or FICON architecture document for the specific link incident record format.						
Distribution:	Director		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 or FICON 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) or the FICON architecture document (FICON). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. See MAP 0000: Start MAP on page 2-12 for instructions.						
Event Data:	Refer to the T11/99-017v0 or FICON architecture document for the specific link incident record format.						
Distribution:	Director		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 or FICON 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) or the FICON architecture document (FICON). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. See MAP 0000: Start MAP on page 2-12 for instructions.						
Event Data:	Refer to the T11/99-017v0 or FICON architecture document for the specific link incident record format.						
Distribution:	Director		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 or FICON 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) or the FICON architecture document (FICON). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. See MAP 0000: Start MAP on page 2-12 for instructions.						
Event Data:	Refer to the T11/99-017v0 or FICON architecture document for the specific link incident record format.						
Distribution:	Director		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 or FICON 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) or the FICON architecture document (FICON). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. See MAP 0000: Start MAP on page 2-12 for instructions.						
Event Data:	Refer to the T11/99-017v0 or FICON architecture document for the specific link incident record format.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
			✓				✓

SBAR Assembly Events (600 through 699)

Event Code: 600							
Message:	SBAR assembly hot-insertion initiated.						
Severity:	Informational						
Explanation:	Installation of a backup SBAR was initiated with the director powered on and operational. The event indicates that operational firmware detected the presence of the SBAR, but the SBAR is not seated. When the SBAR is seated in the director chassis and identified by firmware, an event code 601 is generated.						
Action:	If event code 601 follows this event and the amber LED on the SBAR assembly extinguishes, the replacement SBAR assembly is installed and no additional action is required. If event code 601 does not follow this event, re-seat the SBAR assembly. If event code 601 still does not display, replace the SBAR assembly.						
Event Data:	Byte 0 = SBAR slot position (00 or 01). Bytes 4 through 7 = elapsed millisecond tick count.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 601							
Message:	SBAR assembly recognized.						
Severity:	Informational.						
Explanation:	An SBAR assembly is installed and recognized by director operational firmware.						
Action:	No action required.						
Event Data:	Byte 0 = SBAR slot position (00 or 01). Bytes 4 through 7 = elapsed millisecond tick count.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 602							
Message:	SBAR assembly anomaly detected.						
Severity:	Informational.						
Explanation:	Director operational firmware detected a deviation in the normal operating mode or operating status of the indicated SBAR assembly.						
Action:	No action required. An event code 604 is generated if the SBAR assembly fails.						
Event Data:	<p>Byte 0 = SBAR slot position (00 or 01).</p> <p>Byte 1 = anomaly reason code.</p> <p>Bytes 4 through 7 = elapsed millisecond tick count.</p> <p>Bytes 8 and 9 = high-availability error callout #1.</p> <p>Bytes 10 and 11 = high-availability error callout #2.</p> <p>Byte 12 = detecting port.</p> <p>Byte 13 = connected port.</p> <p>Byte 14 = participating SBAR assembly.</p> <p>Bytes 16 and 17 = high-availability error callout #3.</p> <p>Bytes 18 and 19 = high-availability error callout #4.</p>						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 603							
Message:	SBAR assembly hot-removal completed.						
Severity:	Informational.						
Explanation:	An SBAR assembly was removed with the director powered on and operational.						
Action:	No action required.						
Event Data:	Byte 0 = SBAR slot position (00 or 01). Bytes 4 through 7 = elapsed millisecond tick count.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 604							
Message:	SBAR assembly failure.						
Severity:	Major.						
Explanation:	The indicated SBAR assembly failed. If the active SBAR assembly fails, the backup SBAR takes over operation. If the backup SBAR assembly fails, the active SBAR is not impacted.						
Action:	Replace the failed SBAR assembly with a functional assembly. Perform the data collection procedure and return the Zip disk and faulty assembly to HP support personnel.						
Event Data:	Byte 0 = SBAR slot position (00 or 01). Byte 1 = engineering failure reason code. Bytes 4 through 7 = elapsed millisecond tick count. Bytes 8 through 11 = event code specific data.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 605							
Message:	SBAR assembly revision not supported.						
Severity:	Minor.						
Explanation:	The indicated SBAR assembly is not recognized and displays uninstalled to the director firmware.						
Action:	Ensure the director model supports the operating firmware version. If the firmware version is supported, replace the SBAR assembly with a functional assembly. Perform the data collection procedure and return the Zip disk and faulty assembly to HP support personnel.						
Event Data:	Byte 0 = SBAR slot position (00 or 01). Bytes 4 through 7 = elapsed millisecond tick count. Bytes 8 and 9 = detected module identifier.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓		✓				

Event Code: 607							
Message:	Director contains no operational SBAR assemblies.						
Severity:	Severe.						
Explanation:	The director firmware does not recognize an installed SBAR assembly.						
Action:	Install at least one functional SBAR assembly and power-on reset (POR) the director.						
Event Data:	Bytes 4 through 7 = elapsed millisecond tick count.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓		

Event Code: 608

Message:	User initiated SBAR switch-over.						
Severity:	Informational.						
Explanation:	The backup SBAR has become the active SBAR at a user's request. The previously active SBAR is now the backup SBAR.						
Action:	No action required.						
Event Data:	There is no supplementary data included with this event.						
Distribution:	Director		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: 800							
Message:	High temperature warning (UPM card thermal sensor).						
Severity:	Major.						
Explanation:	The thermal sensor associated with an UPM card indicates the warm temperature threshold was reached or exceeded.						
Action:	Replace the indicated UPM card with a functional UPM card of the same type. Perform the data collection procedure and return the Zip disk and faulty card to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 801							
Message:	Critically hot temperature warning (UPM card thermal sensor).						
Severity:	Major.						
Explanation:	The thermal sensor associated with an UPM card indicates the hot temperature threshold was reached or exceeded.						
Action:	Replace the indicated UPM card with a functional UPM card of the same type. Perform the data collection procedure and return the Zip disk and faulty card to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 802							
Message:	UPM card shutdown due to thermal violation.						
Severity:	Major.						
Explanation:	An UPM card failed and was powered off because of excessive heat. This event follows an indication that the hot temperature threshold was reached or exceeded (event code 801).						
Action:	Replace the failed UPM card with a functional UPM card of the same type. Perform the data collection procedure and return the Zip disk and faulty card to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 805							
Message:	High temperature warning (SBAR assembly thermal sensor).						
Severity:	Major.						
Explanation:	The thermal sensor associated with an SBAR assembly indicates the warm temperature threshold was reached or exceeded.						
Action:	Replace the indicated SBAR assembly with a functional assembly. Perform the data collection procedure and return the Zip disk and faulty assembly to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 806							
Message:	Critically hot temperature warning (SBAR assembly thermal sensor).						
Severity:	Major.						
Explanation:	The thermal sensor associated with an SBAR assembly indicates the hot temperature threshold was reached or exceeded.						
Action:	Replace the indicated SBAR assembly with a functional assembly. Perform the data collection procedure and return the Zip disk and faulty assembly to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 807							
Message:	SBAR assembly shutdown due to thermal violation.						
Severity:	Major.						
Explanation:	An SBAR assembly failed and was powered off because of excessive heat. This event follows an indication that the hot temperature threshold was reached or exceeded (event code 806). If the active SBAR assembly fails, the backup SBAR takes over operation. If the backup SBAR assembly fails, the active SBAR is not impacted.						
Action:	Replace the failed SBAR assembly with a functional assembly. Perform the data collection procedure and return the Zip disk and faulty assembly to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

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 indicated CTP card with a functional card. Perform the data collection procedure and return the Zip disk and faulty card to HP support personnel.							
Event Data:	No supplementary data included with this event.							
Distribution:	Director		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 indicated CTP card with a functional card. Perform the data collection procedure and return the Zip disk and faulty card to HP support personnel.							
Event Data:	No supplementary data included with this event.							
Distribution:	Director		HAFM Server			Host		
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident	
	✓	✓	✓	✓	✓	✓		

Event Code: 812							
Message:	CTP card shutdown due to thermal violation.						
Severity:	Major.						
Explanation:	A CTP card failed and was powered off because of excessive heat. This event follows an indication that the hot temperature threshold was reached or exceeded (event code 811). If the active CTP card fails, the backup card takes over operation. If the backup CTP card fails, the active card is not impacted.						
Action:	Replace the failed CTP card with a functional card. Perform the data collection procedure and return the Zip disk and faulty card to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 850							
Message:	System shutdown due to CTP card thermal violations.						
Severity:	Severe.						
Explanation:	The director powered off because of excessive thermal violations on the last operational CTP card.						
Action:	Replace the failed CTP card with a functional card. Perform the data collection procedure and return the Zip disk and faulty card to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		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 guide or related to this product and is not a comprehensive glossary of computer terms.

access control

Method of control (with associated permissions) by which a set of devices can access other devices across a network. *See also* persistent binding and zoning.

active FRU

A redundant field-replaceable unit that is operating as the active and not the backup FRU. *Contrast with* backup FRU.

active zone set

Single zone set that is active in a multi-switch fabric. It is created when you enable a specified zone set. This zone set is compiled by checking for undefined zones or aliases.

agent

Software that processes queries on behalf of an application and returns replies.

alarm

Simple network management protocol (SNMP) message notifying an operator of a network or device problem.

alias server

Fabric software facility that supports multicast group management.

allowed port connection

In S/390 mode, this attribute establishes dynamic connectivity capability.

arbitration

Process of selecting one device from a collection of devices that request service simultaneously.

audit log

Log summarizing actions (audit trail) made by the user.

authentication

Verification of identity for a person or process.

backplane

The backplane provides 48 VDC power distribution and connections for all logic cards.

backup FRU

When an active FRU fails, an identical backup FRU takes over operation automatically (failover) to maintain director and Fibre Channel link operation. *Contrast with* active FRU.

BB_Credit

See buffer-to-buffer credit.

beaconing

Use of light-emitting diodes on ports, port cards, field-replaceable units, and directors to aid in the fault-isolation process; when enabled, active beaconing causes LEDs to flash for selected components.

BER

See bit error rate.

bidirectional

In Fibre Channel, the capability to simultaneously communicate at maximum speeds in both directions over a link.

bit error rate (BER)

Ratio of received bits that contain errors to total of all bits transmitted.

blocked port

Devices communicating with the port are prevented from logging into the director or communicating with other devices attached to the director. A blocked port continuously transmits the offline sequence.

bridge

Device that connects and passes packets between two network segments that use the same communications protocol.

broadcast

Send a transmission to all N_Ports on a fabric. *See also* multicast.

broadcast frames

Data packet, also known as a broadcast packet, whose destination address specifies all computers on a network.

buffer

Storage area for data in transit. Buffers compensate for differences in processing speeds between devices. *See also* buffer-to-buffer credit.

buffer-to-buffer credit (BB_Credit)

Indicates the maximum number of frames a port can transmit without receiving a receive ready signal from the receiving device.

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.

channel

Point-to-point link that transports data from one point to the other.

channel path

A single interface between a central processor and one or more control units along which signals and data can be sent to perform I/O requests.

channel path identifier

In a channel system, a value assigned to each installed channel path of the system that uniquely identifies that path to the system.

channel wrap test

A diagnostic procedure that checks S/390 host-to-director connectivity by returning the output of the host as input. The test is host-initiated and transmits Fibre Channel frames to a director port. A director port enabled for channel wrapping echoes the frame back to the host.

class of Fibre Channel service

Defines the level of connection dedication, acknowledgment, and other characteristics of a connection. Class F, Class 2, and Class 3 services are supported.

Class F Fibre Channel service

Used by switches to communicate across interswitch links (ISLs) to configure, control, and coordinate a multi-switch fabric.

Class 2 Fibre Channel service

Provides a connectionless (not dedicated) service with notification of delivery or nondelivery between two N_Ports. In-order delivery of frames is not guaranteed.

Class 3 Fibre Channel service

Provides a connectionless (not dedicated) service without notification of delivery or nondelivery between two N_Ports. Also known as datagram.

community profile

Information that specifies which management objects are available to what management domain or SNMP community name.

concurrent maintenance

Ability to perform maintenance tasks, such as removal or replacement of field-replaceable units (FRUs), while normal operations continue without interruption. *See also* nondisruptive maintenance.

configuration data

Configuration data includes: identification data, port configuration data, operating parameters, 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 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.

connector

See optical fiber connector.

control processor (CTP) card

Circuit card that contains the director microprocessor. The CTP card also initializes hardware components of the system after power-on.

control unit

A device that controls the reading, writing, or displaying of data at one or more input/output units.

control unit port

An internal director port on the CTP card that communicates with the attached IBM S/390 or similar processor channels to report error conditions and link initialization.

CRC

See cyclic redundancy check.

CTP/CTP card

See control processor (CTP) card.

cyclic redundancy check (CRC)

System of error checking performed at both the sending and receiving station using the value of a particular character generated by a cyclic algorithm. When the values generated at each station are identical, data integrity is confirmed.

DASD

Acronym for direct access storage device.

datagram

See Class 3 Fibre Channel service.

default

Pertaining to an attribute, value, or option that is assumed when none is explicitly specified.

default zone

Contains all attached devices that are not members of a separate zone.

destination identifier (D_ID)

Address identifier that indicates the targeted destination of a data frame.

device

Product (server or storage), connected to a managed director, that is not controlled directly by the *Product Manager* application. See also node.

diagnostics

Procedures used by computer users and service personnel to diagnose hardware or software error conditions.

dialog box

Dialog box is a window containing informational messages or data fields to be modified or filled in with desired options.

D_ID

See destination identifier.

Director

An intelligent Fibre Channel switching device providing any-to-any port connectivity between nodes (end devices) on a switched fabric. The director sends data transmissions (data frames) between nodes in accordance with the address information present in the frame headers of those transmissions.

Director Product Manager application

See *Product Manager* application.

DNS name

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 ID

Number (1 through 31) that uniquely identifies a switch in a multi-switch fabric. A distinct domain ID is automatically allocated to each switch in the fabric by the principal switch.

domain name service (DNS)

See DNS name.

E_D_TOV

See error detect time-out value.

E_Port

See expansion port.

Embedded Web Server

Administrators or operators with a browser-capable PC and Internet connection can monitor and manage a director through an Embedded Web Server interface. The interface provides a GUI similar to the *Product Manager* application, and supports director configuration, statistics monitoring, and basic operation.

error detect time-out value (E_D_TOV)

User-specified value that defines the time a director waits for an expected response before declaring an error condition.

error message

Software message that indicates an error was detected. See also information message and warning message.

Ethernet

A widely implemented local area network (LAN) protocol that uses a bus or star topology and serves as the basis for the IEEE 802.3 standard, which specifies the physical and software layers. Baseband LAN allows multiple station access to the transmission medium at will without prior coordination and which avoids or resolves contention.

Ethernet hub

A device used to LAN-connect the HAFM server and managed directors.

event code

Error code that provides the operator with information concerning events that indicate degraded operation or failure of a director.

event log

Record of significant events that have occurred at the director, such as FRU failures, degraded operation, and port problems.

expansion port (E_Port)

Physical interface on a Fibre Channel switch within a fabric, that attaches to an expansion port (E_Port) on another Fibre Channel switch to form a multi-switch fabric. *See also* segmented E_Port.

fabric

Fibre Channel 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.

fabric element

An active switch, director, or node in a Fibre Channel switched fabric.

fabric port (F_Port)

Physical interface on the director that connects to a node port (N_Port) through a point-to-point full duplex connection.

failover

Automatic and nondisruptive transition of functions from an active FRU that has failed to a backup FRU.

FCC-IOC

See Fibre Channel input/output controller.

FE-MIB

See Fibre Channel fabric element.

fiber

Physical media types supported by the Fibre Channel specification, such as optical fiber, copper twisted pair, and coaxial cable.

fiber optics

Branch of optical technology concerned with the transmission of light pulses through fibers made of transparent materials such as glass, fused silica, and plastic.

fiber port module (FPM) card

Each fiber port module card provides four Channel connections through duplex small form factor pluggable (SFP) fiber-optic transceivers. 1 gigabit per second enabled. *See also* universal port module card.

Fibre Channel

Integrated set of standards recognized by the 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 input/output controller (FCC-IOC)

A device that controls the embedded Fibre Channel port and configures the ports' ASICs.

field-replaceable unit (FRU)

Assembly removed and replaced in its entirety when any one of its components fails.

firmware

Embedded program code that resides and executes on the director.

FPM card

See fiber port module card.

F_Port

See fabric port.

FICON

An IBM set of products and services 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 1 Gb/s bidirectional data transfer).

FICON Management Server

An optional feature that can be enabled on the director or switch through the *Product Manager* application. When enabled, host control and management of the director or switch is provided through an S/390 Parallel Enterprise or 2/Series Server attached to a director or switch port.

FRU

See field-replaceable unit.

gateway

A multi-homed host used to route network traffic from one network to another, and to pass network traffic from one protocol to another.

gateway address

A unique string of numbers (in the format xxx.xx.xxx.xxx) that identifies a gateway on the network.

generic port (G_Port)

Physical interface on a director 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.

G_Port

See generic port.

HAFM application

See HP StorageWorks HA-Fabric Manager (HAFM) application.

HAFM server

See HP StorageWorks HA-Fabric Manager (HAFM) server.

hardware log

Record of FRU insertions and removals for the director.

hardware management console

The console runs the Hardware Management Console application (HWMCA), and is the operations and management PC platform for S/390 and 2/Series Servers.

HBA

See host bus adapter.

heterogeneous fabric

A fabric with both HP and non-HP products.

high availability

A performance feature characterized by hardware component redundancy and hot-swappability (enabling non-disruptive maintenance). High-availability systems maximize system uptime while providing superior reliability, availability, and serviceability.

homogeneous fabric

A fabric consisting of only HP products.

hop

Data transfer from one fabric node to another node.

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.

hot-swapping

Removing and replacing a device's components while the device continues to operate normally.

HP StorageWorks HA-Fabric Manager (HAFM) application

Application that implements the management user interface for HP Fibre Channel switching products, and as a launching point for the Director 2/140 *Product Manager* application. The application runs locally on the HAFM server or on a remote workstation.

HP StorageWorks HA-Fabric Manager (HAFM) server

Notebook computer shipped with a director to run the HAFM and Director 2/140 *Product Manager* applications.

hub

In Fibre Channel, a device that connects nodes into a logical loop by using a physical star topology.

IML

See initial machine load.

inband management

Management of the director through a Fibre Channel connection to a port card.

information message

Software message that indicates to a user that a function is performing normally or has completed normally. *See also* error message and warning message.

initial machine load (IML)

Hardware reset for all installed CTP cards on the director. It does not affect other hardware. It is initiated by pushing the white button on a director's CTP card.

initial program load (IPL)

Process of initializing the device and causing the operating system to start. Initiated through a menu in the *Product Manager* application, this option performs a hardware reset on the active CTP only.

input/output configuration

The collection of channel paths, control units, and I/O devices that attaches to the S/390 or 2/Series Processor.

input/output configuration program

A program that defines all available I/O devices and channel paths to an IBM S/390 or 2/Series Processor system. Replaced by the Hardware Configuration Definition Program starting with MVS/ESA Version 4.0.

interface

Hardware, software, or both, linking systems, programs, or devices.

internet protocol (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.

interswitch link (ISL)

Physical E_Port connection between two directors in a fabric.

I/O configuration

See input/output configuration.

IOCDs

A data set that contains an I/O configuration definition built by the IOCP.

IOCP

See input/output configuration program.

IP address

See internet protocol address.

IPL

See initial program load.

ISL

See interswitch link.

jumper cable

Optical cable that provides physical attachment between two devices or between a device and a distribution panel. *Contrast with* trunk cable.

latency

When used in reference to a Fibre Channel switching device, latency refers to the amount of time elapsed between receipt of a data transmission at a switch's incoming F_Port (from the originating node port) to retransmission of that data at the switch's outgoing F_Port (to the destination N_Port). The amount of time it takes for data transmission to pass through a switching device.

LIN

See link incident.

link

Physical connection between two devices in a switched fabric.

link incident (LIN)

Interruption to a Fibre Channel link due to loss of light or other cause.

load balancing

Ability to evenly distribute traffic over multiple interswitch links within a fabric. Load balancing on HP directors takes place automatically.

logical port address

The port numbering system for a director with the FICON Management Server active.

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.

loopback plug

In a fiber optic environment, a type of duplex connector used to wrap the optical output signal of a device directly to the optical input.

loopback test

Test that checks attachment or control unit circuitry, without checking the mechanism itself, by returning the output of the mechanism as input.

LUN

See logical unit number.

MAC address

See Media Access Control address.

maintenance port

Connector on the director where a PC running an ASCII terminal emulator can be attached or dial-up connection made for specialized maintenance support.

managed product

Hardware product that can be managed with the *Product Manager* application. For example, the Director 2/140 is a managed product. *See also* device.

management information base (MIB)

Related set of software objects (variables) containing information about a managed device and accessed via SNMP from a network management station.

Management Services application

Software application that provides back-end product-independent services to the *HAFM* application. Management Services runs only on the HAFM server, and cannot be downloaded to remote workstations.

management session

A management session exists when a user logs on to the *HAFM* application. The application can support multiple concurrent management sessions. The user must specify the network address of the HAFM server at logon time.

Media Access Control (MAC) address

Hardware address of a node (device) connected to a network.

MIB

See management information base.

multicast

Delivery of a single transmission to multiple destination node ports (N_Ports). Can be one to many or many to many. All members of the group are identified by one IP address. *See also* broadcast.

multi-switch fabric

Fibre Channel fabric created by linking more than one director or switching device within a fabric.

name server

Program that translates names from one form into another. For example, the domain name service (DNS) translates domain names into IP addresses.

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.

network address

Name or address that identifies a managed product on a transmission control protocol/internet protocol (TCP/IP) network. The network address can be either an IP address in dotted-decimal notation (containing four three-digit octets in the format xxx.xxx.xxx.xxx), or a domain name (as administered on a customer network).

nickname

Alternate name assigned to a world wide name for a node or director in the fabric.

node

In Fibre Channel terminology, node refers to an end device (server or storage device) that is or can be connected to a switched fabric.

node port (N_Port)

Physical interface within an end device which can connect to an F_Port on a switched fabric or directly to another N_Port (in point-to-point communications).

nondisruptive maintenance

Ability to service FRUs (including maintenance, installation, removal and replacement) while normal operations continue without interruption. *See also* concurrent maintenance.

N_Port

See node port.

offline sequence (OLS)

Sequence sent by the transmitting port to indicate that it is attempting to initialize a link and has detected a problem in doing so.

OLS

See offline sequence.

Open Systems Management Server

An optical feature that can be enabled on the director or switch through the Product Manger application. When enabled, host control and management of the director or switch are provided through an open systems interconnection (OSI) device attached to a director or switch port.

optical cable

Fiber, multiple fibers, or a fiber bundle in a structure built to meet optical, mechanical, and environmental specifications. *See also* jumper cable, optical cable assembly, and trunk cable.

optical cable assembly

Optical cable that is connector-terminated. *See also* jumper cable, optical cable, and trunk cable.

optical fiber connector

Hardware component that transfers optical power between two optical fibers or bundles and is designed to be repeatedly connected and disconnected.

out-of-band management

Transmission of management information using frequencies or channels (Ethernet) other than those routinely used for information transfer (Fibre Channel).

packet

Logical unit of information (usually in the form of a data frame) transmitted on a network. It contains a header (with all relevant addressing and timing information), the actual data, and a trailer (which contains the error checking function, usually in the form of a cyclic redundancy check).

password

Unique string of characters known to the computer system and to a user who must specify it to gain full or limited access to a system and to the information stored within it.

path

In a network, any route between any two ports.

persistent binding

A form of server-level access control that uses configuration information to bind a server to a specific Fibre Channel storage volume (or logical device) using a unit number.

port

Receptacle on a device to which a cable leading to another device can be attached.

port card

Field-replaceable hardware component that provides the port connections for fiber cables and performs specific device-dependent logic functions. *See also* fiber port module card and universal port module card.

port card map

Map showing numbers assigned to each port card by card slot.

port name

Name that the user assigns to a particular port through the *Product Manager* application.

POST

See power-on self test.

power-on self test (POST)

Series of self-tests executed each time the unit is booted or reset.

preferred domain ID

Domain ID that a director or switch is assigned by the principal switch in a switched fabric. The preferred domain ID becomes the active domain ID except when configured otherwise by the user.

principal switch

The director or switch that allocates domain IDs to itself and to all other switches in a fabric. There is always one principal switch in a fabric. If a switch is not connected to any other switches, it acts as its own principal switch.

Product Manager application

Application that implements the management user interface for a specified director. When a product instance is opened from the *HAFM* application's **Products View**, the director *Product Manager* application is invoked.

product name

User-configurable identifier assigned to a managed product. Typically, this name is stored on the product itself. For the Director 2/140, the product name can also be accessed by an SNMP manager as the system name.

prohibited port connection

In S/390 operating mode, an attribute that removes dynamic connectivity capability.

R_A_TOV

See resource allocation time-out value.

redundancy

Performance characteristic of a system or product whose integral components are backed up by identical components to which operations will automatically failover in the event of a component failure. Redundancy is a vital characteristic of virtually all high-availability (24 hours per day, seven days per week) computer systems and networks.

remote access link

Connection to a device or program on a computer network via a (geographically) remote workstation.

remote notification

A process by which a system is able to inform remote users and/or workstations of certain classes of events that occur on the system. E-mail notification and the configuration of SNMP trap recipients are two examples of remote notification programs that can be implemented on director-class switches.

remote user workstation

Workstation, such as a PC, using the *HAFM* and *Product Manager* applications that can access the *HAFM* server over a LAN connection.

resource allocation time-out value (R_A_TOV)

User-specified value for time out operations that depend on the maximum possible time that a frame could be delayed in a fabric and still be delivered.

RFI

Acronym for radio frequency interference.

SAN

See storage area network.

SA/OS 390

See system automation for operating system 390 (SA OS/390).

SBAR

See serial crossbar assembly.

SC

Acronym for subscriber connector.

segmented E_Port

Expansion port (E_Port) that has ceased to function as an E_Port within a multi-switch fabric due to an incompatibility between the fabrics that it joins. *See also* expansion port.

SEL

Acronym for system error light.

serial crossbar (SBAR) assembly

Responsible for Fibre Channel frame transmission from any director port to any other director port. Connections are established without software intervention.

SFP

Acronym for small form factor pluggable (a type of Fibre Channel connector). *See also* fiber port module card and universal port module card.

simple network management protocol (SNMP)

A protocol that specifies a mechanism for network management that is complete, yet simple. Information is exchanged between agents, which are the devices on the network being managed, and managers, which are the devices on the network through which the management is done.

SNMP

See simple network management protocol.

SNMP community

Also known as SNMP community string. An SNMP community is a cluster of managed products (in SNMP terminology, hosts) to which a server or managed product running the SNMP agent belongs.

SNMP community name

The name assigned to a given SNMP community. Queries from an SNMP management station to a device running an SNMP agent will only elicit a response if those queries are addressed with the correct SNMP community name.

SSP

See system services processor.

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.

subnet 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.

switchover

Changing a backup FRU to the active state, and the active FRU to the backup state.

switch priority

Value configured into each switch in a fabric that determines its relative likelihood of becoming the fabric's principal switch.

system 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 MVS, ESCON Manager, and Target System Control Facility.

system services processor (SSP)

Controls the RS-232 maintenance port, the Ethernet port, and the operator panel of a Fibre Channel director.

TCP/IP

See transmission control protocol/internet protocol.

topology

Logical and/or physical arrangement of stations on a network.

transmission control protocol/internet protocol (TCP/IP)

A suite of communication protocols used to connect host systems to the Internet. *See also* network address.

trap

Unsolicited notification of an event originating from an SNMP managed device and directed to an SNMP network management station.

trap host

SNMP management workstation that is configured to receive traps.

trunk cable

Cable consisting of multiple fiber pairs that do not directly attach to an active device. This cable usually exists between distribution panels. *See also* optical cable. *Contrast with* jumper cable.

unblocked port

Devices attached to an unblocked port can login to the director and communicate with devices attached to any other unblocked port.

unicast

Communication between a single sender and a single receiver over a network. Compare to *multicast* and *anycast* (communication between any sender and the nearest of a group of receivers).

universal port module (UPM) card

Each universal port module card provides four Fibre Channel connections through duplex small form factor pluggable (SFP) fiber-optic transceivers. 1 or 2 gigabits per second enabled. *See also* fiber port module card.

UPM card

See universal port module card.

vital product data (VPD)

System-level data stored by the backplane in the electrically erasable programmable read-only memory. This data includes serial numbers and identifies the manufacturer.

VPD

See vital product data.

warning message

Software message that indicates a possible error was detected. *See also* error message and information message.

world wide name (WWN)

Eight-byte address that uniquely identifies a switch, or a node (end device) on global networks.

wrap plug

See loopback plug.

WWN

See world wide name.

zone

Set of devices that can access one another. All connected devices may be configured into one or more zones. Devices in the same zone can see each other. Those devices that occupy different zones cannot.

zone member

Specification of a device to be included in a zone. A zone member can be identified by the port number of the director to which it is attached or by its world wide name. In multi-switch fabrics, identification of end-devices/nodes by world wide name is preferable.

zone set

See zone.

zoning

Grouping of several devices by function or by location. All devices connected to a connectivity product, such as the director, may be configured into one or more zones. *See also* zone.

Index

10/100 BaseT ethernet hub 1-1
10/100 Mbps ethernet port 1-18
10/100 Mbps LAN connectors 1-9

A

AC filter module
 removal 4-30
AC module
 removing and replacing 4-21
AC system harness 1-20
acoustical noise, director 1-7
active zone set, zone set view 3-20
airflow clearances, director 1-7
AIX operating system 1-15
altitude
 operating environment 1-8
 shipping and storage environment 1-8
angular velocity, of fans 1-21
applications
 management services 1-23
ASN.1 format 1-27
asynchronous RS-232 null modem cable 1-29
audit logs
 director 3-6
 HAFM application 3-3

B

backing up, director configuration file 3-59
backplane 1-21
 removing and replacing 4-32
bar graph 3-30
bb_credit
 node list view 3-18
beaconing

 fault isolation 1-12
 LED 1-17
blocking
 port 3-48
 UPM card 3-49

C

call-home notification
 information, use of 3-4
 reporting 1-27
CD-ROM
 drive 1-10
CFR, laser compliance 1-18
channel wrap test, procedure 3-37
class 1 laser transceivers 1-18
class F processing 1-18
cleaning fiber-optic components 3-42
clear system error light function 1-17
clock speed 1-10
clock speed, processor 1-15
Code of Federal Regulations 1-18
configuration changes, audit log 3-6
configuration data
 managing 3-58
configure panel 1-26
configure SNMP dialog box 1-27
configure switch parameters dialog box 2-89,
 2-105, 2-106, 2-109
connectivity failures, causes of 1-5
console PC, MAP 2-112
CTP2 card
 removing and replacing 4-5
CTP2 cards
 description 1-18

- event codes tables B-29
- failover 1-18
- firmware, managing 3-51
- FLASH memory 3-40
- LEDs 1-18
- MAP 2-71
- NV-RAM, backing up 3-58
- resetting 1-18
- customer checklist for fault isolation 2-12
- D**
- data collection, procedure 3-40
- default settings, resetting 3-61
- degraded fabric performance, causes of 1-5
- diagnostic features, software 1-21
- diagnostic functions, list of 1-26
- diagnostics
 - embedded web server 1-25
 - HAFM application 1-22
 - MAPs 2-1
 - port diagnostics 3-21
 - product manager 1-22
- dialog boxes
 - configure switch parameters 2-89, 2-105, 2-106, 2-109
- dimensions, director 1-7
- director
 - audit log 3-6
 - CTP2 card 1-18
 - diagnostic features, software 1-21
 - embedded web server 1-25
 - ethernet link, MAP 2-58
 - event codes B-1
 - event log
 - clearing 3-8
 - description 3-6
 - recording events B-1
 - refreshing 3-8
 - fabric log 3-5
 - fan module 1-21
 - fault isolation 1-11, 2-12
 - features 1-3

- firmware 1-25
 - version 1-11
- firmware library dialog box 3-52
- firmware, release notes 3-52
- general description 1-1
- illustrated parts breakdown 5-1
- IPL procedure 3-44
- management access methods 1-2
- MAPs 2-1
- ports
 - blocking or unblocking 3-47
 - port list view 3-13
- power requirements 1-7
- power supplies 1-20
- power-off procedure 3-43
- power-on procedure 3-43
- product manager
 - messages A-24
- product status log 3-5
- SBAR assembly 1-21
- setting online or offline 3-46
- SNMP traps 1-27
- specifications 1-7
- status table 1-22
- weight 1-7
- zoning features 1-4

director 2/64

- See director

- disk drive 1-10
- domain ID 1-5
 - zone member 3-21
- DRAM 3-40
- duplex LC connectors 1-19

- E**
- E_port segmentation
- causes of 1-6
- link incident log 3-10
- MAP 2-99
- multiswitch fabrics 1-5
- reasons for 3-27
- zone set view 3-21

- E_ports
 - UPM card 1-19
 - electric shock, warning 3-43
 - electrostatic discharge
 - grounding cable 1-30
 - wrist strap 1-30
 - electrostatic discharge (ESD)
 - information 4-2
 - repair procedures, caution 3-2
 - e-mail notification
 - reporting 1-27
 - embedded port subsystem 1-18
 - embedded web server 1-9, 1-25
 - ethernet link, MAP 2-58
 - fault isolation 2-12
 - interface 1-11
 - EP subsystem 1-18
 - equipment rack 1-1
 - service clearances 1-8
 - equipment symbols xiii
 - error detection
 - director features 1-3
 - ESD 3-2
 - FRU replacement instructions 4-2
 - FRUs, removing and replacing 4-1
 - grounding point
 - front 4-3
 - information 4-2
 - precaution requirement 4-5
 - precaution requirements 4-4
 - repair procedures, caution 3-2
 - ethernet communication link, MAP 2-58
 - ethernet hubs
 - description 1-10
 - ethernet LAN connectors 1-9
 - event codes
 - CTP2 card events B-29
 - description B-1
 - fan module events B-22
 - power supply events B-18
 - SBAR assembly B-56
 - system events B-3
 - thermal events B-61
 - UPM card B-44
 - event logs
 - director 3-6
 - clearing 3-8
 - refreshing 3-8
 - HAFM application 3-3
 - HAFM server B-1
 - exception frame processing 1-18
- ## F
- F_ports
 - UPM cards 1-19
 - zoning 1-4
 - fabric element MIB, performance view 3-31
 - fabric log 3-5
 - fabric logout, MAP 2-99
 - fabric manager
 - FRU list view 3-15
 - logs, list of 3-3
 - MAP 2-51
 - messages A-1, A-24
 - node list view 3-17
 - performance view 3-18
 - port list view 3-13
 - topology view 3-18
 - zone set view 3-20
 - fabric, definition of 1-5
 - factory default settings, resetting 3-61
 - failover, SBAR assembly 1-21
 - failure analysis 3-42
 - fan module
 - removing and replacing 4-27
 - fan module events, event codes tables B-22
 - fan modules
 - description 1-21
 - MAP 2-71
 - fault isolation
 - customer checklist 2-12
 - diagnostics 2-1
 - FRU list view 3-15
 - intranet service caution 1-14

- logs 3-3
- maintenance approach 1-11
- MAPs 2-1
- SNMP traps 1-27
- zone set view 3-21
- FC fabric element MIB, version 1-4
- FC-PH 4.3 1-2
- Fiber Channel link incidents, MAP 2-79
- fiber-optic cleaning kit 1-30
- fiber-optic protective plug 1-29
- fiber-optic transceivers, types of 1-19
- fiber-optic wrap plug 1-28
- Fibre Alliance MIB 1-4
- Fibre Channel address, port properties dialog box 3-26
- Fibre Channel FE MIB 1-27
- Fibre Channel physical and signalling interface 1-2
- field replaceable units
 - See FRUs
- firmware
 - adding version 3-52
 - deleting version 3-56
 - determining version 3-51
 - downloading version 3-56
 - modifying description 3-55
 - release notes 3-52
 - versions, managing 3-51
- firmware library 3-52
- FLASH memory 3-40
- front-accessible FRUs, parts list 5-2
- FRU list view 3-15
- FRUs
 - backplane 1-21
 - concurrent 4-4
 - CTP2 card 1-18
 - description 1-16
 - diagnostic features 1-22
 - ESD information 4-2
 - ESD precautions 4-1
 - fan module 1-21
 - front-accessible 5-1

- parts list 5-2
- illustration 5-1
- illustrations 5-1
- miscellaneous 5-5
- nonconcurrent 4-5
- power supply 1-20
- rear-accessible 5-3
 - parts list 5-4
- removals and replacements, hardware log 3-8
- removing and replacing 4-2
- SBAR assembly 1-21
- serial number, hardware log 3-9
- UPM cards 1-18

G

- G_ports
 - UPM card 1-19
 - UPM cards 1-18
- gateway address, default 2-1
- getting help xiv
- grounding point
 - front 4-3

H

- HA PA-RISC processor 1-15
- HAFM application
 - audit logs 3-3
 - diagnostic features 1-22
 - general description 1-2
 - logs, list of 3-3
 - MAP 2-51
 - maximum concurrent users 1-12
 - messages A-1
- HAFM server
 - description 1-9
 - ethernet link, MAP 2-58
 - event log B-1
 - fault isolation 1-11
 - MAP 2-12
 - Fibre Alliance MIB 1-4
 - firmware versions, storing 3-51
 - MAP 2-51, 2-112
 - remote workstation 1-2

session log 3–4
 specifications 1–10
 hard drive 1–10
 hard drives
 remote workstation 1–15
 hardware log 3–8
 hardware, MAP 2–112
 HBA, zoning 1–4
 heat dissipation, director 1–7
 help
 online user documentation 1–26
 help, obtaining xiv
 hexagonal adapter 1–28
 HP
 authorized reseller xv
 firmware versions 3–52
 home page 3–52
 technical support xiv
 website xv
 hp StorageWorks director 2/64
 See director
 hp StorageWorks ha-fabric manager application
 See HAFM application
 hp StorageWorks ha-fabric manager server
 See HAFM server
 HP-UX operating system 1–15
 humidity
 operating environment 1–8
 shipping and storage environment 1–8
 HyperTerminal 1–30, 2–66
I
 illustrated parts breakdown 5–1
 IML button 1–18
 IML, compared to IPL 3–44
 inclination, director 1–7
 initial machine load button 1–18
 initial machine load, compared to IPL 3–44
 initial program load, MAP 2–46
 input filter 1–20
 installing software 3–62
 Intel Pentium processor 1–10, 1–15

Internet Explorer 1–15
 version 1–26
 interswitch link
 G_port 1–19
 MAP 2–99
 intranet
 service caution 1–14
 IP address, default 2–1
 IPL
 MAP 2–46
 procedure 3–44
 ISL
 G_port 1–19
 MAP 2–99

L

LAN segments 1–12
 laser transceivers 1–18
 LC connectors 1–19
 LEDs
 beaconing 1–12, 1–17
 CTP2 card 1–18
 fan module 1–21
 power supplies 1–20
 SBAR assembly 1–21
 system error 1–17
 UPM card 3–22
 LIN alerts 3–15
 link incident alerts 3–15
 link incident log
 clearing 3–11
 description 3–10
 refreshing 3–11
 link incident, problem descriptions, list of 3–10
 Linux operating system, version 1–15
 logs
 audit
 director 3–6
 HAFM application 3–3
 event
 director 3–6, 3–8
 HAFM application 3–3

- fabric 3–5
- hardware 3–8
- link incident 3–10
- list of 3–3
- product status 3–5
- session 3–4

longwave laser transceivers 1–20

loopback tests

- external 3–35
- internal 3–32
- performing 3–32

M

maintenance analysis procedures

- See MAPs

maintenance approach 1–11

maintenance data, collecting 3–40

maintenance functions, list of 1–26

management access methods, out-of-band 1–2

management services application

- description 1–23

managing, configuration data 3–58

MAPs 2–1

- definition 1–11
- MAP 0000-Start Map 2–12
- MAP 0100-Power Distribution Analysis 2–36
- MAP 0200-POST or IML Failure Analysis 2–46
- MAP 0300-Console Application Problem Determination 2–51
- MAP 0400-Loss of Console Communication 2–58
- MAP 0500-FRU Failure Analysis 2–71
- MAP 0600-Port Card Failure and Link Incident Analysis 2–79
- MAP 0700-Fabric, ISL, and Segmented Port Problem Determination 2–99
- MAP 0800-Console PC Problem Determination 2–112
- quick start 2–2

memory

- HAFM server 1–10
- RAM 1–10

memory, remote workstation 1–15

messages

- fabric manager A–1, A–24
- HAFM application A–1
- product manager A–24

MIBs 1–4

Microsoft Internet Explorer

- hardware specification 1–15
- version 1–26

modem (external) 1–10

monitor panel 1–26

multiswitch fabric

- connectivity failures, causes of 1–5
- degraded performance, causes of 1–5
- description 1–5
- domain IDs 1–5
- E_port segmentation
 - causes of 1–6
 - reasons for 3–27
- E_ports 1–19
- zone set, definition 1–5
- zoning 1–5

N

N_ports

- UPM card 1–19
- zoning 1–4

name server zoning feature 1–4

Netscape Navigator 1–15

- version 1–26

network addresses, product status log 3–5

node list view 3–17

nodes, types, list of 3–17

notebook PC 1–9

null modem cable 1–29

NV-RAM, backing up 3–58

O

OFC class 1 laser transceivers 1–18

offline state, setting 3–47

online state, setting 3–46

online user documentation 1–26
operating environment, director 1–8
operations panel 1–26
optic transceivers 1–19
out-of-band, management access methods 1–2

P

part numbers

- front-accessible FRUs 5–1
- miscellaneous FRUs 5–5
- rear-accessible FRUs 5–3

password, customer

- default 2–1

password, maintenance

- default 2–1

PCMCIA slots 1–9

Pentium processor 1–10

performance view 3–18

personal computer, HAFM server 1–9

physical characteristics, director 1–7

port card

- external loopback test 3–35

- internal loopback test 3–32

- operational states 3–24

port card view 3–22

port list view 3–13

port loopback diagnostic tests, fiber-optic wrap

- plug 1–28

port number, zoning 1–4

port operational states table 3–24

port properties dialog box 3–15, 3–26

ports

- bar graph 3–30

- bb_credit, node list view 3–18

- blocking 3–48

- diagnostics, performing 3–21

- operational states, list of 3–24

- statistic information, performance view 3–18

- unblocking 3–49

- WWN, node list view 2–90, 3–18

POSTs

- MAP 2–46

power distribution system MAP 2–36

power module assembly

- removing and replacing 4–30

power plugs

- illustrations 5–5

power receptacles, illustrations 5–5

power requirements, director 1–7

power supplies 1–20

- LEDs 1–20

power supply

- removing and replacing 4–19

power supply events, event codes tables B–18

POWER3 microprocessor 1–15

power-off procedure 3–43

power-on procedure 3–43

power-on self-tests, MAP 2–46

PowerPC microprocessor 1–15

preventive maintenance, cleaning fiber-optic

- components 3–42

procedural notes 3–2

procedures

- blocking ports 3–48

- data collection 3–40

- external loopback test 3–35

- FRU removal 4–2

- FRU replacement 4–2

- installing software 3–62

- internal loopback test 3–32

- IPL 3–44

- managing configuration data 3–58

- managing firmware versions 3–51

- MAPs 2–1

- power-off 3–43

- power-on 3–43

- setting offline 3–46

- setting online 3–46

- unblocking ports 3–49

- upgrading software 3–62

ProComm Plus 1–30

product manager

- diagnostic features 1–22

- FRU list view 3–15

- logs, list of 3-3
- MAP 2-51
- messages A-24
- MIB variable, modifying 1-27
- node list view 3-17
- performance view 3-18, 3-30
- port card view 3-22
- port list view 3-13
- SNMP agent 1-2
- topology view 3-18
- zone set view 3-20
- product status log 3-5
- protective plug 1-29
- public intranet, service caution 1-14

Q

- quick start, MAPs 2-2

R

- rack stability, warning xiv
- RAM 1-10
- rear-accessible FRUs, parts list 5-4
- redundant power supplies
 - description 1-20
- relative humidity
 - operating environment 1-8
 - shipping and storage environment 1-8
- reloading firmware 1-18
- remote user workstations
 - configurations 1-12
 - LAN segment 1-12
 - minimum specifications 1-15
- remove and replace procedures
 - See RRP
- repair procedures, notes 3-2
- reporting
 - director features 1-3
- resetting
 - CTP2 card 1-18
 - director configuration data 3-61
- restoring
 - director configuration file 3-60
- RFC 1213 1-27

- definition 1-4

RJ-45

- twisted pair connector 1-18

RRPs

- AC module 4-21
- backplane 4-32
- CTP2 card 4-5
- fan module 4-27
- power module assembly 4-30
- power supply 4-19
- procedural notes 4-1
- SBAR assembly 4-24
- SFP optical transceiver 4-14
- UPM card 4-9
- UPM filler blank 4-17

RS-232

- maintenance port 1-18
- null modem cable 1-29

S

S/390 mode

- channel wrap tests
 - performing 3-21
 - procedure 3-37

Fibre Channel

- port address, swapping 3-15, 3-29, 3-31
- port channel wrapping, enabling and disabling 3-15, 3-29, 3-31
- swapping ports, procedure 3-38

safety

- basic ESD note 4-1
- electric shock, warning 3-43
- electrostatic discharge
 - grounding cable with wrist strap 1-30

ESD

- information 4-2
- repair procedures 3-2
- fiber-optic protective plug 1-29

SBAR assembly

- description 1-21
- event codes B-56

- failover 1–21
 - frame transmission 1–18
 - LEDs 1–21
 - MAP 2–71
 - removing and replacing 4–24
 - tools 4–24
 - segmentation
 - causes of 1–6
 - MAP 2–99
 - serial numbers, FRUs, hardware log 3–9
 - service
 - maintenance and diagnostic functions 1–26
 - service caution
 - public intranet 1–14
 - serviceability
 - director features 1–3
 - session log 3–4
 - setting
 - offline state 3–47
 - online state 3–46
 - SFP optical transceivers 1–19
 - MAP 2–79
 - removing and replacing 4–14
 - tools 4–14
 - shipping environment, director 1–8
 - shock tolerance, director 1–7
 - shortwave laser transceivers 1–20
 - small form factor optical transceivers
 - See SFP optical transceivers
 - SNMP
 - agent, general description 1–2
 - trap messages, maximum recipients 1–4
 - trap messages, reporting 1–27
 - traps, list of 1–27
 - software
 - diagnostic features 1–21
 - installing 3–62
 - management services application 1–23
 - upgrading 3–62
 - software diagnostics 1–1
 - Solaris operating system 1–15
 - spare parts
 - See FRUs
 - specifications, director 1–7
 - specifications, remote workstations 1–15
 - SSP subsystem 1–18
 - statistical information, performance view 3–30
 - status table
 - director 1–22
 - storage environment, director 1–8
 - subnet mask, default 2–1
 - SunOS operating system 1–15
 - swapping ports, procedure 3–38
 - symbols on equipment xiii
 - system error LED 1–17
 - system events 1–11
 - event codes tables B–3
 - system services processor 1–18
- ## T
- TCP/IP MIB-II 1–27
 - definition 1–4
 - technical support, HP xiv
 - temperature
 - operating environment 1–8
 - shipping and storage environment 1–8
 - thermal events, event codes tables B–61
 - tools
 - AC module 4–21
 - backplane 4–32
 - CTP2 card 4–5
 - fan module 4–27
 - power module assembly 4–30
 - SBAR assembly 4–24
 - SFP optical transceiver 4–14
 - supplied by service personnel 1–30
 - supplied with director 1–28
 - UPM cards 4–10
 - UPM filler blank 4–17
 - topology view 3–18
 - torque tool 1–28
 - trap messages
 - maximum recipients 1–4

U

UltraSPARC-II processor 1-15

unblocking

port 3-49

UPM card 3-50

UNIX workstation, specifications 1-15

upgrading software 3-62

UPM cards

blocking 3-49

description 1-18

event codes B-44

heat dissipation 1-7

inband management 1-2

LEDs 3-22

loopback tests, performing 3-32

MAP 2-79

port card view 3-22

ports, blocking or unblocking 3-47

removing and replacing 4-9

tools 4-10

unblocking 3-50

UPM filler blank

removing and replacing 4-17

tools 4-17

V

velocity, angular, of fans 1-21

versions

AIX operating system 1-15

director firmware 1-2, 1-11, 1-25

FC fabric element MIB 1-4

firmware

adding 3-52

deleting 3-56

determining 3-51

downloading 3-56

managing 3-51

modifying description 3-55

HP-UX operating system 1-15

Intel processor 1-10

Internet Explorer 1-15, 1-26

Linux operating system 1-15

Netscape Navigator 1-15, 1-26

Solaris operating system 1-15

SunOS operating system 1-15

Windows 2000 1-10

Windows 2000 operating system 1-2

Windows NT operating system 1-2

Windows operating systems 1-15, 1-30

vibration tolerance, director 1-7

video card, remote workstation 1-15

view panel 1-26

views

FRU list 3-15

node list 3-17

performance 3-18, 3-30

port card 3-22

port list 3-13

topology 3-18

zone set 3-20

voltage

AC power connectors 1-20

backplane 1-21

director 1-7

power supplies 1-20

W

warning

rack stability xiv

web server, embedded 1-9

interface 1-11

web server, overview 1-2

websites

HP xv

weight, director 1-7

wet-bulb temperature

operating environment 1-8

shipping and storage environment 1-8

Windows 2000 1-10

Windows 2000 operating system

MAP 2-51

Windows operating systems, versions 1-15,
1-30

workstation, UNIX 1-15

world wide name, caution, zoning 1-4
wrap plug
 multimode 1-28
 singlemode 1-28
WWN
 node list view 2-90, 3-18
 port properties dialog box 3-26
 zone member 3-21
 zoning, caution 1-4

Z

Zip drive 1-10
zone set
 definition 1-5
zone set view 3-20
zones, definition of 1-4
zoning
 features 1-4
 joining, rules of 1-5

