

hp StorageWorks

director 2/140 installation guide

Part Number: AA-RTDSA-TE/958-000275-000

First Edition (January 2003)

This guide provides procedures for setting up, configuring, and managing 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, Windows, and Windows NT 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 installation guide

First Edition (January 2003)

Part Number: AA-RTDSA-TE/958-000275-000

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 Overview

Director Description	1-1
Features	1-3
Director Management	1-3
Error-Detection, Reporting, and Serviceability	1-4
Multi-Switch Fabrics	1-6
Hardware Components	1-8
Front View	1-8
Power/System LED Assembly	1-9
Power Supplies	1-10
UPM Card	1-10
CTP Card	1-12
Rear View	1-12
Fan Modules	1-13
SBAR Assembly	1-14
AC Module	1-14
Backplane	1-14
Tools and Test Equipment	1-14

Tools Supplied with the Director	1–15
Tools Supplied by Service Personnel	1–16
Optional Kits	1–17

2 Installing and Configuring the Director 2/140

Summary of Installation Tasks	2–1
Installation Options	2–4
Review Installation Requirements	2–4
Items Required for Installation	2–5
Select an Operating Location	2–6
Cooling and Power Requirements	2–6
Unpack, Inspect, and Install the Director	2–6
Unpack and Inspect the Director	2–7
Desktop Installation	2–7
Power-On Self Test	2–9
Configure Director Network Information	2–9
Default Settings	2–9
Changing the Director’s IP Address	2–10
LAN-Connect the Director	2–15
HAFM Server	2–16
Record or Verify HAFM Server Restore Information	2–17
Enabling HAFM to Manage the Director	2–17
Verify Communication Between the Director and HAFM Server	2–18
Set Director Date and Time	2–20
Set Date and Time Manually	2–21
Synchronize Date and Time	2–22
Frequently Used HAFM Settings	2–22
Configure Feature Key	2–23
Procedure	2–23
Set the Director Online	2–25
Set the Director Offline	2–25
Configure Director Identification	2–26
Configuring Switch Operating Parameters	2–27
Switch Parameters	2–28
Domain ID	2–28
Preferred	2–29
Insistent	2–29

Rerouting Delay	2-30
Domain RSCNs	2-30
Operating Mode	2-30
Configure Fabric Operating Parameters	2-31
Fabric Parameters	2-32
BB_Credit.	2-32
R_A_TOV	2-32
E_D_TOV.	2-32
Switch Priority	2-33
Interop Mode	2-33
Configure Ports	2-34
Configure SNMP Trap Message Recipients	2-35
Configure and Enable E-mail Notification	2-37
Configure and Enable Call-Home Features.	2-38
Configure the Call-Home Feature.	2-38
Configure Threshold Alerts.	2-38
Create New Alerts.	2-39
Modify Alerts	2-45
Activate or Deactivate Alerts	2-46
Delete Alerts	2-46
Test Remote Notification	2-47
Back Up HAFM Configuration Data.	2-47
Enable Embedded Web Server.	2-48
Enable Telnet	2-48
Optional Features	2-48
FICON Management Server	2-48
Installation.	2-49
Configuring the FICON Management Server.	2-49
Open Systems Management Server.	2-52
Installation.	2-52
Configuring the Open Systems Management Server	2-52
SANtegrity Features	2-53
Fabric Binding.	2-53
Enable/Disable and Online State Functions	2-53
Switch Binding	2-54
Configuring Switch Binding—Overview.	2-54
Notes	2-55
Enable/Disable Switch Binding.	2-55

Editing the Switch Membership List	2-56
Enable/Disable and Online State Functions	2-58
Zoning with Switch Binding Enabled	2-59
Enterprise Fabric Mode	2-59
Fabric Binding.	2-59
Switch Binding	2-60
Rerouting Delay	2-60
Domain RSCNs.	2-60
Insistent Domain Identification (ID).	2-61
Connect Cables to the Fibre Channel Ports	2-61
Connect the Director to a Fabric.	2-61
Unpack, Inspect, and Install the Ethernet Hub (Optional)	2-63
Using HAFM from a Remote Location	2-64
Remote Workstation Minimum Requirements	2-64
Install HAFM Client on a Remote Workstation	2-65
Launch HAFM from the Remote Client	2-66

3 Using EWS to Configure the Director 2/140

Launch EWS.	3-1
Configure Director Ports.	3-3
Configure Director Identification	3-4
Configure Date and Time	3-5
Configure Operating Parameters	3-6
Switch Parameters	3-9
Domain ID.	3-9
Preferred.	3-9
Insistent.	3-9
Rerouting Delay	3-10
Domain RSCNs.	3-10
Configure Fabric Operating Parameters.	3-11
Fabric Parameters	3-13
BB_Credit	3-13
R_A_TOV	3-13
E_D_TOV	3-13
Switch Priority	3-13
Interop Mode.	3-14
Configure Network Information.	3-15
Configure SNMP Trap Message Recipients.	3-17

Configure User Rights	3–19
4 Manage Firmware Versions	
Determine a Director Firmware Version	4–1
Add a Firmware Version	4–2
Modify a Firmware Version Description	4–5
Delete a Firmware Version	4–6
Download a Firmware Version to a Director	4–6
Back Up the Director’s Configuration	4–9
A Regulatory Compliance Notices	
Regulatory Compliance ID Numbers	A–1
Federal Communications Commission Notice	A–2
Class A Equipment	A–2
Class B Equipment	A–2
Declaration of Conformity for Products Marked with FCC Logo—	
United States Only	A–3
Modifications	A–3
Network and Serial Cables	A–3
IEC EMC Statement (Worldwide)	A–4
Spécification ATI Classe A (France)	A–4
Canadian Notice (Avis Canadien)	A–4
Class A Equipment	A–4
Class B Equipment	A–4
European Union Notice	A–4
Japanese Notice	A–5
Taiwanese Notice	A–5
Harmonics Conformance (Japan)	A–6
German Noise Declaration	A–6
Laser Safety	A–6
Certification and Classification Information	A–6
Declaration of Conformity	A–8
B Technical Specifications	
Physical Dimensions	B–1
Environmental Specifications	B–2
Power Requirements	B–2
Operating Tolerances	B–3

Laser Information B-3

C Electrostatic Discharge

Precautions Against Electrostatic Discharge C-1
 Grounding Methods C-1

Glossary

Index

Figures

1-1 Director 2/140s and HAFM server in a cabinet. 1-2
 1-2 Director components—front 1-9
 1-3 UPM card LEDs and connectors 1-11
 1-4 Director components—rear 1-13
 1-5 Torque tool and hex adapter 1-15
 1-6 Loopback plug 1-15
 1-7 Fiber-Optic protective plug 1-16
 1-8 Null modem cable 1-16
 2-1 AC power connections (director) 2-8
 2-2 Connection Description dialog box 2-11
 2-3 Connect To dialog box 2-12
 2-4 COMn Properties dialog box 2-13
 2-5 HyperTerminal dialog box 2-14
 2-6 LAN-connect the director 2-16
 2-7 New Product dialog box 2-17
 2-8 Products View page 2-18
 2-9 Hardware View page (with FRU failures) 2-20
 2-10 Configure Date and Time dialog box 2-21
 2-11 Configure Feature Key dialog box 2-24
 2-12 New Feature Key dialog box 2-24
 2-13 Configure Identification dialog box 2-26
 2-14 Configure Switch Parameters dialog box 2-28
 2-15 Configure Fabric Parameters dialog box 2-31
 2-16 Configure Ports check boxes 2-34
 2-17 Configure SNMP dialog box 2-36
 2-18 Configure E-Mail dialog box 2-37

2-19	Configure Threshold Alerts dialog box	2-40
2-20	New Threshold Alerts dialog box—first screen	2-41
2-21	New Threshold Alerts dialog box—second screen	2-42
2-22	New Threshold Alerts dialog box—third screen	2-43
2-23	New Threshold Alerts dialog box—summary screen	2-44
2-24	Configure Threshold Alerts dialog box—alert activated	2-45
2-25	Test Remote Notification dialog box	2-47
2-26	Configure FICON Management Server dialog box	2-51
2-27	Configure Open Systems Management Server dialog box	2-52
2-28	Switch Binding State Change dialog box	2-55
2-29	Switch Binding Membership List dialog box	2-57
2-30	Port Properties dialog box	2-63
2-31	HAFM remote client install	2-65
3-1	Enter Network Password dialog box	3-2
3-2	View page	3-3
3-3	Ports page	3-4
3-4	Identification page	3-5
3-5	Date/Time Properties page	3-6
3-6	Current State page	3-7
3-7	Parameters page	3-8
3-8	Current State page	3-11
3-9	Fabric Parameters page	3-12
3-10	Network page	3-15
3-11	Activate message box	3-16
3-12	SNMP page	3-17
3-13	User Rights page	3-19
4-1	Firmware Library dialog box	4-2
4-2	New Firmware Version dialog box	4-4
4-3	New Firmware Description dialog box	4-4
4-4	Modify Firmware Description dialog box	4-5
4-5	Backup and Restore Configuration dialog box	4-7
4-6	Send Firmware confirmation box	4-8

Tables

1	Document Conventions	xii
1-1	Director 2/140 Optional Kits	1-17
2-1	Installation Task Summary	2-1

2-2	Director Operational States and Symbols	2-19
2-3	Available Code Pages	2-50
B-1	Dimensions	B-1
B-2	Environmental Specifications	B-2
B-3	Power Requirements	B-2
B-4	Operating Tolerances.	B-3
B-5	Laser Specs—2 Gb	B-3

About This Guide

This guide provides information on installing, configuring, managing, and verifying operation of the HP StorageWorks Director 2/140. The Director 2/140 switch connects storage devices, hosts, and servers in a SAN. The director is easily managed and configured to optimize the performance of your SAN.

Intended Audience

This guide is part of a documentation set that supports the Director 2/140. It is intended for use by trained service and installation representatives experienced with the SAN technology and Fibre Channel technology.

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 included in [Table 1](#) apply.

Table 1: Document Conventions

Element	Convention
Cross-reference links	Blue text: Figure 1
Key names, menu items, buttons, and dialog box titles	Bold
File names, application names, and text emphasis	<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>.

Overview

This chapter contains the following HP StorageWorks Director 2/140 information:

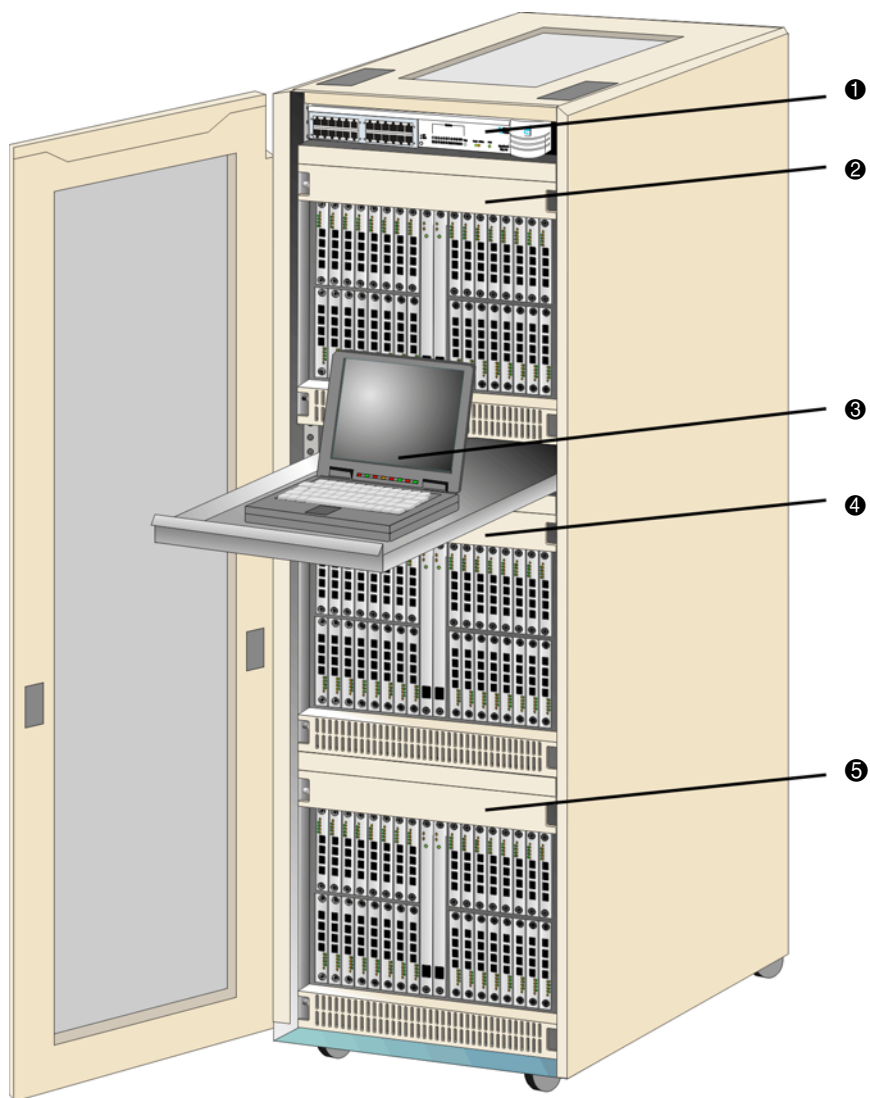
- [Director Description](#), page 1–1
- [Features](#), page 1–3
- [Hardware Components](#), page 1–8
- [Tools and Test Equipment](#), page 1–14
- [Optional Kits](#), page 1–17

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 are managed and controlled through a HAFM server with the *High Availability Fabric Manager (HAFM)* and *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).

[Figure 1–1](#) illustrates an equipment rack with three directors, the HAFM server, and Ethernet hub.



- ❶ Ethernet hub
- ❷ Director 2/140
- ❸ HAFM server
- ❹ Director 2/140
- ❺ Director 2/140

Figure 1–1: Director 2/140s and HAFM server in a cabinet

Features

Features of the Director 2/140 include:

- Scalable from 64 to 140 User ports
- 100% dynamic non-blocking, cut through switching with congestion queuing
- Online error detection, error isolation, and error recovery
- Redundant, hotpluggable components
- Full duplex 200 MB/sec per port performance
- Less than 2- μ s average switch latency
- 100-km distance support (60 buffers), with use of repeaters
- Small form factor, hot-pluggable optical transceivers, auto configure G_ports
- Combination short-wave or long-wave laser transceivers
- Redundant power supplies and fan modules
- Online product repair for Field Replaceable Units (FRUs)
- Periodic health check and enhanced system monitoring
- Non-disruptive firmware load and update

Director Management

The director is managed and controlled 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 2/140 *Product Manager* application.
- 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*.
- The Internet using the Embedded Web Server (EWS) 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 2/140

Product Manager application. Administrators launch the EWS interface from a remote PC by entering the director's IP address as the internet URL, then entering a user name and password at a login screen. The PC browser then becomes a management console.

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

- The command line interface (CLI). The CLI allows you to access many HAFM and Product Manager functions while entering commands during a telnet session with the 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*.
- A customer-supplied remote workstation communicating with the HAFM server through a corporate intranet.
- A customer-supplied PC platform with a network connection to the EWS interface installed on the director.
- A customer-supplied server platform communicating with the switch through a LAN or corporate intranet. The *HAFM* applications are ordered and installed on the server by the customer.

Error-Detection, Reporting, and Serviceability

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 remote workstation.
- Diagnostic software that performs power-on self-tests (POSTs) and port diagnostics (internal loopback, external loopback, and Fibre Channel (FC) wrap tests). The FC loopback test applies only when the director is configured to operate in S/390 mode.

- Automatic notification of significant system events (to support personnel or administrators) through e-mail messages or the call-home feature at the HAFM server.
- A modem for use by support personnel to dial-in to the HAFM server for event notification and to perform remote diagnostics.
- 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 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 multi-switch 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.
- SNMP management 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 management using the Fibre Channel Fabric Element MIB (Version 2.2), transmission control protocol/internet protocol (TCP/IP), MIB-II definition (RFC 1213), or a product-specific MIB that runs on 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.

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

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 port number to which a device is attached, or by the eight-byte (16-digit) World Wide Name (WWN) assigned to the host bus adapter (HBA) or Fibre Channel interface installed in a device. A device can belong to multiple zones.



CAUTION: If zoning is implemented by port number, a change to the 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.

In Open Fabric mode, only zoning by WWN is supported. Zoning by port numbers is not.

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

Multi-Switch Fabrics

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

Because a multi-switch fabric is typically complex, maintenance 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**—Zoning in a multi-switch 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.

Hardware Components

The director provides a modular design that enables quick removal and replacement of FRUs. The following sections define Director 2/140 main components.

Front View

[Figure 1–2](#) shows Director 2/140 components accessible from the front of the director. Component descriptions follow the figure.

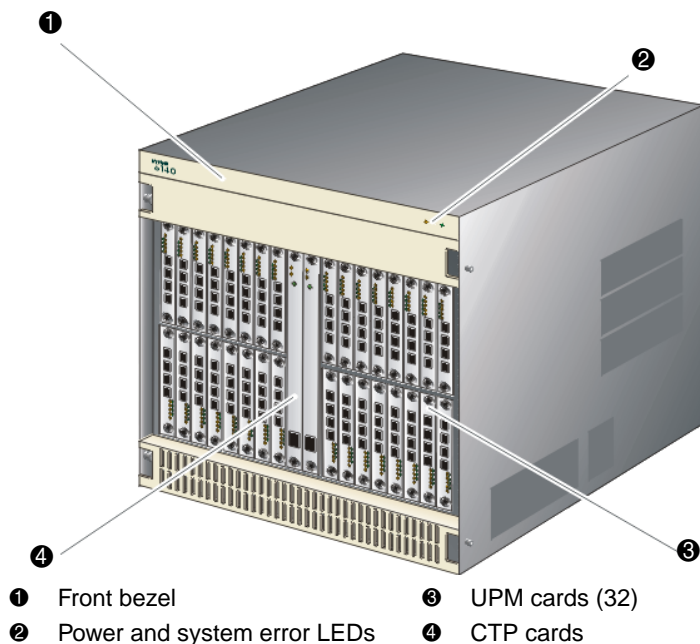


Figure 1–2: Director components—front

Power/System LED 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/System LED 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 beaoning is enabled. An illuminated system error LED (indicating a failure) takes precedence over unit beaoning.

Power Supplies

The Director 2/140 uses redundant, load-sharing power supplies which step down and rectify facility input power to provide 48-VDC power to director FRUs. The power supplies also provide over-voltage and over-current protection. Either power supply can be replaced while the switch 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 VAC. The faceplate of each power supply provides the following status LEDs:

- A green **PWR OK** LED turns ON if the power supply is operational and receiving AC power.
- An amber **FAULT** LED turns ON if the power supply fails.
- An amber **TEMP** LED turns ON if the power supply shuts down due to an over temperature condition.
- An amber **I LIM** LED turns ON if the power supply is overloaded and operating at the current limit (15.6 A).

Power supply requirements are listed in [Appendix B](#).

UPM Card

Each Universal Port Module (UPM) card provides four full-duplex generic ports (G_Ports) that transmit or receive data at 1.063 or 2.125 gigabits per second (Gbps). G_Port functionality depends on the type of cable attachment. UPM cards use Non-Open Fiber Control (NOFC) Class 1 laser transceivers that comply with Section 21 of the Code of Federal Regulations (CFR), Subpart J as of the date of manufacture.

Depending on device connections, G_Ports work 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 to form an Interswitch Link (ISL), the port functions as an expansion port (E_Port). A multi-switch fabric is formed through multiple directors and ISLs.

[Figure 1–3](#) shows the faceplate of an UPM.

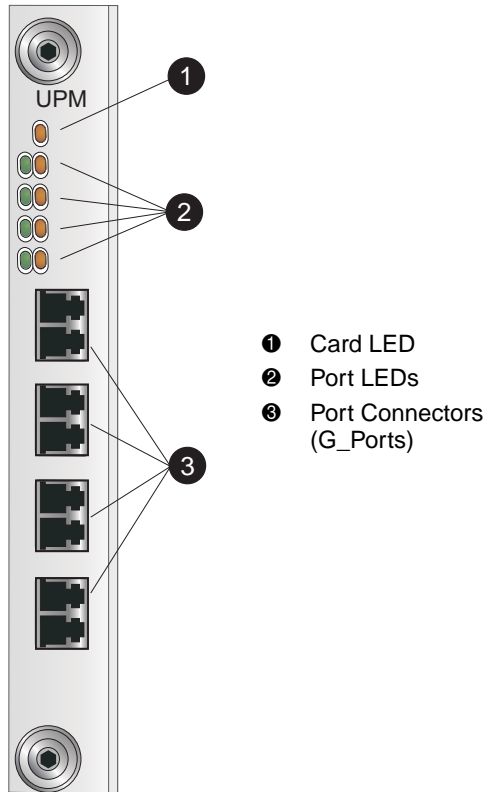


Figure 1–3: UPM card LEDs and connectors

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

- **Short-wave Laser**—Short-wave laser transceivers provide connections for transferring data over short distances (2 to 500 meters) through 50- μm (500 meters) or 62.5- μm (200 meters) multi-mode fiber.

NOTE: HP recommends 50- μm fiber-optic cable for any new installation requiring multi-mode fiber.

- **Long-wave Laser**—Long-wave laser transceivers provide connections for transferring data over long distances (up to 10 kilometers) through 9- μm single-mode fiber.

- **Extended reach long-wave Laser**—Long-wave laser transceivers that provide connections for transferring data over extended long distances (up to 35 kilometers) through 9- μ m single-mode fiber.

CTP Card

The Director 2/140 ships with two Control Processor (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. The second CTP card serves as a backup. 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).

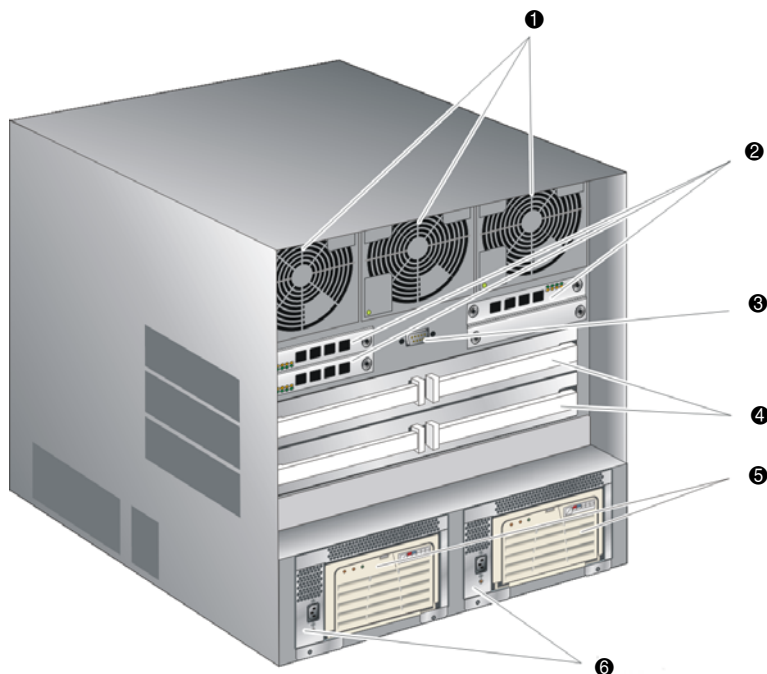
Each CTP card provides System Services Processor (SSP) and Embedded Port (EP) subsystems. The SSP subsystem runs director applications, communicates with director ports, and controls the RS-232 maintenance port and 10/100 Mbps ethernet port. The EP subsystem provides Class F processing, and manages frame transmission to and from the Serial Crossbar Assembly (SBAR). In addition, CTP cards provide non-volatile 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 light emitting diode (LED) that turns ON if the card is operational and active, and an amber LED that turns ON if the card fails. The LEDs are OFF on the backup CTP. The amber LED FLASHES if beaconing is enabled.

Rear View

[Figure 1–4](#) shows the components accessible from the rear of the Director 2/140.



- | | | |
|--------------------|-----------------|-------------------|
| ❶ Fan modules | ❷ UPM cards (3) | ❹ SBAR assemblies |
| ❸ Maintenance port | ❺ AC modules | ❻ Power supplies |

Figure 1–4: Director components—rear

Fan Modules

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.

The fan module can be replaced while the director is powered on and operating, provided the module is replaced within 10 minutes (after which software powers off the director). An amber LED for each fan module turns ON if one or more fans fail or rotate at insufficient velocity.

SBAR Assembly

The director ships 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. The transition 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 turns ON if the assembly is operational and active, and an amber LED that turns ON if the assembly fails. The amber LED FLASHES if FRU beaconing is enabled.

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, 220 VAC, power connectors.
- An input filter and AC system harness (internal to the FRU) that provides the wiring to connect the AC power connectors to the power supplies (through the backplane).

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.

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. Use of the tools may be required to perform test, installation, service, or verification tasks.

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

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.

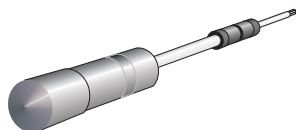


Figure 1–5: Torque tool and hex adapter

- **Loopback plug**—An SFP multi-mode (shortwave laser) or single-mode (longwave laser) loopback plug as shown in [Figure 1–6](#) is required to perform port loopback diagnostic tests. One loopback plug is shipped with the director, depending on the type of port transceivers installed. Both plugs are shipped if shortwave laser and longwave laser transceivers are installed.

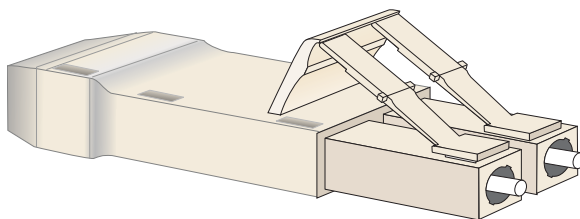


Figure 1–6: Loopback plug

- **Fiber-optic protective plug**—For safety and port transceiver protection, fiber-optic protective plugs as shown in [Figure 1–7](#) must be inserted in all director ports without fiber-optic cables attached. The director is shipped with protective plugs installed in all ports.

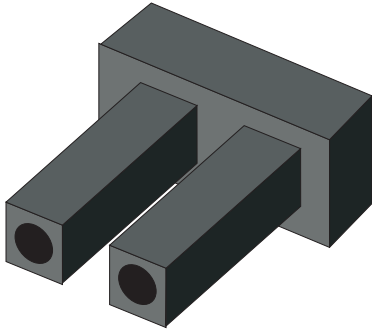


Figure 1–7: Fiber-Optic protective plug

- **Null modem cable**—An asynchronous RS-232 null modem cable as shown in [Figure 1–8](#) 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.

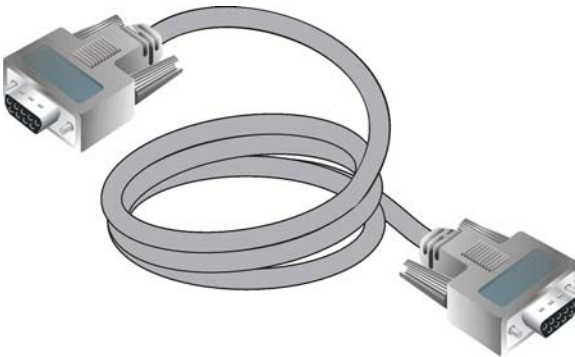


Figure 1–8: Null modem cable

Tools Supplied by Service Personnel

The following tools are expected to be supplied by service personnel performing director installation or 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 Millennium Edition operating system installed.
 - RS-232 serial communication software (such as ProComm Plus™ or HyperTerminal) installed. HyperTerminal is provided with Windows operating systems.
- **Fiber-optic cleaning kit**—The kit contains tools and instructions to clean fiber-optic cable, connectors, loopback plugs, and protective plugs.

Optional Kits

Contact your HP authorized service provider to purchase the following optional Director 2/140 kits. [Table 1–1](#) lists the optional kits.

Table 1–1: Director 2/140 Optional Kits

Supporting Kit	Description
2Gb UPM Port Module Kit, Part Number:A6574-87951 / DS-DMPMK-AA / 300833-B21	Provides 8 additional short-wave ports for the Director 2/140.
300m Optical Transceiver Kit, Part Number:DS-DMSHT-AA / 300834-B21	Provides short-wave optical transceiver for the Director 2/140.

Table 1–1: Director 2/140 Optional Kits (Continued)

Supporting Kit	Description
10km Long Distance Optical Transceiver Kit, Part Number: DS-DMLNG-AA / 300835-B21	Provides 10 km long-wave optical transceiver for the Director 2/140.
35 km Extended Reach Optical Transceiver Kit, Part Number: DS-DMEXT-AA / 300836-B21	Provides 35 km long-wave optical transceiver for the Director 2/140.

Installing and Configuring the Director 2/140

This chapter describes tasks to install, configure, and verify operation of the Director 2/140. The director can be installed on a table or desk top, or mounted in any standard equipment rack.

For a list of the factory-set defaults for the director and the Reset Configuration option, refer to [Appendix B](#).

Summary of Installation Tasks

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

Table 2–1: Installation Task Summary

Description	Required or Optional	Page
Review Installation Requirements	Required	2–4
Unpack, Inspect, and Install the Director	Required	2–6
Configure Director Network Information	Optional—configure if connecting multiple directors or if connecting a director and HAFM server to a public LAN.	2–9
LAN-Connect the Director	Required	2–15

Table 2–1: Installation Task Summary (Continued)

Description	Required or Optional	Page
HAFM Server	Optional but recommended and required for availability of all features, such as event logging and call-home—if not done, then the director should be configured using the embedded web server (EWS) interface.	2–16
Record or Verify HAFM Server Restore Information	Required if HAFM Server task was done.	2–17
Enabling HAFM to Manage the Director	Required if HAFM Server task was done.	2–17
Verify Communication Between the Director and HAFM Server	Required if HAFM Server task was done.	2–18
Set Director Date and Time	Optional	2–20
Configure Feature Key	Optional—configure if a feature key is ordered by the customer.	2–23
Frequently Used HAFM Settings	Required	2–22
Test Remote Notification	Optional	2–47
Back Up HAFM Configuration Data	Required	2–47
Enable Embedded Web Server	Optional—if not done, then the director should be configured using the HAFM server.	2–48
Configuring the FICON Management Server	Optional—configure if the HAFM server is installed.	2–49
Configuring the Open Systems Management Server	Optional—configure if the HAFM server is installed.	2–52
Connect Cables to the Fibre Channel Ports	Required	2–61
Connect the Director to a Fabric	Optional—perform this task to connect the director to a fabric.	2–61
Unpack, Inspect, and Install the Ethernet Hub (Optional)	Optional—install only if ordered and Ethernet segment does not exist to connect directors and the HAFM server.	2–63

Table 2–1: Installation Task Summary (Continued)

Description	Required or Optional	Page
Using HAFM from a Remote Location	Optional	2–64

Installation Options

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

- **Table or desk top**—One or more directors and an optional HAFM server are delivered and installed at the customer facility on a desk or table top. Ethernet cabling distance, and local area network (LAN) addressing issues must be considered.
- **Customer-supplied equipment rack**—One or more directors and an optional HAFM server are delivered to the customer facility for installation in an hp or customer-supplied equipment rack. Rack-mount hardware is provided in the shipping container. Ethernet cabling, distance, and LAN addressing issues must be considered.

Review Installation Requirements

The director is delivered stand-alone and ready to be mounted in an HP 9000, HP 10000, HP 11000, HP rack system/e, or industry-standard 19-in rack. Ethernet cabling, distance, and LAN addressing issues must be considered. Refer to *hp StorageWorks director 2/140 rack mount kit installation instructions* for detailed rack mount instructions.

Review the following checklist before installing the director:

- Prepare a site plan. Consult the *hp StorageWorks high availability planning guide*.
- Verify that required technical personnel are available and scheduled for the installation.
- Obtain the required fiber-optic cables (multi-mode or single-mode). Verify cable length and required connectors.
- Obtain an HP 19-inch equipment rack.
- Verify that the front panel air temperature does not exceed 40 °C (104 °F) during operation.
- Verify that there is space in the rack. The director is 12U (20 in) high.
- If applicable, obtain the necessary remote workstations or Simple Network Management Protocol (SNMP) workstations. Workstations are customer-supplied and connected through a corporate or dedicated LAN.

- Verify that all other equipment installed in the rack is connected to a reliable ground connection; do not rely on connections to a branch circuit, such as a power strip.
- HP recommends securing the rack mechanically to prevent it from tipping over during a natural disaster, such as an earthquake.

Items Required for Installation

Locate the following items before beginning the installation procedure:

- Lift device (recommended)
- Director 2/140
- An HP 9000, HP 10000, HP 11000, HP rack system/e, or industry-standard 19-in rack, or any rack with the following specifications:
 - A minimum depth of 24.5 in
 - 19 in wide
 - A minimum opening size of 13U available (12U for the director and 1U for space recommended for routing of cables).
- Two power outlets or different branches (for redundancy)
- Torque driver with cross-tip bit (for setting 22 in/lb of torque)
- Fiber-optic protective plug—For safety and port transceiver protection, fiber-optic protective plugs must be inserted in all director ports without fiber-optic cables attached. The director is shipped with protective plugs installed in all ports.
- Null modem cable—An asynchronous RS-232 null modem cable is required to configure director network addresses and obtain event log information through the maintenance port. The cable has nine conductors and two DB-9 female connectors. A null modem cable specially designed for this application is supplied with the Director 2/140.
- Standard flat-tip and cross-tip Phillips screwdrivers—Required to remove, replace, adjust or tighten various FRUs, chassis, or rack components.
- Electrostatic discharge (ESD) grounding cable with attached wrist strap—Required when working in and around the director card cage.
- Maintenance terminal (desktop or notebook computer)—Required to configure director network addresses and acquire event log information through the maintenance port. Computer requirements include:

- Microsoft Windows 98, Windows Millennium Edition, Windows NT 4.0, Windows 2000, or Windows XP operating system installed
- RS-232 serial communication software (for example, ProComm Plus, or HyperTerminal).

NOTE: The HAFM server may be used for this function. The *HyperTerminal* application is included with the Windows 2000 operating system provided with the HAFM server.

Select an Operating Location

Install the director in a secure or limited-access area to ensure that cable connections are not compromised. Also, make sure to install the director in an area with the ventilation and power requirements.

Cooling and Power Requirements

Three fan modules, each containing one fans (three fans total), provide cooling and redundancy fan for the director. The air intake for the director must satisfy an operating environment temperature requirement of 40°F to 104°F (4°C to 40°C).

Director power requirements:

Input voltage: 180 to 264 VAC

- Input frequency: 47/63 Hz



CAUTION: Do not block Director 2/140 air vents. The director uses ambient air for cooling.

Unpack, Inspect, and Install the Director

The following paragraphs provide instructions to unpack and inspect one or more Director 2/140s, and install the directors on a desktop or in a rack-mount configuration.

Unpack and Inspect the Director

Unpack and inspect the director(s) as follows:

1. Inspect the shipping containers for damage caused during transit. If a container is damaged, ensure a representative from the freight carrier is present when the container is opened.
2. Unpack the shipping containers and inspect each item for damage. Ensure the items match the items listed on the bill of materials (BOM).
3. If any items are damaged or missing, customers should call the toll-free telephone number printed on the service label attached to the back of the director.

Desktop Installation

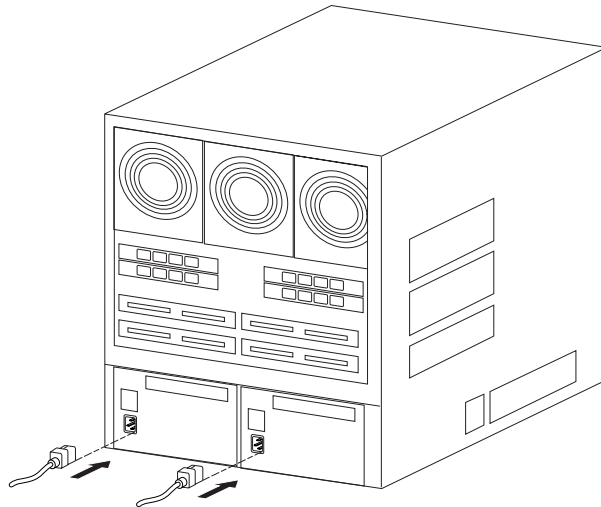
To install the director on a desktop:

1. Position the director on a table or desktop as directed by the customer.



CAUTION: Four person lift—the director weighs approximately 167 lbs. Do not attempt to lift or carry the director with fewer than four people. Failure to observe this CAUTION may result in injury to personnel or damage to the director.

2. Verify all field-replaceable units (FRUs), including logic cards, fans, and power supplies are installed as ordered.
3. Connect the U.S. or country-specific (optional) AC power cords to the right (PS0) and left (PS1) receptacles at the rear of the director, as shown in [Figure 2-1](#).



SHR-2594A

Figure 2–1: AC power connections (director)



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 cord(s), and ensure the facility power receptacle is the correct type, supplies the required voltage, and is properly grounded.

NOTE: The director does not have a power switch. Therefore the director powers on when its power cords are connected to facility power.

4. Connect the remaining ends of the AC power cords to separate (for redundancy) facility power sources that provide single-phase, 180 to 264 volt alternating current (VAC) current. The director powers on and performs power-on self-tests (POSTs). During POSTs:
 - a. Amber LEDs on both CTP cards and all universal port module (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.

5. 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.
6. If a POST error or other malfunction occurs, refer to the *hp StorageWorks director 2/140 service manual* to isolate the problem.

Power-On Self Test

Use the following steps to run a Power-On Self Test (POST):

1. Power on the PDUs (if used).

The director powers on. The following occurs during POST:

- Amber LEDs on both CTP cards and all universal port module (UPM) cards illuminate momentarily.
 - The green LED on each CTP card (active and backup) turns ON as the card is tested and UPM cards are tested.
 - Green LEDs associated with Fibre Channel ports sequentially illuminate as the ports are tested.
2. 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 ON.
 3. If a POST error or other malfunction occurs, refer to the *hp StorageWorks director 2/140 service manual*.

Configure Director Network Information

Use the following sections to configure the director's network addressing scheme.

Default Settings

The director is delivered with the following default network addresses:

- MAC address—The Media Access Control (MAC) address is programmed into FLASH memory on the CTP card at the time of manufacture. The address is in xx.xx.xx.xx.xx.xx format, where xx is a hexadecimal pair.
- IP address—The factory preset, default IP address is 10.1.1.10.

If the **Reset Configuration** option is selected from HAFM, the director resets to the default address of 10.1.1.10.

NOTE: If multiple directors are installed on the same LAN, each director (and server) must use a unique IP address. One director can use the factory-set address, but the addresses of the remaining directors require change.

- Subnet mask—The subnet mask is 255.0.0.0. If the director is installed on a complex public LAN with one or more routers, the address may require change.
- Gateway address—The gateway address is 0.0.0.0. If the director is installed on a dedicated LAN with no connection through a router, the address does not require change. If the director is installed on a public LAN (corporate intranet), the gateway address must be changed to the address of the corporate intranet's local router.

Verify the type of LAN installation with the customer's network administrator. If one director is installed on a dedicated LAN, network addresses must be verified but do not require change.

Changing the Director's IP Address

If multiple directors are installed, or a public LAN segment is used, network addresses must be changed to conform to the customer's LAN addressing scheme. The following items are required to perform this task.

- A local workstation (desktop or notebook computer) with:
 - Microsoft Windows 98, Windows 2000, Windows XP, or Windows NT 4.0 operating system.
 - RS-232 serial communication software (for example, ProComm Plus or HyperTerminal)

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

- An asynchronous RS-232 null modem cable (supplied with the Director 2/140).

Use the following steps to verify or change (if required) a director IP address, subnet mask, or gateway 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).
2. Connect the 9-pin end of the RS-232 modem cable to the maintenance port.

3. Connect the other cable end to a 9-pin communication port (COM1 or COM2) at the rear of the local workstation.
4. Choose **Start > Programs > Accessories > Communications > HyperTerminal**. The **Connection Description** dialog box displays, as shown in [Figure 2–2](#).

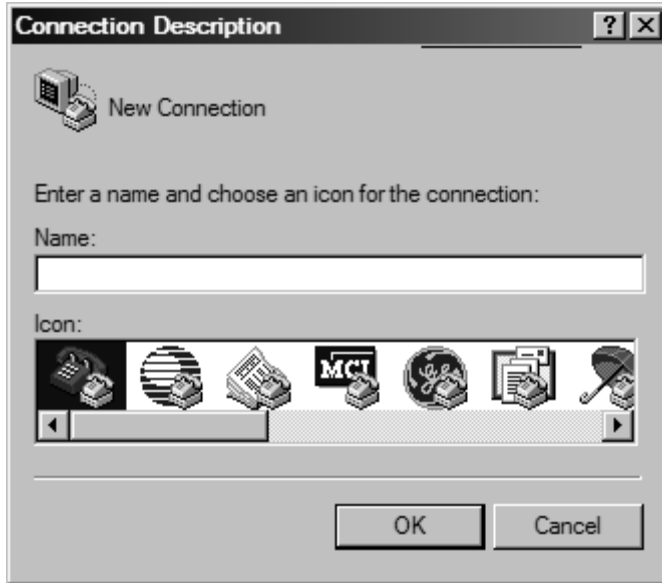


Figure 2–2: Connection Description dialog box

5. Type 2140 in the **Name** field and click **OK**. The **Connect To** dialog box displays, as shown in [Figure 2–3](#).



Figure 2–3: Connect To dialog box

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, as shown in [Figure 2–4](#).

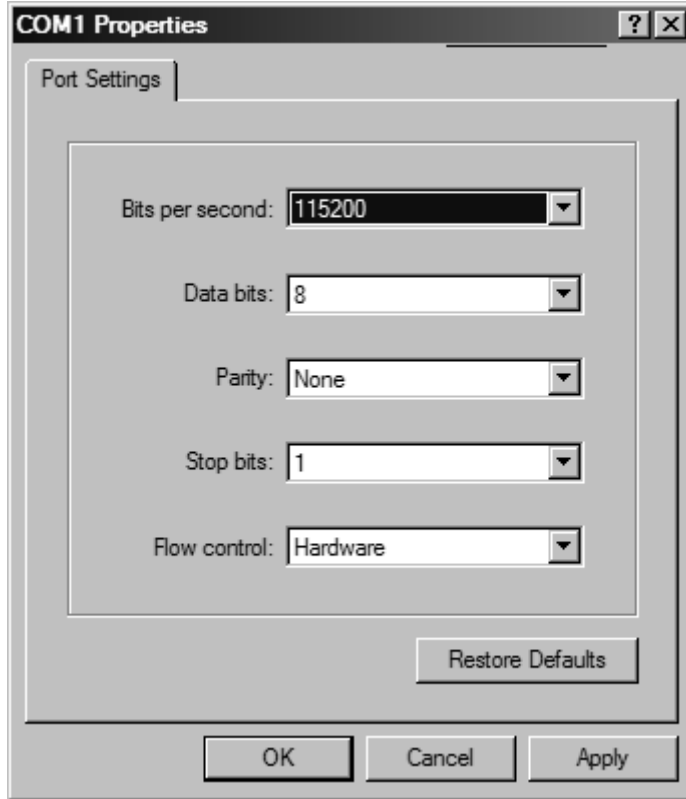


Figure 2–4: COM n Properties dialog box

7. Configure the Port Settings parameters as follows:
 - Bits per second: 115200
 - Data bits: 8
 - Parity: None
 - Stop bits: 1
 - Flow control: Hardware
8. Click **OK**. The HyperTerminal window displays.
9. At the > prompt, type the user-level password (the default is password) and press the **Enter** key. The password is case-sensitive. The **HyperTerminal** window displays with an C> prompt at the top of the window.

10. At the C> prompt, type `ipconfig` and press **Enter**. The **HyperTerminal** window displays, as shown in [Figure 2-5](#).

- MAC Address
- IP Address (default is 10.1.1.10)
- Subnet Mask (default is 255.0.0.0)
- Gateway Address (default is 0.0.0.0)

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

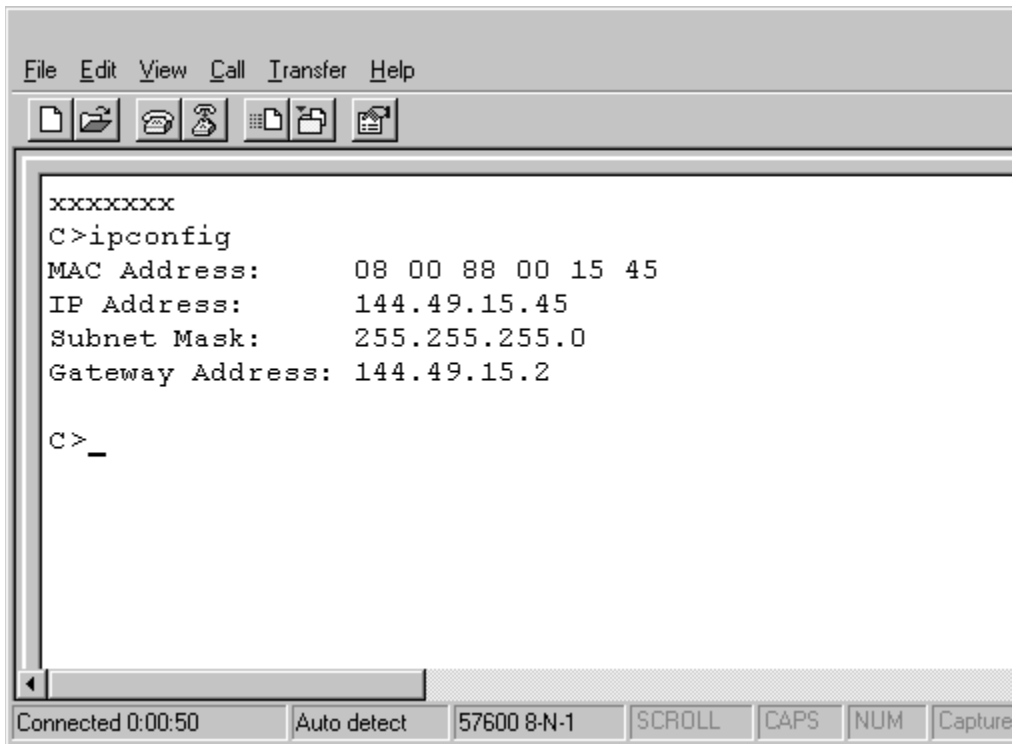


Figure 2-5: HyperTerminal dialog box

11. To change director network addresses, type the following at the C> prompt and press **Enter**.

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

The IP address format is xxx.xxx.xxx.xxx. The subnet mask format is yyy.yyy.yyy.yyy. The gateway address format is zzz.zzz.zzz.zzz. The octets xxx, yyy, and zzz are decimals from 0 through 255. If a network address is to remain unchanged, type the current address in the respective field.

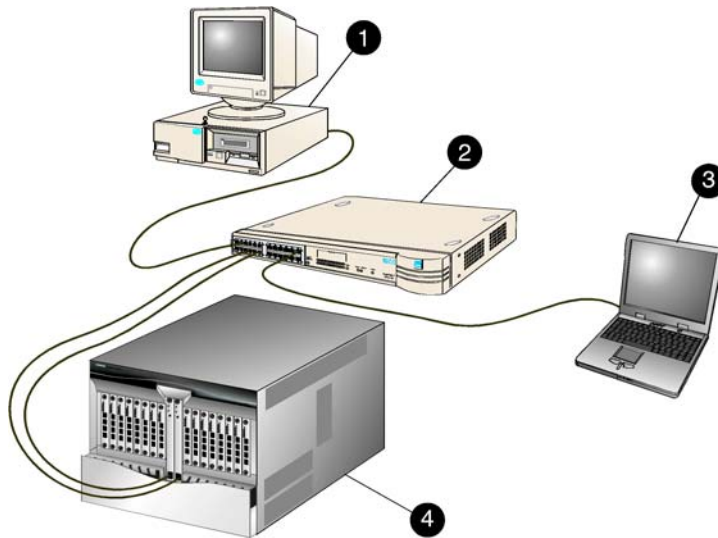
When the new network addresses are configured at the director, the message Request completed OK displays at the bottom of the **HyperTerminal** window.

12. Choose **Exit** from the **File** drop-down menu.
13. Click **Yes**.
14. Click **No** to exit and close the **HyperTerminal** window.
15. Power off the maintenance terminal:
 - a. Choose **Start > Shut Down**. The **Shut Down Windows** dialog box displays.
 - b. Choose **Shut down** and click **Ok** to power off the PC.
16. Disconnect the RS-232 null modem cable from the director and the maintenance terminal. Replace the protective cap over the maintenance port.
17. IPL the director.

LAN-Connect the Director

Use these steps to connect the rack-mounted director to the Ethernet LAN segment.

1. Connect one end of an Ethernet cable to the RJ-45 connector on each CTP card, as shown in [Figure 2-6](#).



SHR-2275

- | | |
|--|------------------|
| ❶ Remote workstation | ❸ HAFM server |
| ❷ Ethernet hub or switch (customer supplied) | ❹ Director 2/140 |

Figure 2-6: LAN-connect the director

2. Connect the remaining end of each Ethernet cable to the LAN as directed by the customer's network administrator.

NOTE: If an HAFM server is not available, use the Embedded Web Server (EWS) interface. Attach the Ethernet LAN segment to an Internet connection and see [Chapter 3](#).

HAFM Server

To run HAFM software, you must set up and configure the laptop server to function as an HAFM server.

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

- Setting up the HAFM server.
- Connecting the HAFM server to the LAN.
- Configuring the network addressing for the HAFM server.
- Setting HAFM server date and time.

- creating HAFM user names and passwords

Record or Verify HAFM Server Restore Information

Configuration information must be recorded to restore the HAFM server in case of hard drive failure. The Windows 2000 operating system and the HAFM and director *Product Manager* application must also be restored. Refer to the *hp StorageWorks director 2/140 service manual* for instructions.

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

Enabling HAFM to Manage the Director

To manage a new director, it must be recognized by the *HAFM* application. Follow these steps to enable HAFM to recognize a new director:

1. Click the **Product** menu and choose **New** from the drop-down list. The **New Product** dialog box displays, as shown in [Figure 2-7](#).



Figure 2-7: New Product dialog box

2. Type the IP address you configured earlier, see "[Configure Director Network Information](#)" on page 2-9.
3. Choose **Director-140** from the **Product Type** drop-down list and click **OK**. A new director icon displays at the **Products View** page.
4. Repeat this procedure for each new director.

Verify Communication Between the Director and HAFM Server





Follow these steps to check director-to-server communication.

1. From the **Products View** page (as shown in [Figure 2–8](#)), take note of the shape and color of the symbol behind the director icon. [Table 2–2](#) explains these symbols.



Figure 2–8: Products View page

Table 2–2: Director Operational States and Symbols

Operational State	Symbol
Operational —Director-to-server communication has been established, the director is operational, and no failures are indicated.	
Degraded —Director-to-server communication has been established, but the director is operating in degraded mode and requires service. This condition is typical if a port or redundant FRU fails. Go to step 2 .	
Failed —Director-to-server communication has been established, but the director failed and requires immediate service. Go to step 2 .	
Status Unknown —the director status is unknown because of a network communication failure between the director and HAFM server. Go to step 2 .	

2. Double-click the **Director-140** icon. The **Hardware View** page for the selected Director 2/140 displays, as shown in [Figure 2–9](#).

In the example, there are link incidents (yellow triangles), and director operational is indicated by the green circle in the alert panel.

3. Check director status at the **Hardware View** page and complete one of the following steps:
 - a. If the director displays as operational (no FRU alert symbols and a green circle at the alert panel), go to “[Set Director Date and Time](#)” on page 2–20.
 - b. If director operation displays as degraded or a director failure is indicated (FRU alert symbols and a yellow triangle or red diamond at the alert panel), refer to the *hp StorageWorks director 2/140 service manual*.

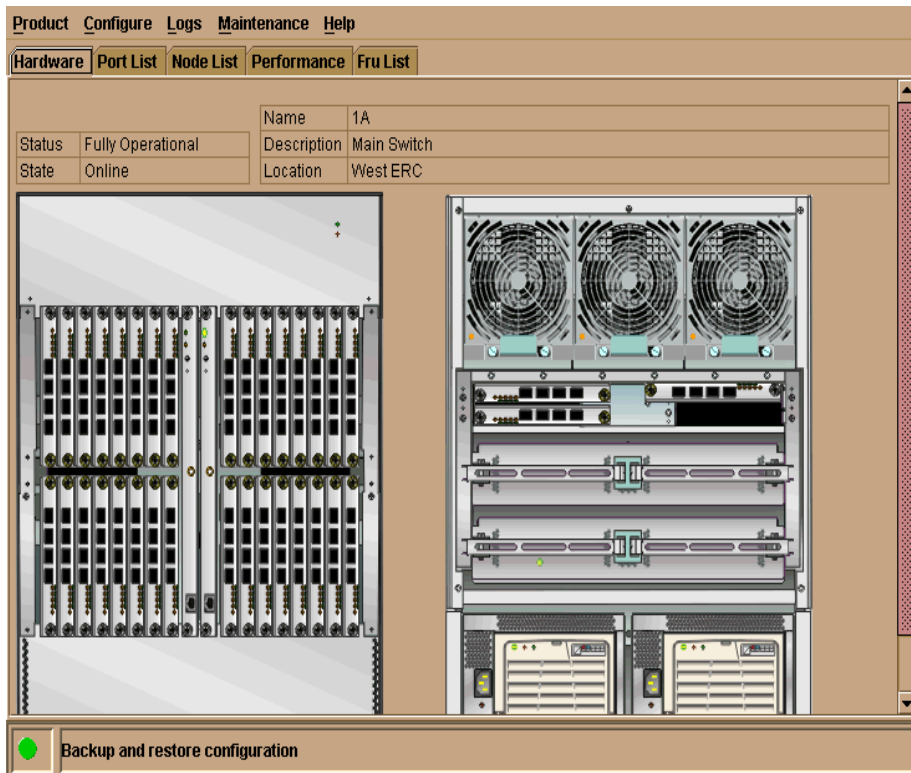


Figure 2–9: Hardware View page (with FRU failures)

Set Director Date and Time

The Director 2/140 Product Manager log entries are stamped with the date and time received from the director. Use these steps to set the effective date and time for the director.

NOTE: The director and HAFM synchronize at least once daily.

1. At the **Hardware View** page, click the **Configure** menu.
2. Choose **Date/Time** from the drop-down menu. The **Configure Date and Time** dialog box displays, as shown in [Figure 2–10](#).

3. Set director date and time manually, or set for periodic updates. For specific instructions, see the following sections:
 - [Set Director Date and Time](#), page 2–20
 - [Synchronize Date and Time](#), page 2–22

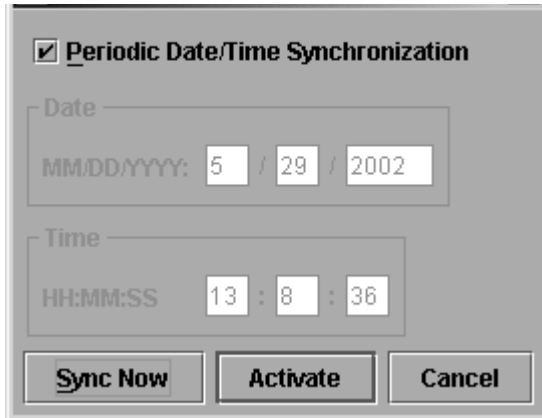


Figure 2–10: Configure Date and Time dialog box

Set Date and Time Manually

Use these steps to set the director date and time manually.

1. At the **Configure Date and Time** dialog box, click the **Periodic Date/Time Synchronization** check box to deselect the option (no check mark in the box). The greyed-out **Date** and **Time** fields activate.
2. Click the **Date** fields that require change, and type numbers in the following ranges:
 - Month (MM): 1 through 12
 - Day (DD): 1 through 31
 - Year (YYYY): greater than 1980
3. Click the **Time** fields that require change, and type numbers in the following ranges:
 - Hour (HH): 0 through 23
 - Minute (MM): 0 through 59
 - Second (SS): 0 through 59

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

Synchronize Date and Time

Use these steps to set the director to periodically synchronize date and time with HAFM.

1. At the **Configure Date and Time** dialog box, choose the **Periodic Date/Time Synchronization** check box. The **Date** and **Time** fields are greyed-out and not selectable.
2. Click **Activate** to enable synchronization and close the **Configure Date and Time** dialog box. The director date and time synchronize with the HAFM date and time at the next update period (at least once daily).
3. Click **Sync Now** to synchronize the director and HAFM immediately. The **Date and Time Synced** dialog box displays.
4. Click **OK**.
5. Click **Activate** to enable synchronization and close the **Configure Date and Time** dialog box.

Frequently Used HAFM Settings

This section summarizes the most common HAFM tasks, including:

NOTE: For a complete reference on HAFM functionality, refer to the *hp StorageWorks ha-fabric manager user guide*.

- [Configure Feature Key](#), page 2–23
- [Set the Director Online](#), page 2–25
- [Set the Director Offline](#), page 2–25
- [Configure Director Identification](#), page 2–26
- [Configuring Switch Operating Parameters](#), page 2–27
- [Configure Fabric Operating Parameters](#), page 2–31
- [Configure Ports \(Open Systems Mode\)](#), page 2–34
- [Configure SNMP Trap Message Recipients](#), page 2–35
- [Configure and Enable E-mail Notification](#), page 2–37

- [Configure and Enable Call-Home Features](#), page 2–38
- [Configure Threshold Alerts](#), page 2–38
- [Test Remote Notification](#), page 2–47
- [Enable Embedded Web Server](#), page 2–48
- [Enable Telnet](#), page 2–48
- [Optional Features](#), page 2–48

Configure Feature Key

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

XxXx-XXxX-xxXX-xX.

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

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

To enable an optional feature on the director, first set the director offline, then enter the feature key into the **New Feature Key** dialog box.

Display this dialog box by selecting **Feature** from the **Configure** menu on the menu bar.

FICON Management Server Feature: If you are enabling the FICON Management Server feature, the operating mode automatically configures to S/390 mode. You cannot change the operating mode to open systems mode with the FICON Management Server feature is enabled.

Procedure

To configure a feature key, use the following steps:

1. Set the director offline using the **Set Online State** dialog box.
 - a. Choose **Maintenance > Set Online State** from the **Product Manager** window. The **Set Online State** dialog box displays.
 - b. Click **Set Offline**. A warning box displays asking you to confirm the offline state.
 - c. Click **OK**.

2. Choose **Configure > Features** from the **Product Manager** window. The **Configure Feature Key** dialog box displays, as shown in [Figure 2–11](#).

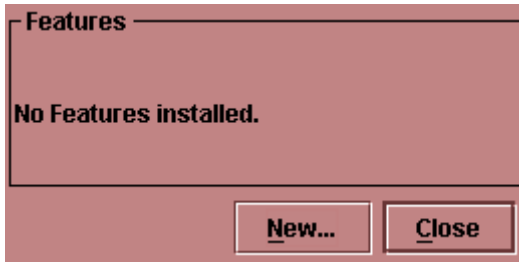


Figure 2–11: Configure Feature Key dialog box

3. Click **New** to add a new feature key. The **New Feature Key** dialog box displays, as shown in [Figure 2–12](#).

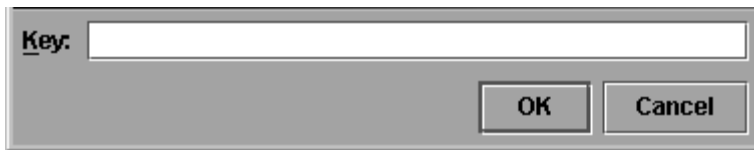


Figure 2–12: New Feature Key dialog box

4. Enter the director’s feature key in the **Key** field and click **OK**.
 - Feature keys are only valid for a director with a specific serial number. They cannot be interchanged between directors. If an error stating “Invalid serial number” displays, verify that you have entered the feature key that was assigned to the director. To verify, check the serial number of the director through the **Switch Properties** dialog box and compare it to the serial number listed in the documentation provided with your feature key.
 - The feature key is a string of alphanumeric characters with dashes. The key is case-sensitive, so enter the key exactly as printed in the documentation that you received for the feature. If an error stating “Invalid feature key” displays, verify that you have entered the feature key correctly.

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

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

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

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

6. Set the director back online.
 - a. Choose **Maintenance > Set Online State** from the **Product Manager** window. The **Set Online State** dialog box displays.
 - b. Click **Set Online**. A warning box displays asking you to confirm the online state.
 - c. Click **OK**.
7. When you are finished configuring the director, you can back up the configuration data.

Set the Director Online

When the director is set online, an attached device can log into the director if the port is not blocked. Attached devices can communicate with each other if they are configured in the same zone. Use these steps to set the director online:

1. Open HAFM. The **Products View** page displays.
2. Double-click the appropriate director icon. The **Hardware View** page for the selected director displays.
3. Choose **Maintenance > Set Online State**. If the director is offline, the **Set Online State** dialog box displays, indicating the status is offline.
4. Click **Set Online**. A **Warning** dialog box displays, indicating status is online.
5. Click **OK**. The **Status** table displays `Online`.

Set the Director Offline

When the Director 2/140 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. Use these steps to set the director offline:

1. Notify the customer that the director is going offline.

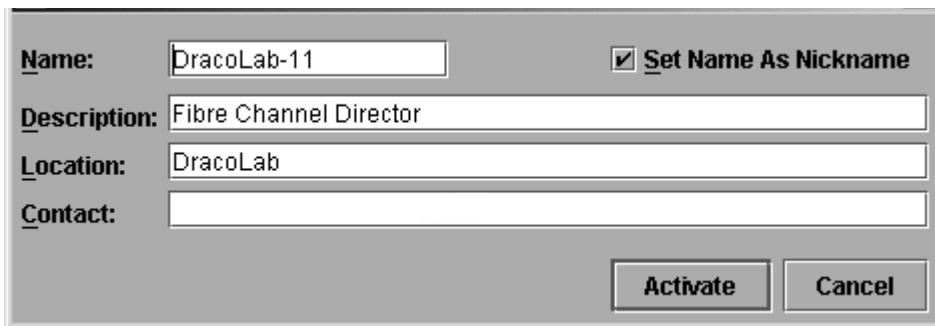
2. Open HAFM. The **Products View** page displays.
3. Choose the appropriate director icon. The **Hardware View** page for the selected director displays.
4. Choose **Maintenance > Set Online State**. If the director is online, the **Set Online State** dialog box displays, indicating the status is `Online`.
5. Click **Set Offline**. A **Warning** dialog box displays, indicating the director will be set offline.
6. Click **OK**.

Configure Director Identification

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

Follow these steps to configure the director identification.

1. At the **Hardware View** page, choose **Configure > Identification**. The **Configure Identification** dialog box displays, as shown in [Figure 2–13](#).



The screenshot shows a dialog box titled "Configure Identification". It has a gray background and contains the following elements:

- Name:** A text input field containing "DracoLab-11". To its right is a checked checkbox labeled "Set Name As Nickname".
- Description:** A text input field containing "Fibre Channel Director".
- Location:** A text input field containing "DracoLab".
- Contact:** An empty text input field.
- At the bottom right, there are two buttons: "Activate" and "Cancel".

Figure 2–13: Configure Identification dialog box

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

If the director is installed on a public LAN, the name should reflect the director's Ethernet network DNS host name. For example, if the DNS host name is SAN140.hp.com, the name entered in this dialog box is SAN140.

- b. Type a director description of 255 or fewer alphanumeric characters in the **Description** field.
 - c. Type the director's physical location (255 or fewer alphanumeric characters) in the **Location** field.
 - d. Type the name of a contact person (255 or fewer alphanumeric characters) in the **Contact** field.
2. Click **Activate** to save the information and close the dialog box.

Configuring Switch Operating Parameters

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

1. The director must be offline to change **Preferred Domain ID** and **Operating Mode** parameters. Verify that the director is set offline. For instructions, refer to the "[Set the Director Offline](#)" on page 2–25.



CAUTION: Setting the director offline terminates all Fibre Channel connections.

2. Choose **Configure > Operating Parameters > Switch Parameters**. The **Configure Switch Parameters** dialog box displays, as shown in [Figure 2–14](#).

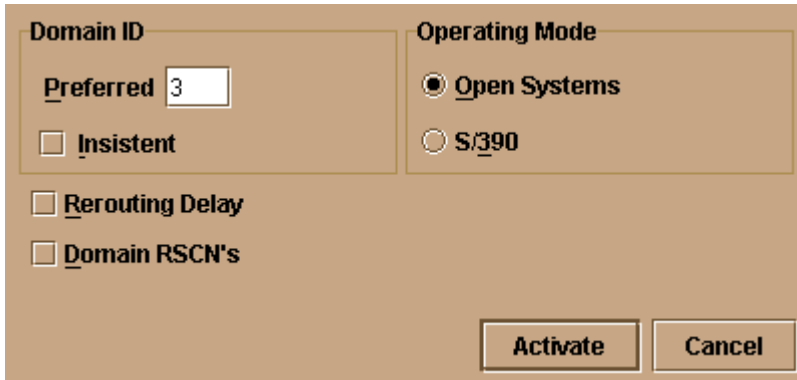


Figure 2–14: Configure Switch Parameters dialog box

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

1. Use information under “[Switch Parameters](#)” to change settings as required for parameters in this dialog box.
2. After you change settings, click the **Activate** button.
3. Set the director online. For instructions, see “[Set the Director Online](#)” on page 2–25.

Switch Parameters

Configure the following parameters as required by your fabric.

Domain ID

The domain identification is a value between 1 and 31 that provides a unique identification for the director in a fabric. A fabric director cannot contain the same domain ID as another director or their E_Ports will segment when they try to join.

In the **Configure Switch Parameters** dialog box, a field is provided to enter a preferred domain ID and a check box is provided to enable this ID as an insistent domain ID.

Preferred

NOTE: To change this value, you must first set the director offline. Choose Set Online State from the Maintenance menu to display the Set Online State dialog box, then click the Set Offline button. Be sure to set the director back online after you change this value.

Use this field to set a unique domain ID for the director. The default value is 1. Set a value between 1 and 31. When a director comes online with a preferred ID, it requests an ID from the fabric's principal director (indicating its preferred value as part of the request). If the requested domain ID is not allocated to the fabric, the domain ID is assigned to the requesting director. If the requested domain ID is already allocated, an unused domain ID is assigned. Note that you must set the director offline before you can change to the preferred domain ID.

The preferred domain ID must be unique for each director and switch in a fabric. If two switches or directors have the same preferred domain ID, the E_Ports segment, causing the fabric to segment.

For more information on domain ID, refer to the section on domain ID assignment for multi-switch fabrics in the *hp StorageWorks high availability planning guide* for details.

Insistent

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

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

- This option is required if Enterprise Fabric Mode (optional SANtegrity binding feature) is enabled.
- If you enable Insistent Domain while the switch or director is online, the Preferred Domain ID will change to the current active domain ID if the IDs are different.



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

Rerouting Delay

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

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

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

NOTE: This option is required if Enterprise Fabric Mode (optional SANtegrity binding feature) is enabled.

Domain RSCNs

Domain register for state change notifications (domain RSCNs) are sent between end devices in a fabric to provide additional connection information to host bus adapters (HBA) and storage devices. As an example, this information might be that a logical path has been broken because of a physical event, such as a fiber optic cable being disconnected from a port. Consult with your HBA and storage device vendor to determine if enabling Domain RSCNs will cause problems with your HBA or storage products. Note that this option is required if Enterprise Fabric Mode (optional SANtegrity binding feature) is enabled.

Operating Mode

NOTE: To change this value, you must first set the director offline. Choose **Set Online State** from the **Maintenance** menu to display the **Set Online State** dialog box, then click **Set Offline**. Be sure to set the director back online after you change this value.

Click either the **S/390** or **Open Systems** radio buttons:

- If the FICON Management Server feature is enabled, the default mode will be S/390. The operating mode cannot be changed to Open Systems with the FICON Management Server feature enabled. Typically, S/390 mode is used when

attaching an IBM S/390 Parallel Enterprise or IBM zSeries server to the director and implementing inband director management through a Fibre Connection (FICON) channel.

- Use **Open Systems** mode for all other (non-FICON) Fibre Channel environments.

Configure Fabric Operating Parameters

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

1. Verify that the director is set offline. For instructions, refer to the “[Set the Director Offline](#)” on page 2–25.



CAUTION: Setting the director offline terminates all Fibre Channel connections.

2. Choose **Configure > Operating Parameters > Fabric Parameters** from the **Product Manager** window. The **Configure Fabric Parameters** dialog box displays, as shown in [Figure 2–15](#).

BB_Credit:

R_A_TOV: (tenths of a second)

E_D_TOV: (tenths of a second)

Switch Priority:

Interop Mode:

Figure 2–15: Configure Fabric Parameters dialog box

3. Use information under “[Fabric Parameters](#)” to change settings as required for parameters in this dialog box.
4. After you change settings, click **Activate**.
5. Back up the configuration data when you are finished configuring the director.
6. Set the director online. For instructions, see “[Set the Director Online](#)” on page 2–25.

Fabric Parameters

Configure the following parameters as required by your fabric.

BB_Credit

Configure the director to support buffer-to-buffer credit (BB_Credit) from 1 through 60. This is the value used for all ports, except those configured for extended distance buffering (10-100 km). The default value is 16. For a description of the buffer-to-buffer credit, refer to the industry specification, *Fibre Channel Physical and Signaling Interface*.

R_A_TOV

Configure resource allocation time-out value (R_A_TOV) in tenth-of-a-second increments. This variable works with the error detect time-out value (E_D_TOV) variable to control the director’s behavior when an error condition occurs. Resources are allocated to a circuit when errors are detected and are not released for reuse until the time set by the R_A_TOV value expires. The default value is 100 tenths (10 seconds). Set a value between 10 tenths and 1200 tenths (1 through 120 seconds).

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

E_D_TOV

Adjust the E_D_TOV in tenth-of-a-second increments. An error condition occurs when an expected response is not received within the time limit set by this value. The default value is 20 tenths (2 seconds). Set a value between 2 tenths through 600 tenths (.2 through 60 seconds).

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

Switch Priority

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

Setting these priority values determines the principal director selected for the multi-switch fabric. For example, if you have three directors in the fabric and set one as **Principal**, one as **Default**, and one as **Never Principal**, the unit set to **Principal** becomes the principal director in the fabric.

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

- If you have three directors and set all to **Default**, the director with the lowest WWN becomes the principal director.
- If you have three directors and set two to **Principal** and one to **Default**, the director with the **Principal** setting that has the lowest WWN becomes the principal director.
- If you have three directors and set two to **Default** and one to **Never Principal**, the director with the **Default** setting and the lowest WWN becomes the principal director.

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

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

In, for example, the audit log, you may notice that the **Principal** setting maps to a number code of 1, **Default** maps to a number code of 254, and **Never Principal** maps to a number code of 255. The number codes of 2 - 253 are not currently in use.

Interop Mode

Select one of the following options:

- **Homogeneous Fabric**—Select this mode if the fabric contains only HP directors and switches that are operating in Homogeneous Fabric mode.

- **Open Fabric 1.0**—Default. Select this mode if the fabric contains HP directors and switches, as well as other open-fabric compliant switches. Select this mode for managing heterogeneous fabrics.

Configure Ports

Perform this procedure to define Fibre Channel port names, configure ports as blocked or unblocked, enable extended distance operation and Link Incident (LIN) alerts, and define port types.

1. At the **Hardware View** page, choose **Configure > Ports**. The **Configure Ports** dialog box displays.
 - a. Choose a blank **Name** field and type a descriptive port name of 24 or fewer alphanumeric characters. Use a unique name that reflects the device connected to the port. This name will be associated with the port and will not change regardless of the device connected.
 - b. Click the **Blocked** check box to block or unblock a port, as shown in [Figure 2–16](#). A check mark in the box indicates the port is blocked. Blocking the port prevents the attached device from communicating with the director. A blocked port continuously transmits the offline sequence.

Port #	Name	Blocked	10-100 km	LIN Alerts	Type	Speed	Port Binding	Bound WWN
0		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	1 Gb/sec	<input type="checkbox"/>	
1		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	1 Gb/sec	<input type="checkbox"/>	
2		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	2 Gb/sec	<input type="checkbox"/>	
3		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	1 Gb/sec	<input type="checkbox"/>	
4		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	1 Gb/sec	<input type="checkbox"/>	
5		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	1 Gb/sec	<input type="checkbox"/>	
6		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	2 Gb/sec	<input type="checkbox"/>	
7		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	1 Gb/sec	<input type="checkbox"/>	
8		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	1 Gb/sec	<input type="checkbox"/>	
9		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	1 Gb/sec	<input type="checkbox"/>	
10		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	2 Gb/sec	<input type="checkbox"/>	
11		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	1 Gb/sec	<input type="checkbox"/>	
12		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	1 Gb/sec	<input type="checkbox"/>	
13		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	1 Gb/sec	<input type="checkbox"/>	
14		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	G_PORT	2 Gb/sec	<input type="checkbox"/>	
15		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	1 Gb/sec	<input type="checkbox"/>	
16		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	1 Gb/sec	<input type="checkbox"/>	
17		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	1 Gb/sec	<input type="checkbox"/>	
18		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	2 Gb/sec	<input type="checkbox"/>	
19		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	1 Gb/sec	<input type="checkbox"/>	
20		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	1 Gb/sec	<input type="checkbox"/>	
21		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	1 Gb/sec	<input type="checkbox"/>	
22		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	2 Gb/sec	<input type="checkbox"/>	
23		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	G_PORT	1 Gb/sec	<input type="checkbox"/>	

Figure 2–16: Configure Ports check boxes

- c. Click the **10-100 km** check box to enable extended distance buffering for a port. A check mark in the box indicates the extended distance operation up to 100 kilometers (through repeaters) is enabled.
 - d. Click the **LIN Alerts** check box to enable or disable LIN alerts for a port. A check mark in the box indicates alerts are enabled. When the feature is enabled and an incident occurs on the link, an alert indicator (yellow triangle) displays at the **Hardware View**, **Port List View**, and **Port Card View** pages, and a message is sent to configured e-mail recipients. LIN alerts are enabled by default.
 - e. Choose a **Type** field and choose generic port (**G_Port**), fabric port (**F_Port**), or expansion port (**E_Port**) from the list box. If **F_Port** or **E_Port** is selected, the port will only operate as the port type selected. If **G_Port** is selected, the port type is automatically detected and will operate as an **E_Port** or **F_Port**.
 - f. Click the **Speed** field for a port. A **Speed** drop-down list displays. Choose **1 Gb/sec**, **2 Gb/sec**, or **Negotiate** as the desired setting depending on the speed capability of the device to be plugged into the port. A right-click in the **Speed** column will allow selecting from a popup menu to set all ports to 1 Gb/sec, 2 Gb/sec, or Negotiate.
2. Use the vertical scroll bar as necessary to display additional port information rows (up to 140 ports).
 3. Click **Activate** to save the configuration information and close the dialog box. If any port speed was changed, an information message box displays stating, "Port speed changes will temporarily disrupt port data transfers. Would you like to continue?" Click **Yes** to complete activation.

Configure SNMP Trap Message Recipients

Use this procedure to configure community names, write authorizations, network addresses, and UDP port number for up to six SNMP trap message recipients. A trap recipient is a management workstation that receives notification through SNMP.

1. At the **Hardware View** page, choose **Configure > SNMP Agent**. The **Configure SNMP** dialog box displays, as shown in [Figure 2-17](#).

Enable Authorization Traps

Community Name	Write Authorization	Trap Recipient	UDP Port Number
public	<input type="checkbox"/>		161
private	<input type="checkbox"/>		161
	<input type="checkbox"/>		
	<input type="checkbox"/>		
	<input type="checkbox"/>		
	<input type="checkbox"/>		

Figure 2–17: Configure SNMP dialog box

- a. For each trap recipient to be configured, type a community name of 32 or fewer alphanumeric characters in the associated **Community Name** field. The community name is incorporated in SNMP trap messages to ensure against unauthorized viewing or use.
 - b. Click the check box in the **Write Authorization** column to enable or disable write authorization for the trap recipient (default is disabled). A check mark in the box indicates write authorization is enabled. When the feature is enabled, a management workstation user can change the HAFM server's **sysContact**, **sysName**, and **sysLocation** SNMP variables.
 - c. Type the IP address or DNS host name of the trap recipient (SNMP management workstation) in the associated **Trap Recipient** field. Use 64 or fewer alphanumeric characters. HP recommends using the IP address.
 - d. Type a decimal user datagram protocol (UDP) port number in the associated **UDP Port Number** field. (This number is commonly 162.)
2. To enable transmission of trap messages to configured SNMP management workstations, click **Enable Authorization Traps**. A check mark displays in the box when transmission is enabled.

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

Configure and Enable E-mail Notification

Use this procedure to configure and enable e-mail addresses and Simple Mail Transfer Protocol (SMTP) server addresses to receive e-mail notification of director (and other managed product) events. The addresses must be configured via HAFM, then enabled. See “[Test Remote Notification](#)” on page 2–47.

Use these steps to configure and enable e-mail and SMTP server addresses:

1. Open the **Products View** page, choose **Maintenance > Configure E-Mail**. The **Configure E-Mail** dialog box displays, as shown in [Figure 2–18](#).



Figure 2–18: Configure E-Mail dialog box

- a. Type the IP address or DNS host name of the SMTP server in the **SMTP Server** field. Use 64 or fewer alphanumeric characters.
- b. For the **E-Mail Addresses** fields, type the email addresses of up to five recipients who should be informed of system events. Use 64 or fewer alphanumeric characters for each entry.

2. To enable email transmission of configured addresses, click **Enable E-Mail Event Notification**. A check mark displays in the box when transmission is enabled.
NOTE: Using HAFM, enable or disable email event notification for each director individually.
3. Click **OK** to save the information and close the dialog box.
4. Double-click the Director 2/140 icon. The **Hardware View** page for the selected director displays.
5. Choose **Maintenance > Enable E-Mail Notification**. A check mark displays in the check box to indicate that e-mail notification for the director is enabled.

Configure and Enable Call-Home Features

There are two call-home features provided. The HP HAFM server has a call-home feature that provides automatic dial-out through the modem to a service support facility to report director problems. This is provided in the shipped software.

In addition, the Proactive Services Call-Home feature reports events via the LAN to a SANworks Management Appliance or other server running the HP Proactive Services software. To order Proactive Services software, contact your HP customer service representative.

The following sections describe configuring both call-home features.

IMPORTANT: As shipped, the software includes the call-home via dial-out feature. In order to use the Proactive Services call-home, you must order the Proactive Services software. You can use either feature, but not both.

Configure the Call-Home Feature

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

Configure Threshold Alerts

A threshold alert notifies users when the transmit (Tx) or receive (Rx) throughput reaches specified values for specific director ports or port types, (E_Ports or F_Ports). You are notified of a threshold alert by:

- A yellow triangle that displays on the port in the **Port Card View**.
- A yellow triangle that displays on the port in the **Hardware View**.

- A yellow triangle that displays in the **Alert** column of the **Port List View**.
- A yellow triangle that displays by the **Threshold Alerts** field in the **Port Properties** dialog box.
- Detailed threshold alert data recorded in the Threshold Alert Log.

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

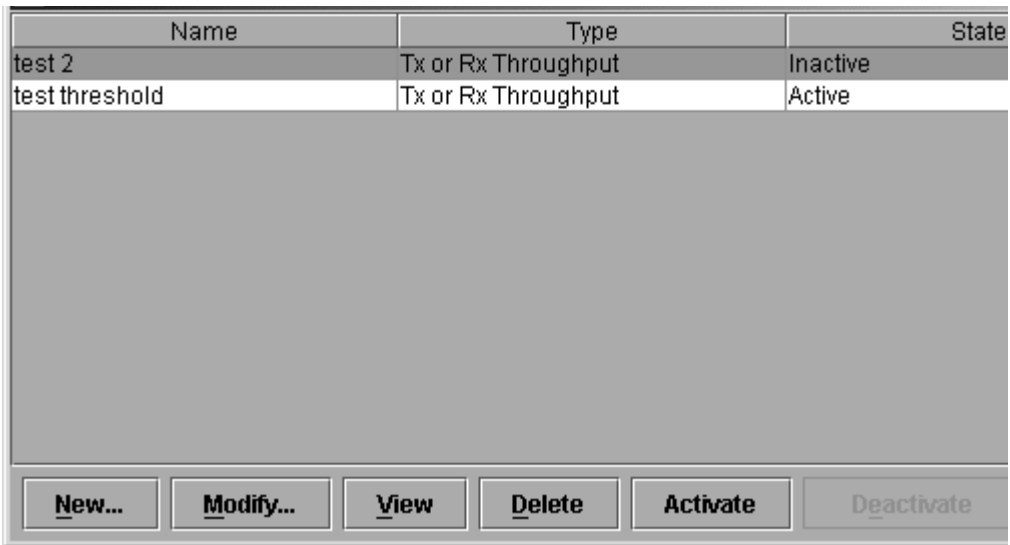
- Name for the alert.
- Type of threshold for the alert (Rx, Tx, or either).
- Active or inactive state of the alert.
- Threshold criteria:
 - Percent traffic capacity utilized—The percent of the port's throughput capacity achieved by the measured throughput. This setting constitutes the threshold value. For example a value of 50 means that the port's threshold is reached when throughput is 50% of capacity.
 - Time interval during which throughput is measured and alert notification can occur.
 - The maximum cumulative time that the throughput percentage threshold can be exceeded during the set time interval before an alert is generated.
- Ports for which you are configuring threshold alerts.

You can configure up to 16 alerts, and any number of alerts can be active at one time. Use the following procedures to create a new threshold alert, or to modify, activate, deactivate, or delete an alert.

Create New Alerts

1. At the **Hardware View** page, choose **Configure > Threshold Alerts**. The **Configure Threshold Alerts** dialog box displays, as shown in [Figure 2-19](#).

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



Name	Type	State
test 2	Tx or Rx Throughput	Inactive
test threshold	Tx or Rx Throughput	Active

Buttons: **New...** **Modify...** **View** **Delete** **Activate** **Deactivate**

Figure 2–19: Configure Threshold Alerts dialog box

2. Click **New**. The **New Threshold Alert** dialog box displays, as shown in [Figure 2–20](#).

Enter name and type of threshold alert:

Threshold Alert Name:

Threshold Type:

<< Previous Next >> Finish Cancel

Figure 2–20: New Threshold Alerts dialog box—first screen

3. Enter a name from one to 64 characters in length. All characters in the ISO Latin-1 character set, excluding control characters, are allowed.
4. Choose one of the following from the drop-down list under the **Name** field:
 - **Rx Throughput**—An alert will occur if the threshold set for receive throughput is reached
 - **Tx Throughput**—An alert will occur if the threshold set for transmit throughput is reached.
 - **Rx or Tx Throughput**—An alert will occur if the threshold set for either receive or transmit throughput is reached.

5. Click **Next**. A new screen displays with additional parameters, as shown in [Figure 2–21](#). The name configured for the alert displays at the top of the screen.

NOTE: Click **Previous** if you need to return to the previous screen.

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

% utilization

At any time

For cumulative minutes or more

during the minute notification interval.

<< Previous Next >> Finish Cancel

Figure 2–21: New Threshold Alerts dialog box—second screen

6. Enter a percentage from 1 through 100 for % utilization. When throughput reaches this percentage of port capacity, a threshold alert will occur.
7. Enter the amount of cumulative minutes in which the % utilization should exist during the notification interval before an alert is generated. You can also choose **At any time** if you want an alert to occur whenever the set % utilization is reached. The valid range is from 1 to the interval value set in [step 8](#).

8. Enter the interval in minutes in which throughput is measured and threshold notifications can occur. The valid range is 5 minutes to 70,560 minutes.
9. Click **Next**. A new screen displays for selecting ports for the alerts, as shown in [Figure 2–22](#).

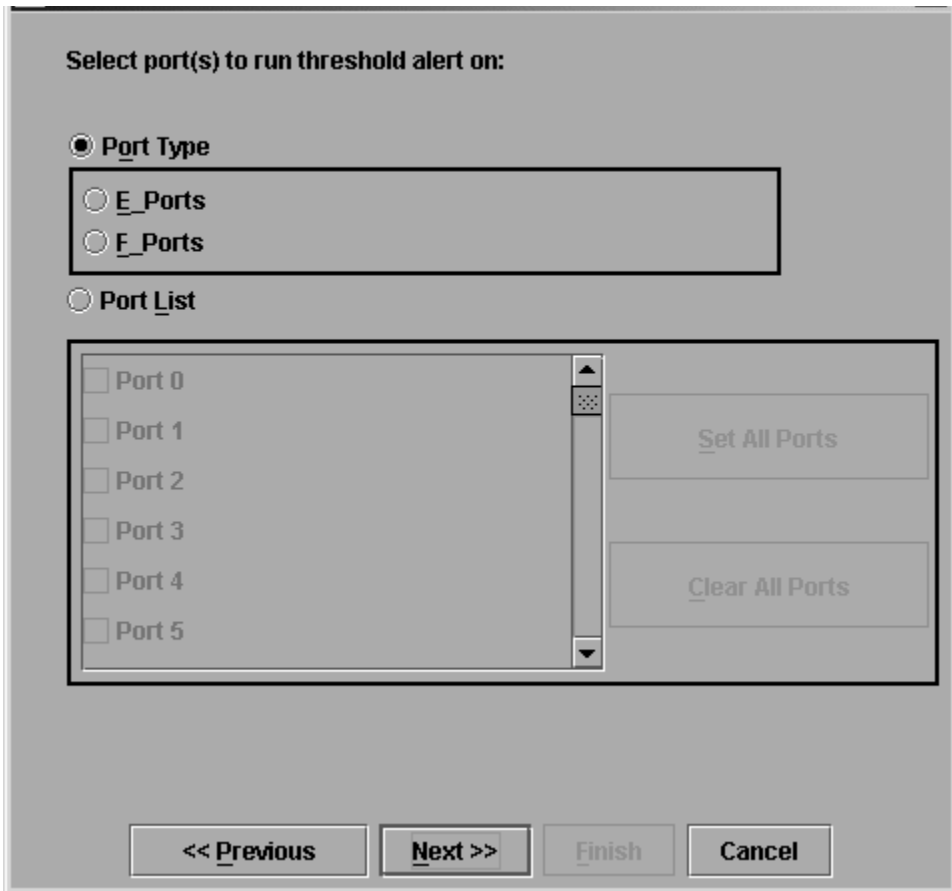


Figure 2–22: New Threshold Alerts dialog box—third screen

10. Choose either **Port Type** or **Port List**.
 - For **Port Type**, choose either E_Ports or F_Ports will cause this alert to generate for all ports configured as E_Ports or F_Ports respectively.

- For **Port List**, you can choose individual ports by clicking the check box by each port number or set all ports. Selecting **Set All Ports** places a check mark by each port number. Selecting **Clear All Ports** will clear the check marks by each port number.
11. Click **Next**. A final screen displays to provide a summary of your alert configuration, as shown in [Figure 2–23](#).

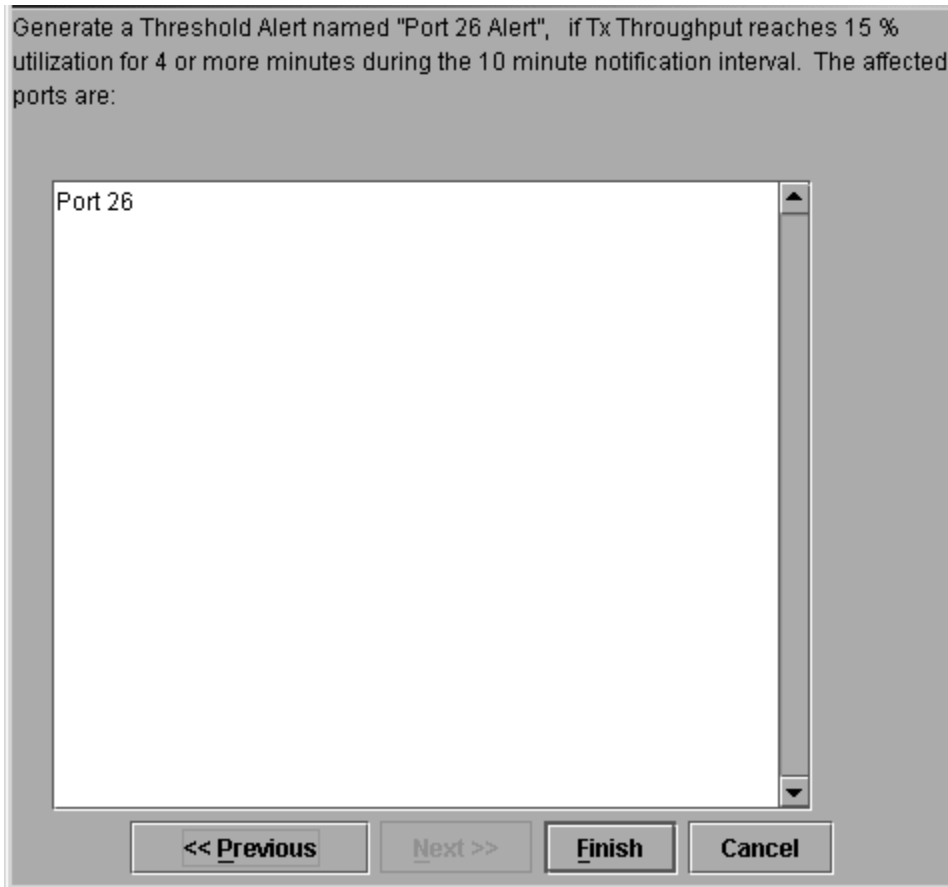


Figure 2–23: New Threshold Alerts dialog box—summary screen

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

13. At this point, the alert is not active. To activate the alert, choose the alert information that displays in the **Configure Threshold Alerts** table and click **Activate**. The alert is activated as shown in [Figure 2–24](#).

Name	Type	State
Port 26 Alert	Tx Throughput	Active
test 2	Tx or Rx Throughput	Inactive
test threshold	Tx or Rx Throughput	Active

Buttons: **New...** **Modify...** **View** **Delete** **Activate** **Deactivate**

Figure 2–24: Configure Threshold Alerts dialog box—alert activated

Modify Alerts

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

1. At the **Hardware View** page, choose **Configure > Threshold Alerts**. The **Configure Threshold Alerts** dialog box displays.

Select the alert that you want to modify by clicking the alert information in the table. If the alert is active, an error message displays prompting you to deactivate the alert.

2. If the alert is active, click **Deactivate**, then choose the alert information in the table again.
3. Click **Modify**. An initial **Modify Threshold** screen displays where you can change the threshold type.
4. Select a threshold type from the drop-down list.

5. Click **Next** when you are done. A **Modify Threshold** screen displays where you can change the % utilization, cumulative minutes for the threshold to occur before notification, and the time interval for measuring throughput and for alert notification.
6. Make appropriate changes, then continue through the **Modify Threshold** screens, making changes as necessary, until the summary screen displays the alert configuration.
7. Perform either of the following steps:
 - If you need to change any parameters, click **Previous** or **Next** to display the desired **Modify Threshold** screen.
 - Click **Finish** when you are done.

Activate or Deactivate Alerts

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

1. At the **Hardware View** page, choose **Configure > Threshold Alerts**. The **Configure Threshold Alerts** dialog box displays.
The port's current state, inactive or active, is listed under the **State** column.
2. To change the state, choose the alert by the alert information in the table.
3. If the alert is active, choose **Deactivate** to change to the inactive state. If the alert is inactive, choose **Activate** to change to the active state.

Delete Alerts

Use the following steps to delete existing threshold alerts.

1. At the **Hardware View** page, choose **Configure > Threshold Alerts**. The **Configure Threshold Alerts** dialog box displays.
2. Select the alert that you want to delete by selecting the alert information in the table and click **Delete**. A message displays asking you to confirm the deletion.
3. Click **Yes**. The alert is removed from the dialog box.

Test Remote Notification

If the e-mail and one of the call-home notification features are enabled, set up the *HAFM* application to test these remote notification features. Because the features are configured at the *HAFM* application, call-home and e-mail notification are enabled for multiple directors.

NOTE: Prior to using test remote notification, complete the steps in the previous sections, “[Configure and Enable E-mail Notification](#)” and [Configure the Call-Home Feature](#).

Use these steps to test remote notification:

1. Close the **Hardware View** page for the director by clicking **Close** at the **Navigation Control** panel.
2. Choose **Maintenance > Test Remote Notification**. The **Test Remote Notification** dialog box displays, as shown in [Figure 2–25](#).



Figure 2–25: Test Remote Notification dialog box

3. Check the **Call-Home** and **E-Mail** check boxes.
4. Click **Send Test**. Call-home and e-mail test messages are transmitted and an **Information** dialog box displays.
5. Click **OK**. Verify that the intended users received the call-home and e-mail notifications.

Back Up HAFM Configuration Data

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

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

Once the HAFM configuration data is backed up, go to “[Connect Cables to the Fibre Channel Ports](#)” on page 2–61.

Enable Embedded Web Server

Use the following steps to enable EWS:

1. At the **Hardware View** page, choose **Configure > Enable Web Server**. Choosing **Enable Web Server** automatically places a check mark in the check box.
2. Choose **Enable Web Server** again to remove the check mark and disable the EWS interface. When disabled, remote users cannot access the interface.

Enable Telnet

Use the following steps to enable Telnet:

1. At the **Hardware View**, choose **Configure > Enable Telnet**. Choosing **Enable Telnet** automatically places a check mark in the check box.
2. Choose **Enable Telnet** again to remove the check mark and disable telnet access. When disabled, remote users cannot access the director through telnet.

Optional Features

This section provides detailed information on using, administering, and configuring optional HAFM features through *HAFM* applications. There are two types of features covered in this chapter:

- “Keyed” features, requiring feature keys to be purchased and enabled through the **Configure Feature Key** dialog box in the product’s *Product Manager* application.
- Features not requiring feature keys themselves, but requiring that specific keyed features be enabled before they can be accessed through *HAFM* or *Product Manager* applications.

FICON Management Server

The FICON Management Server is a keyed feature that allows host control and inband management of the director or switch through an IBM System/390 or zSeries 900 Parallel Enterprise Server server attached to a director or switch port. The server communicates with the switch or director through a FICON channel. Control of connectivity and statistical product monitoring are provided through a host-attached console.

Installation

To install and enable this option, choose the **Configure Feature Key** option under the Product Manager's **Configure** menu.

Configuring the FICON Management Server

Use this procedure to configure whether the host is the controlling manager.

The optional FICON Management Server feature must be installed in order to perform this procedure.

- **Enable Management Server**—Click this check box to add a check mark and enable the management server. Click the check mark to remove it and disable this feature.
- **Switch Clock Alert Mode**—Click this check box to display a check mark and enable clock alert mode. If this is enabled, the following occurs when users set the date and time through the **Configure Date and Time** dialog box (**Configure** menu):
 - If you enable **Periodic Date/Time Synchronization**, an error message displays indicating that Clock Alert Mode must be cleared to enable automatic synchronization of the date and time.
 - If you manually set the date and time (**Periodic Date/Time Synchronization** is not enabled), a confirmation dialog box will display. You must click **OK** on that dialog box to continue manual configuration.
- **Host Control Prohibited**—Click this check box to display a check mark and prohibit a host management program from changing configuration and connectivity parameters on the director. In this case, the host program will have read authorization only and cannot make changes. When the check mark is not displayed, a host program can change configuration and connectivity parameters on the director.
- **Programmed offline state control**—Click this check box to display a check mark and enable a host management program to control the director's offline and online state. When a check mark is not displayed, a host program cannot set the director online or offline.
- **Active=Saved**—Click this check box to display a check mark and enable the active=saved function for the IPL address configuration.

- If **Active=Saved** is enabled (check mark), the IPL and the active address configuration are maintained as identical configurations. If a new configuration is activated through the **Configure Addresses - “Active”** dialog box, that configuration becomes the IPL address configuration.
- If **Active=Saved** is not enabled (no check mark), the IPL address configuration and the active configuration are not maintained as identical, and may be different configurations. If the feature *is not* enabled, you can modify the IPL configuration through the **Configure Addresses - “Active”** dialog box. If the feature *is* enabled, the IPL file is locked to modification through the **Configure Addresses - “Active”** dialog box.
- **Code Page**—Consider the language required for the port name display that appears on the HAFM server. Language support is provided through character set 697 for all Extended Binary-Coded Decimal Interchange Code (EBCDIC) pages.

When planning the installation, select the EBCDIC code page for displaying host-assigned port names or the CUP name. As an example, if the code page for Italy is selected and a port name is assigned in Italian by the host management program, then the Italian language port name will display in the product manager.

This field lists the code pages that are available for configuration. The default code page is United States/Canada 00037. Refer to the following table for other code pages:

Table 2–3: Available Code Pages

Code Page Name	Code Page	Hexadecimal CPGID
United States/Canada	00037	0025
Germany/Austria	00273	0111
Brazil	00275	0113
Italy	00280	0118
Japan	00281	0119
Spain/Latin America	00284	011C
United Kingdom	00285	011D
France	00297	0129
International #5	00500	01F4

To configure FICON management server, use the following steps:

1. Choose **Configure > Management Server** from the **Product Manager** window. The **Configure FICON Management Server** dialog box displays, as shown in [Figure 2–26](#).



Figure 2–26: Configure FICON Management Server dialog box

2. Enable or disable the management server by clicking **Enable Management Server** check box. (To disable the management server, click the check box again to remove the check mark.)
3. Enable or disable director clock alert mode by clicking the **Director Clock Alert Mode** check box. When a check mark displays, the alert mode is enabled.
4. Allow or prohibit host control by clicking the check box in the **Host Control Prohibited** field. When a check mark displays, host control is prohibited.
5. Allow or prohibit offline state control by clicking the check box in the **Programmed offline state control** field. When a check mark displays, programmed control of the offline state is allowed.
6. Enable or disable Active=Saved mode by clicking the check box in the **Active=Saved** field. When a check mark displays, the Active=Saved mode is enabled.
7. If necessary, select a code page from the **Code Page** drop-down list.
8. Activate changes and close the dialog box by clicking **Activate**.
9. If you are finished configuring the director, back up the configuration data.

Open Systems Management Server

The Open System Management Server (OSMS) is a keyed feature that allows host control and inband management of the director or switch through a management application that resides on an open-systems interconnection (OSI) device. This device is attached to a director or switch port. The device communicates with the switch or director through Fibre Channel common transport (FC-CT) protocol.

Installation

To install and enable this option, choose the **Configure Feature Key** option under the Product Manager's **Configure** menu.

Configuring the Open Systems Management Server

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

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

To configure open systems management server, use the following steps:

1. Choose **Configure > Management Server** from the **Product Manager** window. The **Configure Open Systems Management Server** dialog box displays, as shown in [Figure 2–27](#).

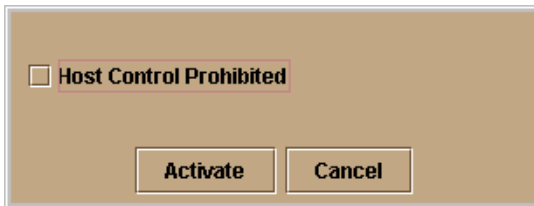


Figure 2–27: Configure Open Systems Management Server dialog box

2. Enable the management server by clicking the **Enable Management Server** check box. (To disable the management server, click the check box again to remove the check mark.)
3. Click the check box in the **Host Control Prohibited** field to display a check mark and to prohibit the host management program from changing configuration and connectivity parameters on the director. In this case, the host program has

read-only access to configuration and connectivity parameters. Clicking the check box when it contains a check mark removes the check mark and allows a host program to change configuration and connectivity parameters on the director.

4. To activate changes and close the dialog box, click **Activate**.
5. If you are finished configuring the director, you can back up the configuration data.

SANtegrity Features

SANtegrity includes a set of features that enhance security in SANs (Storage Area Networks) that contain a large and mixed group of fabrics and attached devices. Through these features you can allow or prohibit director attachment to fabrics and device attachment to directors. These features are enabled by purchasing a feature key, then enabling the key through the **Configure Feature Key** dialog box.

SANtegrity features include:

- Fabric Binding
- Switch Binding

Enterprise Fabric Mode—Although this is not a keyed feature, the SANtegrity Fabric Binding and Switch Binding must be installed before you can use Enterprise Fabric Mode function through the **HAFM Fabrics** menu.

Fabric Binding

This feature is managed through the **Fabric Binding** option, available through the **Fabrics** menu in HAFM when the **Fabrics** tab is selected. Using Fabric Binding, you can allow specific directors to attach to specific fabrics in the SAN. This feature provides security from accidental fabric merges and potential fabric disruption when fabrics become segmented because they cannot merge.

Enable/Disable and Online State Functions

In order for Fabric Binding to function, specific operating parameters and optional features must be enabled. Also, there are specific requirements for disabling these parameters and features when the director or switch is offline or online. Be aware of the following:

- Because directors are bound to a fabric by world wide name (WWN) and domain ID, the **Insistent Domain ID** option in the **Configure Switch Parameters** dialog box is automatically enabled if Fabric Binding is enabled. You cannot disable Insistent Domain ID while Fabric Binding is active and the director is online.
- If Fabric Binding is enabled and the director is online, you cannot disable Insistent Domain ID.
- If Fabric Binding is enabled and the director is offline, you can disable Insistent Domain ID, but this will disable Fabric Binding.
- You cannot disable Fabric Binding or Switch Binding if Enterprise Fabric Mode is enabled. However, if Enterprise Fabric Mode is disabled, you can disable Fabric Binding, Switch Binding, or both.

Switch Binding

This feature is managed through the **Switch Binding** submenu options available on the Product Manager **Configure** menu. Using **Switch Binding**, you can specify devices and directors that can attach to director and switch ports. This feature provides security in environments that include a large number of devices by ensuring that only the intended set of devices attach to a switch or director.

Configuring Switch Binding—Overview

To configure switch binding, you must first activate the feature using the **Switch Binding State Change** dialog box while selecting the type of port where you want to restrict connection (connection policy). Possible selections are E_Ports, F_Ports, or all types.

If the director or switch is online, activating switch binding populates the Membership List in the **Switch Binding - Membership List** dialog box (Product Manager) with the following WWNs currently connected to the director or switch, depending on the connection policy set in the **State Change** dialog box:

- WWNs of devices connected to F_Ports (F_Port connection policy). The WWN is the WWN of the attached device's port.
- WWNs of directors connected to E_Ports (E_Port connection policy). The WWN is the WWN of the attached director.
- WWNs of devices connected to F_Ports and directors connected to E_Ports (all-ports connection policy).

Notes

- When the Switch Binding feature is first installed and has not been enabled, the Switch Membership List is empty. When you enable Switch Binding, the Membership List is populated with WWNs of devices, directors, or both that are currently connected to the director.
- If the director is offline and you activate switch binding, the Membership List is not automatically populated.
- Edits to the Switch Binding Membership list will be maintained when you enable or disable Switch Binding.

After enabling Switch Binding, you prohibit devices and/or directors from connecting with director or switch ports by removing them from the Membership List in the **Switch Binding Membership List** dialog box. You allow connections by adding them to the Membership List. You can also add detached nodes and directors.

Enable/Disable Switch Binding

1. Choose the **Configure > Switch Binding > Change State** from the **Product Manager** window. The **Switch Binding State Change** dialog box displays, as shown in [Figure 2–28](#).

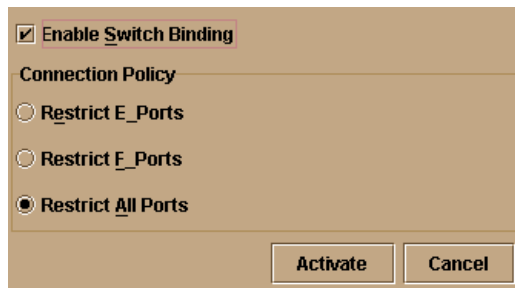


Figure 2–28: Switch Binding State Change dialog box

2. Perform one of the following steps:
 - To disable Switch Binding (a check mark appears in the **Enable Switch Binding** check box), click the **Enable Switch Binding** check box to remove the check mark, then click **Activate**.
 - To enable Switch Binding (check mark is not in the **Enable Switch Binding** check box), click the **Enable Switch Binding** check box to add a check mark. Go on to step 3 to set the Connection Policy.

3. Click one of the **Connection Policy** options.
 - **Restrict E_Ports**—Select if you want to restrict connections from specific directors to director E_Ports. Director WWNs can be added to the Switch Membership List to allow connection and removed from the Membership List to prohibit connection. Devices are allowed to connect to any F_Port.
 - **Restrict F_Ports**—Select if you want to restrict connections from specific devices to director F_Ports. Device WWNs can be added to the Switch Membership List to allow connection and removed from the Membership List to prohibit connection. Directors are allowed to connect to any E_Port.
 - **Restrict All**—Select if you want to restrict connections from specific devices to director F_Ports and directors to director E_Ports. Device and director WWNs can be added to the Switch Membership List to allow connection and removed from the Membership List to prohibit connection.
4. Click **Activate** to enable the changes and close the dialog box.
5. Edit the Switch Membership List through the **Switch Binding Membership List** dialog box to add or remove directors and devices that are allowed to connect with the director.

Editing the Switch Membership List

1. Choose the **Configure > Switch Binding > Edit Membership List** from the **Product Manager** window. The **Switch Binding Membership List** dialog box displays, as shown in [Figure 2–29](#).

The WWNs of devices and/or directors that can currently connect to director ports are listed in the **Switch Membership List** panel.

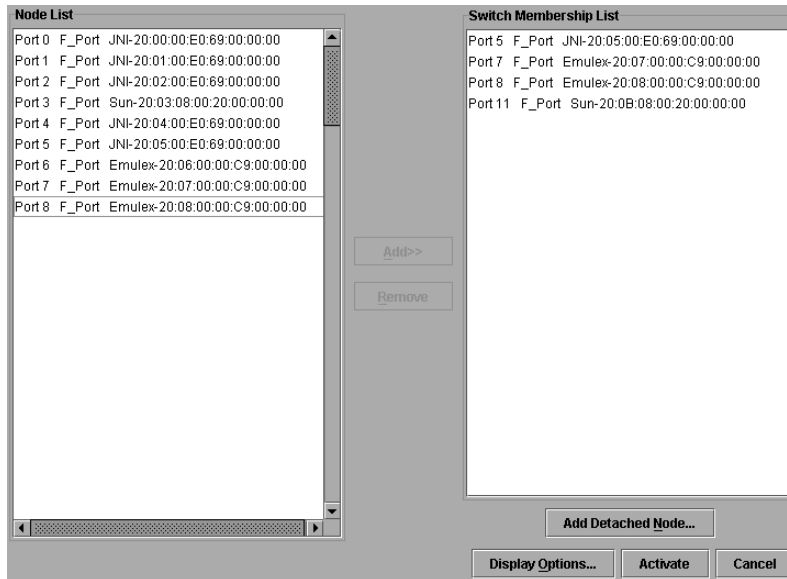


Figure 2–29: Switch Binding Membership List dialog box

Refer to “[Configuring Switch Binding—Overview](#)” on page 2-54 for information on how the Switch Membership List is populated with WWNs according to options set in the **Switch Binding State Change** dialog box.

2. If nicknames are configured for WWNs through HAFM and you want these to display instead of WWNs in this dialog box, click **Display Options**. The **Display Options** dialog box displays.
3. Click **Nickname**, then click **OK**.
4. To prohibit connection to a director port from a WWN currently in the Membership List, click the WWN or nickname in the **Membership List**, then click **Remove**. The WWN or nickname will move to the **Node List** panel. WWNs can only be removed from the fabric if any of the following is true:
 - The director is offline.
 - Switch Binding is disabled.
 - The director or device with the WWN is not connected to the director.

- Switch Binding is not enabled for the same port type as enabled for the Connection Policy in the **Switch Binding State Change** dialog box. For example, a WWN for a director attached to an E_Port can be removed if the Switch Binding Connection Policy was enabled to Restrict F_Ports.
 - The director or device with the WWN is connected to a port that is blocked.
 - The director or device with the WWN is not currently connected to the director (detached node).
5. WWNs can be added to the **Switch Membership List** (and thereby allowed connection) when Switch Binding is either enabled or disabled. To allow connection to a director port from a WWN in the **Node List** panel, select the WWN or nickname in the **Node List** panel, then click **Add**. The WWN or nickname will move to the **Membership List** panel.
 6. To add a WWN for a device or director not currently connected to the director, click **Detached Node**. The **Add Detached Node** dialog box displays.
 7. Enter the appropriate WWN or nickname (if configured through HAFM) and click **OK**. The WWN or nickname appears in the **Switch Membership List**.
 8. Click **Activate** to enable the changes and close the dialog box.

Enable/Disable and Online State Functions

In order for Switch Binding to function, specific operating parameters and optional features must be enabled. Also, there are specific requirements for disabling these parameters and features when the director or switch is offline or online. Be aware of the following:

- Switch Binding can be enabled or disabled whether the director is offline or online.
- Enabling Enterprise Fabric Mode automatically enables Switch Binding.
- You cannot disable Switch Binding if Enterprise Fabric Mode is enabled.
- If Enterprise Fabric Mode is enabled and the director or switch is online, you cannot disable Switch Binding. However, if Enterprise Fabric Mode is disabled, you can disable Fabric Binding, Switch Binding, or both.
- If Enterprise Fabric Mode is enabled and the director or switch is offline you can disable Switch Binding, but Enterprise Fabric Mode will also disable.
- WWNs can be added to the Switch Membership List when Switch Binding is enabled or disabled.

- WWNs can only be removed from the Switch Membership List if any of the following are true:
 - The director or switch is offline.
 - Switch Binding is disabled.
 - The director or device with the WWN is not connected to the director or switch.
 - Switch Binding is not enabled for the same port type as enabled for the Connection Policy in the **Switch Binding State Change** dialog box. For example, a WWN for a director attached to an E_Port can be removed if Switch Binding Connection Policy was enabled to Restrict F_Ports.
 - The director or device with the WWN is connected to a port that is blocked.
 - The director or device with the WWN is not currently connected to the director or switch (detached node).
- If the director or switch is online and Switch Binding is not enabled, all nodes and directors attached to the director or switch are automatically added to the Switch Membership List.

Zoning with Switch Binding Enabled

Note that SANtegrity has no effect on existing zoning configurations. However, note that if a device WWN is in a specific zone, but the WWN is not in the Switch Membership List, the device cannot log in to the director or switch port and cannot connect to other devices in the zone with Switch Binding enabled.

Enterprise Fabric Mode

Enterprise Fabric Mode is an option available on the **Fabrics** menu in the *HAFM* application if the SANtegrity feature key is installed. This option automatically enables the following features and operating parameters that are necessary in multi-switch Enterprise Fabric environments. Note that there are specific requirements for disabling these parameters and features when the director or switch is offline or online. The features and parameters enabled are:

Fabric Binding

This is a SANtegrity feature enabled through the **Fabrics** menu in HAFM that allows or prohibits switches and directors from merging with a selected fabric. Refer to [“Enable/Disable and Online State Functions”](#) on page 2-58 for details on enabling/disabling Fabric Binding with Enterprise Fabric Mode enabled.

Switch Binding

This is a SANtegrity feature enabled through the **Configure** menu in the Product Manager that allows or prohibits switches and/or directors from connecting to director E_Ports, devices from connecting to F_Ports. Refer to “[Enable/Disable and Online State Functions](#)” on page 2-58 for details on enabling/disabling Switch Binding with Enterprise Fabric Mode enabled.

Rerouting Delay

Rerouting delay is a parameter in the **Configure Switch Parameters** dialog box, available from **Configure** menu in the *Product Manager* application.

Rerouting Delay ensures that frames are delivered through the fabric in order to their destination. If there is a change to the fabric topology that creates a new path (for example, a new director is added to the fabric), frames may be routed over this new path if its hop count is less than a previous path with a minimum hop count. This may result in frames being delivered to a destination out of order since frames sent over the new, shorter path may arrive ahead of older frames still in route over the older path. If Rerouting Delay is enabled, traffic ceases in the fabric for the time specified in the E_D_TOV field of the **Configure Fabric Parameters** dialog box (**Configure** menu). This delay enables frames sent on the old path to exit to their destination before new frames begin traversing the new path.

If Enterprise Fabric Mode is enabled, this option is automatically enabled and cannot be disabled unless the director or switch is offline. In this case, disabling Rerouting Delay also disables Enterprise Fabric Mode.

Domain RSCNs

This is a parameter in the **Configure Switch Parameters** dialog box, available from **Configure** menu in the *Product Manager* application. Domain register for state change notifications (domain RSCNs) are sent between end devices in a fabric to provide additional connection information to host bus adapters (HBA) and storage devices. As an example, this information might be that a logical path has been broken because of a physical event, such as a fiber optic cable being disconnected from a port.

If Enterprise Fabric Mode is enabled, this parameter is automatically enabled and cannot be disabled unless the director or switch is offline. In this case, disabling Domain RSCNs also disables Enterprise Fabric Mode.

Insistent Domain Identification (ID)

Insistent Domain Identification (ID) is a parameter in the **Configure Switch Parameters** dialog box, available from **Configure** menu in the *Product Manager* application. Enabling this option sets the domain ID configured in the **Preferred Domain ID** field in the **Configure Switch Parameters** dialog box as the active domain identification when the fabric initializes. A static and unique domain identification is required by the Fabric Binding feature because the feature's Fabric Membership list identifies directors by WWN and Domain ID. If a duplicate preferred domain ID is used, then insisted, warnings occur when directors and switches are added to a Fabric Membership List.

If Fabric Binding or Enterprise Fabric Mode is enabled, this option is automatically enabled and cannot be disabled unless these options are disabled when the director or switch is offline. If the director or switch is online, disabling Insistent Domain ID will disable Enterprise Fabric Mode and Fabric Binding.

Connect Cables to the Fibre Channel Ports

Use these steps to connect Fibre Channel port cables:

1. Route the fiber-optic cables from customer-specified devices to ports at the front of the Director 2/140.
2. Bundle Fibre Channel cables from the director and other equipment (groups of 16 maximum), and secure them as directed by the customer.
3. Set the director online. For instructions, see “[Set the Director Online](#)” on page 2–25.

Connect the Director to a Fabric

To attach the director to a multi-switch fabric, connect the director to an E_Port of another director or switch. The E_Port to E_Port connection is referred to as an ISL.

Use these steps to fabric-attach the director and create an ISL:

1. Verify that the director is defined via HAFM. See “[Enabling HAFM to Manage the Director](#)” on page 2–17.
2. Verify that the preferred domain ID for the director is unique and does not conflict with the ID of another director or switch participating in the fabric. To change the domain ID, see “[Configure Fabric Operating Parameters](#)” on page 2–31.

3. Verify that the R_A_TOV and E_D_TOV values for the director are identical to the values for all directors and switches participating in the fabric.
4. Route a multi-mode or single-mode fiber-optic cable (depending on the ISL distance between directors) between customer-specified E_Ports of both directors.
5. At the **Products View** page, click the Director 2/140 icon. The **Hardware View** page for the selected director displays.
6. Click the UPM card graphic supporting the E_Port connection to open the **Port Card View** page.
7. Click the E_Port connector to open the **Port Properties** dialog box, as shown in [Figure 2–30](#).
8. Verify that the **Link Incident** field displays None and the **Segmentation Reason** field is blank or displays N/A. If an ISL segmentation or other problem is indicated, consult the *hp StorageWorks director 2/140 service manual* to isolate the problem. If no problems are indicated, installation is complete.

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 2–30: Port Properties dialog box

Unpack, Inspect, and Install the Ethernet Hub (Optional)

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

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

Using HAFM from a Remote Location

Use this section to install the HAFM client on a remote workstation.

Remote Workstation Minimum Requirements

The following minimum requirements must be met in order to install HAFM on a remote workstation.

IMPORTANT: In order for HAFM to function properly, compatible versions must be installed on both the client and server machines.

- Windows, UNIX or Workstation with color monitor, keyboard, and mouse using:
 - Intel Pentium processor with a 200 MHz or greater clock speed, and the Microsoft Windows 95, Windows 98, Windows ME, Windows 2000, Windows NT 4.0, Windows XP, Unix, or Linux 2.2 operating system.
 - HP HA PA-RISC processor with a 360 MHz or greater clock speed, using the HP-UX 11 or higher operating system.
 - Sun Microsystems UltraPARC-II processor with a 300 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 233 MHz or greater clock speed, or POWER3 microprocessor with a 333 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.
- 32 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 4.0 or later).

Install HAFM Client on a Remote Workstation

Use these steps to install HAFM on a remote client:

1. Verify the workstation and the Ethernet LAN segment (with the Director 2/140 attached) are connected through the Internet.
2. At the workstation, launch the browser application.
3. At the browser, type the HAFM server IP address.
4. The HAFM splash screen displays with the following options, see [Figure 2–31](#).
 - a. **Install HAFM remote client application**—Choose this option to install the application for your workstation platform.
 - b. **Download SNMP MIB files**—The Management Information Base (MIB) files are provided in standard ASN.1 syntax and may be installed into the MIB database of any SNMPv2 compliant Network Management Station.



Figure 2–31: HAFM remote client install

5. To install the remote client application, scroll down to the information that pertains to your platform, and follow the instructions provided.
6. After you have downloaded the installer executable, the **InstallAnywhere Wizard** displays. Follow the instructions provided to continue the installation.

Launch HAFM from the Remote Client

Use these steps to launch HAFM from a remote client:

1. Double-click the **HAFM** icon to launch HAFM. The **HAFM Login** screen displays.
2. Type the user name and password.

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

3. Choose an HAFM server from the **HAFM Server** drop-down list.
4. Click **Login**. The **Products View** page displays.

Using EWS to Configure the Director 2/140

This chapter contains information on how to launch and configure the Embedded Web Server. The configuration portion defines specific Director 2/140 system settings, including:

- Ports
- Network addresses
- Identification and contact information
- Date and time
- Operating parameters
- SNMP settings
- Passwords and user privileges.

This chapter covers the initial set up of the Director 2/140. For additional information regarding setting up zoning, zone sets, and SAN management in general, see the *hp StorageWorks embedded web server user guide*.

NOTE: Although products can perform normal operations without an HAFM server, the HAFM server should operate at all times to monitor product operations, report failures, log event changes, and log configuration changes.

Launch EWS

Use the following steps to launch EWS.

NOTE: Internet access and a standard Web browser is required. HP recommends Netscape Navigator 4.6 or higher, or Microsoft Internet Explorer 4.0 or higher.

1. Verify that the computer and Ethernet LAN segment (with the Director 2/140 attached) connect through the Internet.
2. Launch the browser application.

3. At the browser, enter the director IP address in the **Uniform Resource Locator (URL)** field. The **Enter Network Password** dialog box displays, as shown in [Figure 3–1](#).
4. Type the default user name and password, or the user name and password assigned by the administrator.
NOTE: The default user name is Administrator and the default password is password. The user name and password are case-sensitive.
5. Click **OK**. EWS opens showing the **View** page, as shown in [Figure 3–2](#).

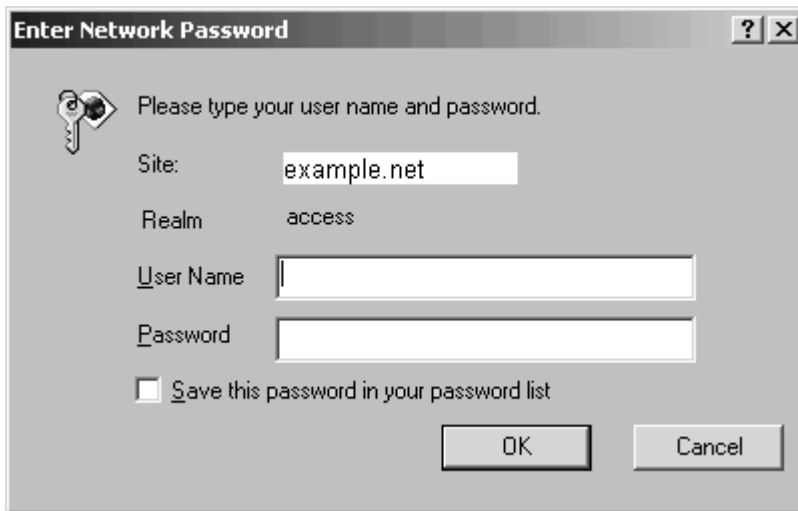


Figure 3–1: Enter Network Password dialog box

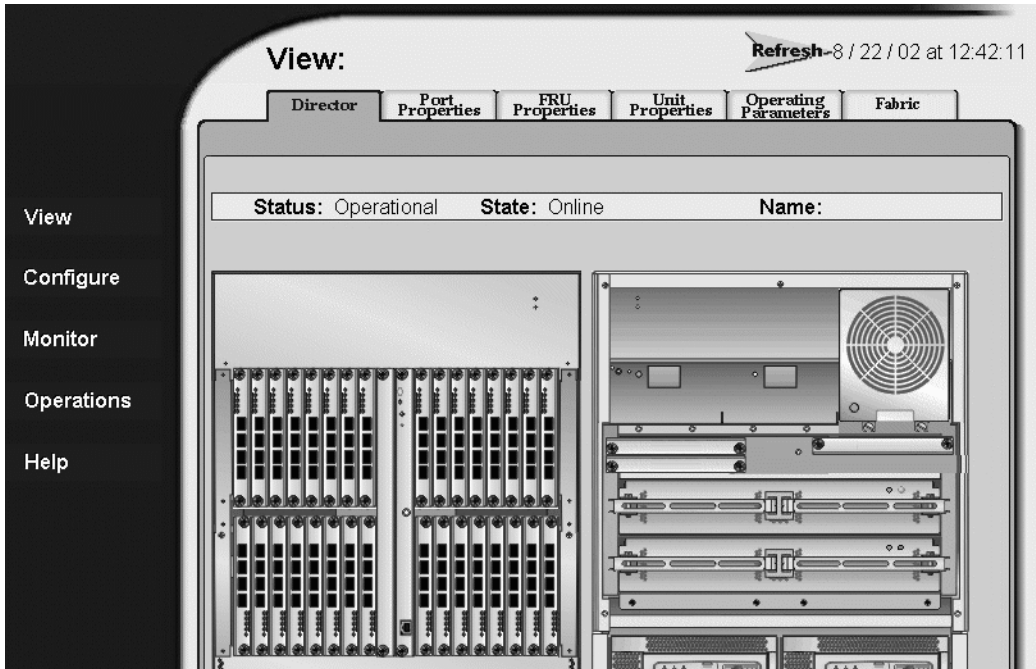


Figure 3–2: View page

Configure Director Ports

Use the following procedure to configure the names and settings for director Fibre Channel ports:

1. At the **View** page, choose the **Configure** option at the left side of the panel. The **Ports** page displays, as shown in [Figure 3–3](#). Use the vertical scroll bar as necessary to display additional port information rows (up to 143 ports).
 - a. For each port, type a port name of 24 or fewer alphanumeric characters in the associated **Name** field. The port name should identify the device to which the port is attached.
 - b. Click the check box in the **Blocked** column to block or unblock a port (default is unblocked). A check mark indicates a blocked port. Blocking a port prevents the attached device from communicating with the director.

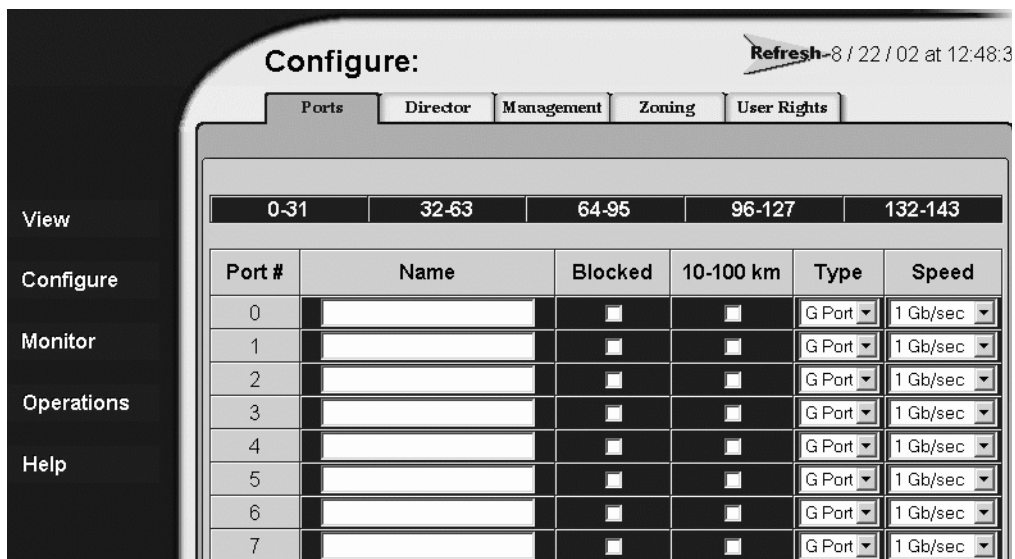


Figure 3–3: Ports page

- c. Click the check box in the **10-100 km** column to enable extended distance buffering for a port (the default is disabled). A check mark in the box enables extended distance operation up to 100 kilometers (through repeaters).
2. Scroll down to the bottom of the page and click **Activate** to save the information. The message “Your changes to the port configuration have been successfully activated” displays.

Configure Director Identification

Perform this procedure to configure the director name, description, location, and contact person. The *Name*, *Location*, and *Contact* variables configured here correspond respectively to the SNMP variables *sysName*, *sysLocation*, and *sysContact*. SNMP management workstations use these variables to obtain data from directors.

Use the following steps to configure the director identification:

1. At the **Configure** page, click the **Director** tab. The **Identification** page displays, as shown in [Figure 3–4](#).

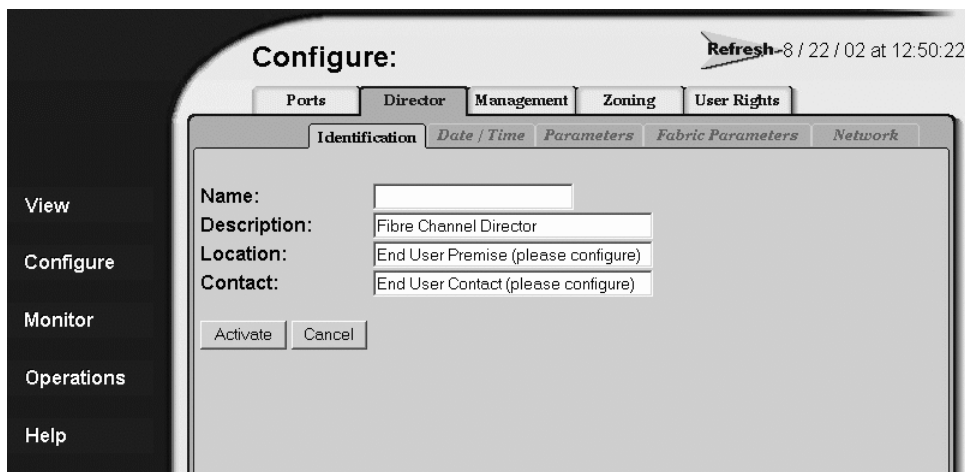


Figure 3–4: Identification page

- a. Type a director name of 24 or fewer alphanumeric characters in the **Name** field. Configure each director with a unique name.
 If the director is installed on a public LAN, the name should reflect the director’s Ethernet network DNS host name. For example, if the DNS host name is SAN140.hp.com, the name entered in this dialog box is SAN140.
 - b. Type a director description of 255 or fewer alphanumeric characters in the **Description** field.
 - c. Type the director’s physical location (255 or fewer alphanumeric characters) in the **Location** field.
 - d. Type the name and phone number of a contact person (255 or fewer alphanumeric characters) in the **Contact** field.
2. Click **Activate** to save the information. The message “Your changes to the identification configuration have been successfully activated” displays.

Configure Date and Time

Use this procedure to configure the director date and time:

1. At the **Configure** page, click the **Director** tab, then choose the **Date/Time** tab. The **Date/Time Properties** page displays, as shown in [Figure 3–5](#).

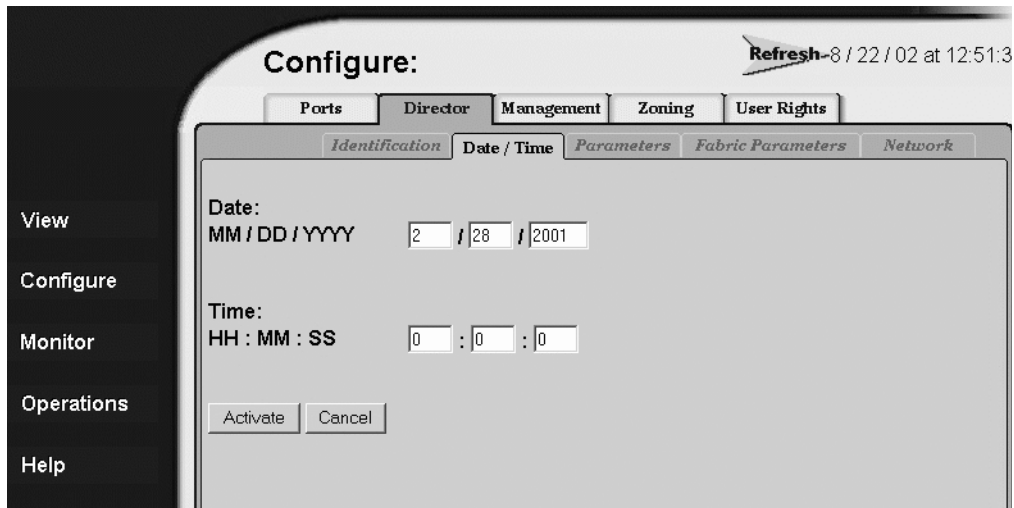


Figure 3–5: Date/Time Properties page

- a. Click the **Date** fields that require change. Type changes using the following ranges:
 - Month (MM): 1 through 12
 - Day (DD): 1 through 31
 - Year (YYYY): greater than 1980
 - b. Click the **Time** fields that require change. Type changes in the following ranges:
 - Hour (HH): 0 through 23
 - Minute (MM): 0 through 59
 - Second (SS): 0 through 59
2. Click **Activate** to save the information. The message “Your changes to the date/time configuration have been successfully activated” displays.

Configure Operating Parameters

Use this procedure to configure the following operating parameters:

- BB_Credit
- R_A_TOV

- E_D_TOV
- Preferred Domain ID
- Interop Mode
- Switch Priority
- Rerouting Delay

First, set the director offline as follows.

1. At the **View** page, select the **Operations** option at the left side of the panel. The **Operations** page opens with the **Port Beaconsing** page displayed.
2. At the **Operations** page, click the **Online State** tab. The **Current State** page displays, as shown in [Figure 3–6](#).

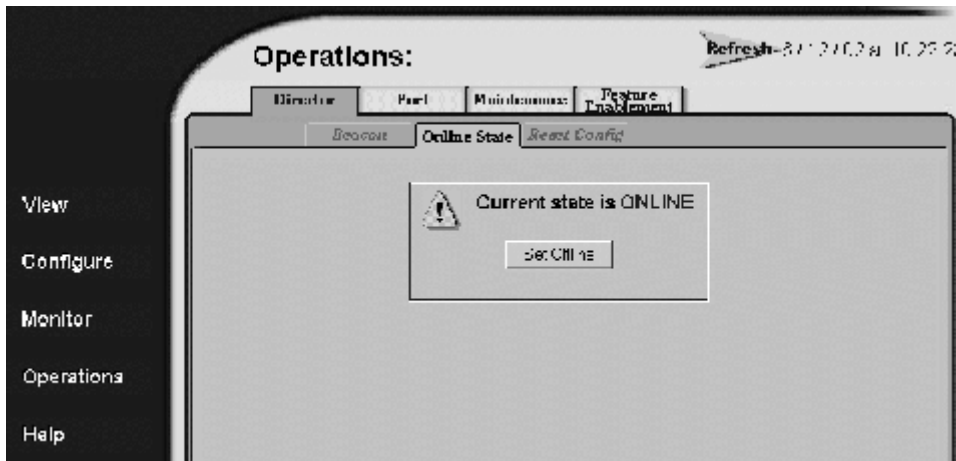


Figure 3–6: Current State page

3. Click **Set Offline**. The message “Your operations changes have been successfully activated” displays.
4. Next, select the **Configure** option at the left side of the panel. The **Configure** page opens with the **Ports** page displayed.
5. Click the **Director** tab, then click the **Parameters** tab. The **Parameters** page displays, as shown in [Figure 3–7](#).

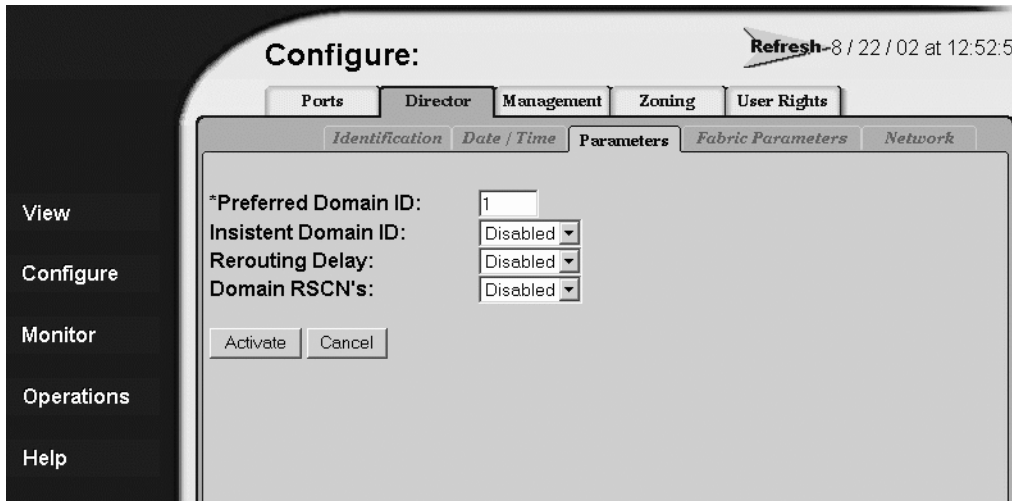


Figure 3–7: Parameters page

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

6. Use information under “[Switch Parameters](#)” to change settings as required for parameters in this dialog box.
7. After you change settings, click the **Activate** button.
8. Return the director to online as follows.
 - a. At the **View** page, select the **Operations** option at the left side of the panel. The **Operations** page opens with the **Port Beaconing** page displayed.
 - b. At the **Operations** page, click the **Online State** tab, then click **Set Online**. The message “Your operations changes have been successfully activated” displays.

Switch Parameters

Configure the following parameters as required by your fabric.

Domain ID

The domain identification is a value between 1 and 31 that provides a unique identification for the director in a fabric. A fabric director cannot contain the same domain ID as another director or their E_Ports will segment when they try to join.

In the **Configure Switch Parameters** dialog box, a field is provided to enter a preferred domain ID and a check box is provided to enable this ID as an insistent domain ID.

Preferred

NOTE: To change this value, you must first set the director offline. Choose **Set Online State** from the **Maintenance** menu to display the **Set Online State** dialog box, then click **Set Offline**. Be sure to set the director back online after you change this value.

Use this field to set the a unique domain ID for the director. The default value is 1. Set a value between 1 and 31. When a director comes online with a preferred ID, it requests an ID from the fabric's principal director (indicating its preferred value as part of the request). If the requested domain ID is not allocated to the fabric, the domain ID is assigned to the requesting director. If the requested domain ID is already allocated, an unused domain ID is assigned. Note that you must set the director offline before you can change to the preferred domain ID.

The preferred domain ID must be unique for each director and switch in a fabric. If two switches or directors have the same preferred domain ID, the E_Ports segment, causing the fabric to segment.

For more information on domain ID, refer to the section on domain ID assignment for multi-switch fabrics in the *hp StorageWorks high availability planning guide* for details.

Insistent

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

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

- This option is required if Enterprise Fabric Mode (optional SANtegrity binding feature) is enabled.
- If you enable Insistent Domain while the switch or director is online, the Preferred Domain ID will change to the current active domain ID if the IDs are different.



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

Rerouting Delay

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

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

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

NOTE: This option is required if Enterprise Fabric Mode (optional SANtegrity binding feature) is enabled.

Domain RSCNs

Domain register for state change notifications (domain RSCNs) are sent between end devices in a fabric to provide additional connection information to host bus adapters (HBA) and storage devices. As an example, this information might be that a logical path has been broken because of a physical event, such as a fiber optic cable being disconnected from a port. Consult with your HBA and storage device vendor to determine if enabling Domain RSCNs will cause problems with your HBA or storage products. Note that this option is required if Enterprise Fabric Mode (optional SANtegrity binding feature) is enabled.

Configure Fabric Operating Parameters

Use procedures in this section to set parameters on the director for fabric operation through the **Fabric Parameters** page. These operating parameters are stored in NV-RAM on the director.

First, set the director offline as follows.

1. At the **View** page, select the **Operations** option at the left side of the panel. The **Operations** page opens with the **Port Beaconsing** page displayed.
2. At the **Operations** page, click the **Online State** tab. The **Current State** page displays, as shown in [Figure 3–6](#).

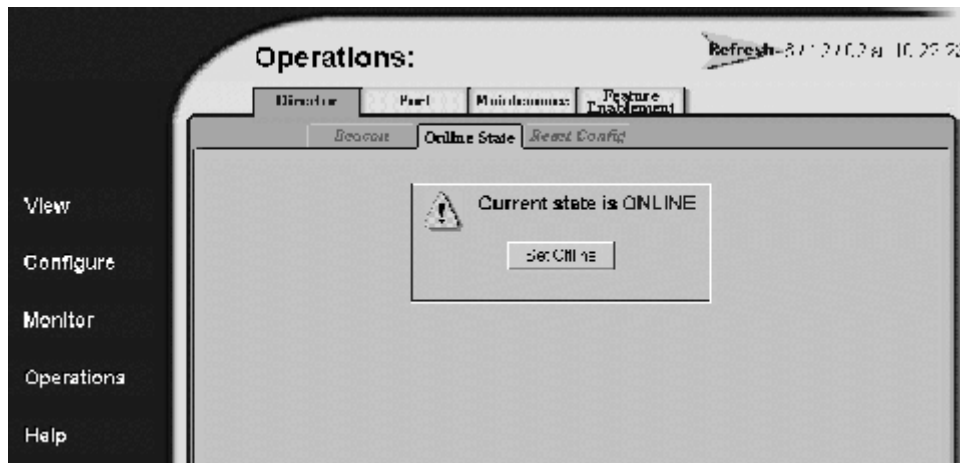


Figure 3–8: Current State page

3. Click **Set Offline**. The message “Your operations changes have been successfully activated” displays.
4. Next, select the **Configure** option at the left side of the panel. The **Configure** page opens with the **Ports** page displayed.
5. Click the **Director** tab, then click the **Fabric Parameters** tab. The **Fabric Parameters** page displays, as shown in [Figure 3–9](#).

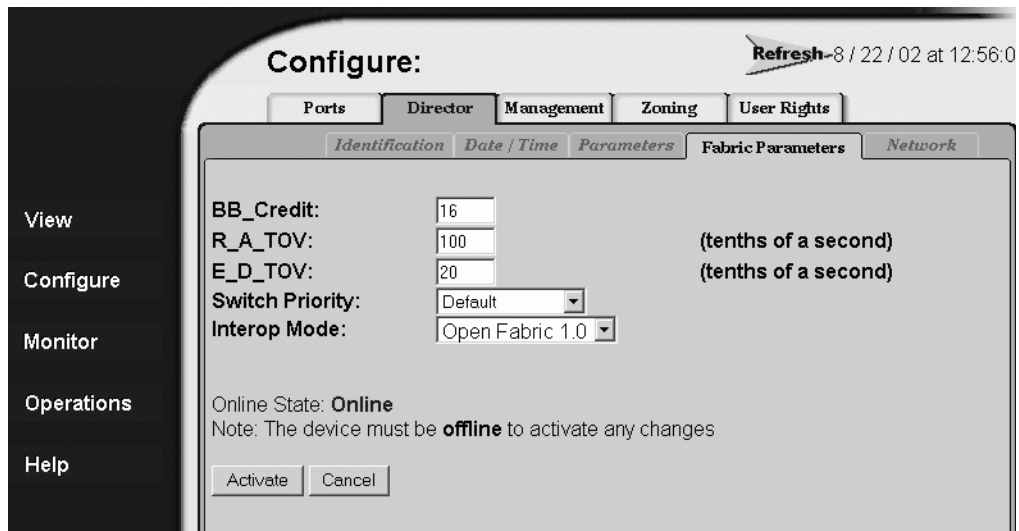


Figure 3–9: Fabric Parameters page

6. Use information under “[Fabric Parameters](#)” to change settings as required for parameters in this dialog box.
7. After you change settings, click **Activate**.
8. Back up the configuration data when you are finished configuring the switch.
9. Return the director to online as follows.
 - a. At the **View** page, select the **Operations** option at the left side of the panel. The **Operations** page opens with the **Port Beaconing** page displayed.
 - b. At the **Operations** page, click the **Online State** tab, then click **Set Online**. The message “Your operations changes have been successfully activated” displays.

Fabric Parameters

Configure the following parameters as required by your fabric.

BB_Credit

Configure the director to support buffer-to-buffer credit (BB_Credit) from 1 through 60. This is the value used for all ports, except those configured for extended distance buffering (10-100 km). The default value is 16. For a description of the buffer-to-buffer credit, refer to the industry specification, *Fibre Channel Physical and Signaling Interface*.

R_A_TOV

Configure resource allocation time-out value (R_A_TOV) in tenth-of-a-second increments. This variable works with the error detect time-out value (E_D_TOV) variable to control the director's behavior when an error condition occurs. Resources are allocated to a circuit when errors are detected and are not released for reuse until the time set by the R_A_TOV value expires. The default value is 100 tenths (10 seconds). Set a value between 10 tenths and 1200 tenths (1 through 120 seconds).

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

E_D_TOV

Adjust the E_D_TOV in tenth-of-a-second increments. An error condition occurs when an expected response is not received within the time limit set by this value. The default value is 20 tenths (2 seconds). Set a value between 2 tenths through 600 tenths (.2 through 60 seconds).

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

Switch Priority

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

Setting these priority values determines the principal director selected for the multi-switch fabric. For example, if you have three directors in the fabric and set one as **Principal**, one as **Default**, and one as **Never Principal**, the unit set to **Principal** becomes the principal director in the fabric.

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

- If you have three directors and set all to **Default**, the director with the lowest WWN becomes the principal director.
- If you have three directors and set two to **Principal** and one to **Default**, the director with the **Principal** setting that has the lowest WWN becomes the principal director.
- If you have three directors and set two to **Default** and one to **Never Principal**, the director with the **Default** setting and the lowest WWN becomes the principal director.

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

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

In, for example, the audit log, you may notice that the **Principal** setting maps to a number code of 1, **Default** maps to a number code of 254, and **Never Principal** maps to a number code of 255. The number codes of 2 - 253 are not currently in use.

Interop Mode

Select one of the following options:

- **Homogeneous Fabric**—Select this mode if the fabric contains only HP directors and switches that are operating in Homogeneous Fabric mode.
- **Open Fabric 1.0**—Default. Select this mode if the fabric contains HP directors and switches, as well as other open-fabric compliant switches. Select this mode for managing heterogeneous fabrics.

Configure Network Information

Verify the type of LAN installation with the customer's network administrator. If one director is installed on a dedicated LAN, network information (IP address, subnet mask, and gateway address) does not require change.

If multiple directors are installed, or a public LAN segment is used, network information must be changed to conform to the customer's LAN addressing scheme.

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

1. Choose the **Configure** option at the left side of the panel. The **Configure** page opens with the **Ports** page displayed.
2. At the **Configure** page, click the **Director** tab, then click the **Network** tab. The **Network** page displays, as shown in [Figure 3–10](#).

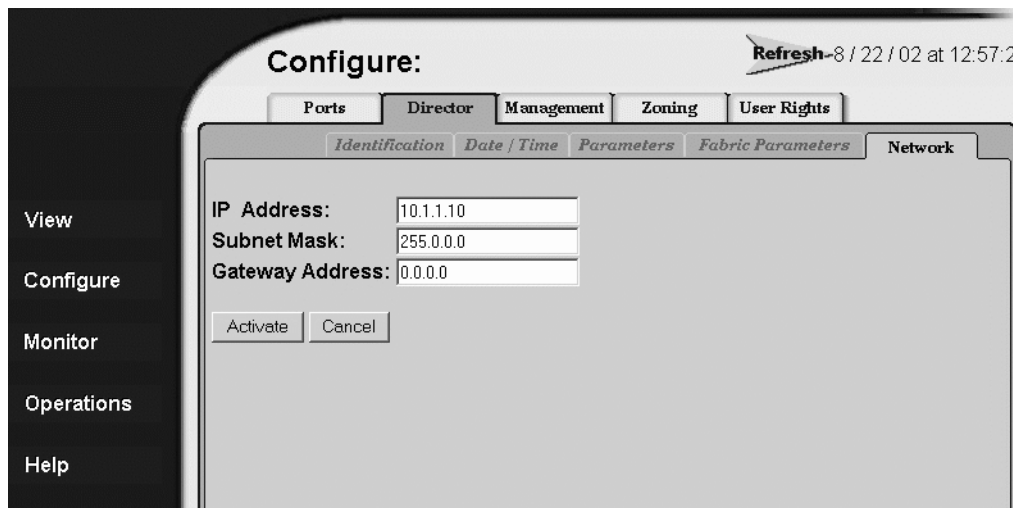


Figure 3–10: Network page

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

3. Click **Activate** to save the information. The **Activate** message displays, as shown in [Figure 3–11](#).

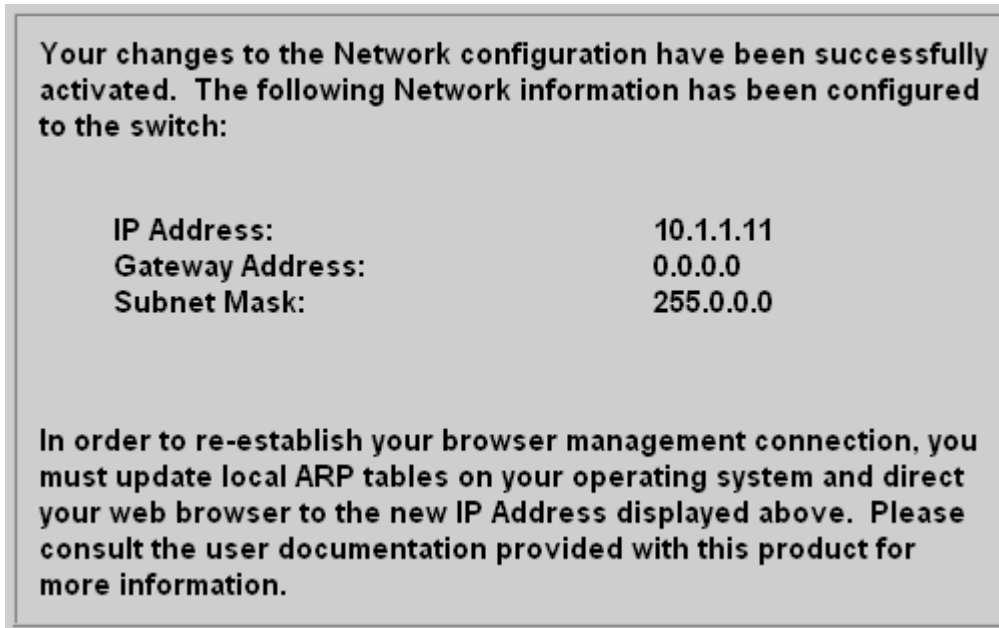


Figure 3–11: Activate message box

4. Update the address resolution protocol (ARP) table as follows.
 - a. Choose **File > Close**. The Windows desktop displays.
 - b. At the Windows desktop, choose **Start > Programs > Accessories > Command Prompt**. A disk operating system (DOS) window displays.
 - c. Delete the director's old IP address from the ARP table. At the command (C:) prompt, type `arp -d xxx.xxx.xxx.xxx`, where `xxx.xxx.xxx.xxx` is the old IP address for the Director 2/140.
 - d. Close the DOS window.

Configure SNMP Trap Message Recipients

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

1. Launch EWS. See “[Launch EWS](#)” on page 3–1.
2. If network information was configured at the browser, go to [step 3](#). If network information was not configured, choose the **Configure** option at the left side of the panel. The **Configure** page opens with the **Ports** page displayed.
3. At the **Configure** page, click the **SNMP** tab. The **SNMP** page displays, as shown in [Figure 3–12](#).

Configure: Refresh - 3 / 15 / 02 at 8:41

Ports Director Management Zoning User Rights

SNMP CLI

Enable Authorization Traps

Community Name	Write Authorization	Trap Recipient	UDP Port Number
public	<input checked="" type="checkbox"/>		163
	<input type="checkbox"/>		
	<input type="checkbox"/>		
	<input type="checkbox"/>		
	<input type="checkbox"/>		
	<input type="checkbox"/>		

Activate Cancel

Figure 3–12: SNMP page

- a. For each trap recipient, type a community name of 32 or fewer alphanumeric characters in the associated **Community Name** field. The community name is incorporated in SNMP trap messages to prevent unauthorized viewing or use.

- b. Click the check box in the **Write Authorization** column to enable or disable write authorization for the trap recipient (default is disabled). A check mark in the box indicates write authorization is enabled. When the feature is enabled, a management workstation user can change *sysContact*, *sysName*, and *sysLocation* SNMP variables.
 - c. Type the IP address or DNS host name of the trap recipient (SNMP management workstation) in the associated **Trap Recipient** field. Use 64 or fewer alphanumeric characters. HP recommends using the IP address.
 - d. The default UDP port number for trap recipients is 162. To override this port number, click the **Advanced** option. The dialog box expands to show a **UDP Port Number** column.
 - e. Type a decimal port number in the associated **UDP Port Number** field to override the default value.
4. Click **Activate** to save the information. The message “Your changes to the SNMP configuration have been successfully activated” displays.

Configure User Rights

Use this procedure to configure the administrator-level and operator-level passwords required to access EWS through the **Username and Password Required** page.

1. At the **Configure** page, click the **User Rights** tab. The **User Rights** page displays, as shown in [Figure 3–13](#).

User	Access Level:	New User Name:	New Password:	Confirm New Password:
Administrator		<input type="text" value="Administrator"/>	<input type="password" value="XXXXXXXXXX"/>	<input type="password" value="XXXXXXXXXX"/>
Operator		<input type="text" value="Operator"/>	<input type="password" value="XXXXXXXXXX"/>	<input type="password" value="XXXXXXXXXX"/>

Figure 3–13: User Rights page

2. For the **Administrator** set of data fields:
 - a. Type the administrator user name (as specified by the customer’s network administrator) in the **New User Name** field. Use 16 or fewer alphanumeric characters.
 - b. Type the administrator password (as specified by the customer’s network administrator) in the **New Password** field. Use 16 or fewer alphanumeric characters.
 - c. Type the administrator password again in the **Confirm New Password** field.
3. For the **Operator** set of data fields:
 - a. Type the operator user name (as specified by the customer’s network administrator) in the **New User Name** field. Use 16 or fewer alphanumeric characters.

- b. Type the operator password (as specified by the customer's network administrator) in the **New Password** field. Use 16 or fewer alphanumeric characters.
 - c. Type the operator password again in the **Confirm New Password** field.
4. Click **Activate** to save the information. The message "Your changes to the user rights configuration have been successfully activated" displays.
5. Choose **File > Close**. The Windows desktop displays.

Manage Firmware Versions

The Director 2/140 internal operating code 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. This chapter contains information on the following firmware management tasks:

- [Determine a Director Firmware Version](#), page 4–1
- [Add a Firmware Version](#), page 4–2
- [Modify a Firmware Version Description](#), page 4–5
- [Delete a Firmware Version](#), page 4–6
- [Download a Firmware Version to a Director](#), page 4–6
- [Back Up the Director's Configuration](#), page 4–9

Determine a Director Firmware Version

Use these steps to determine the Director 2/140 firmware version:

1. At the HAFM server, open the *HAFM* application. The **Products View** page displays.
2. Double-click the icon representing the switch to be inspected for firmware version. The **Hardware View** page for the selected switch displays.
3. Choose **Maintenance > Firmware Library**. The **Director Firmware Library** dialog box displays, as shown in [Figure 4–1](#).

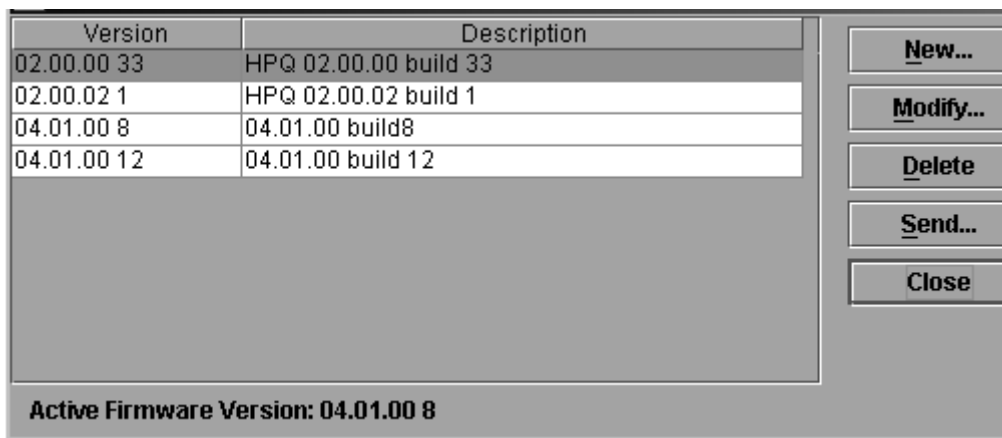


Figure 4–1: Firmware Library dialog box

- 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
 - ZZ is the patch level
- Click **Close**.

Add a Firmware Version

The firmware version shipped with the director is provided on the Director 2/140 documentation 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 the Release Notes that accompany the firmware version. This information supplements information provided in this general procedure.

Use these steps to add a director firmware version to the library stored on the HAFM server hard drive:

- Obtain the new firmware version from the HP website:

NOTE: The following path is subject to change.

- a. At the HAFM server or other personal computer (PC) with Internet access, open the HP website. The uniform resource locator (URL) is <http://thenew.hp.com/country/us/eng/support.html>.
 - b. Click on **Firmware Downloads** in left panel.
 - c. Click the **Director Firmware Version XX.YY.ZZ** entry, where *XX.YY.ZZ* is the desired version. The **Windows Save As** dialog box displays.

Verify or correct the directory path specified in the **Save in** field and the file name specified in the **File name** field.
 - d. 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** page displays.
 3. Double-click the icon representing the director to which the firmware version will be added. The **Hardware View** page for the selected director displays.
 4. Choose **Maintenance > Firmware Library**. The **Director Firmware Library** dialog box displays, as shown in [Figure 4-1](#).
 5. Click **New**. The **New Firmware Version** dialog box displays, as shown in [Figure 4-2](#).

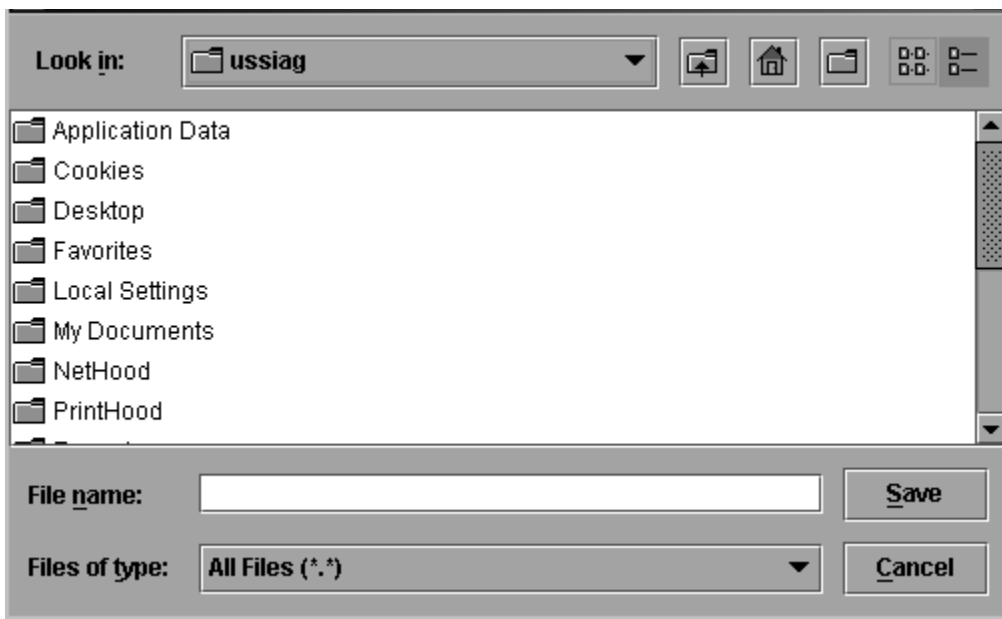


Figure 4–2: New Firmware Version dialog box

6. Select the desired firmware version file (downloaded in [step 1](#)) from the HAFM server Zip drive, CD ROM drive, or hard drive. Verify that the correct directory path and filename display in the **File name** field and click **Save**. The **New Firmware Description** dialog box displays. See [Figure 4–3](#).

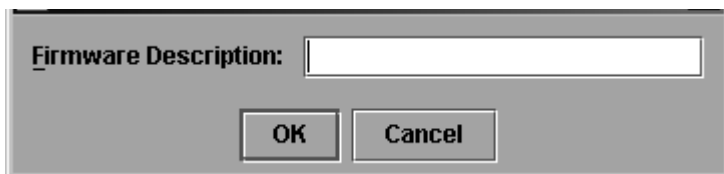


Figure 4–3: New Firmware Description dialog box

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 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 4–6.

Modify a Firmware Version Description

Use these steps 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** page displays.
2. Double-click the icon representing the director for which the firmware version description will be modified. The **Hardware View** page for the selected director displays.
3. Choose **Maintenance > Firmware Library**. The **Director Firmware Library** dialog box displays, as shown in [Figure 4–1](#).
4. Select the firmware version to be modified and click **Modify**. The **Modify Firmware Description** dialog box displays, as shown in [Figure 4–4](#).

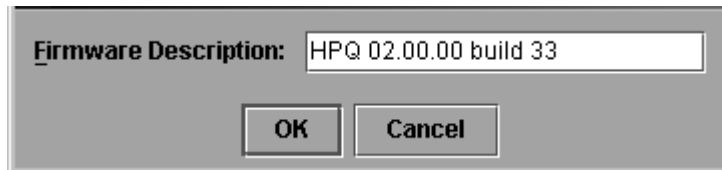


Figure 4–4: Modify Firmware Description dialog box

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 Firmware Library** dialog box. Click **Close** to close the dialog box and return to the *Product Manager* application.

Delete a Firmware Version

Use these steps to delete a firmware version from the library stored on the HAFM server hard drive:

1. At the HAFM server, open the *HAFM* application. The **Products View** page displays.
2. Double-click the icon representing the director from which the firmware version will be deleted. The **Hardware View** page for the selected director displays.
3. Choose **Maintenance > Firmware Library**. The **Director Firmware Library** dialog box displays, as shown in [Figure 4-1](#).
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 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. Although traffic is not disrupted, the green port LEDs will flicker or blink during the IPL portion of this operation as control is passed to the other CTP card.

NOTE: When downloading a firmware version, follow procedural information in the Release Notes that accompany the firmware version. This information supplements information provided in this general procedure.

Use these steps to download a firmware version to a director:

1. At the HAFM server, open the *HAFM* application. The **Products View** page displays.

2. Before downloading firmware version *XX.YY.ZZ* to a director, ensure the required, compatible version of the *HAFM* application is running on the HAFM server. Refer to the Release Notes that shipped with HAFM.
 - a. Choose **Help >About**. 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.
3. Double-click the icon representing the director to which the firmware version will be downloaded. The **Hardware View** page for the selected director displays.
4. As a precaution to preserve director configuration information, complete the data collection procedure as follows:
 - a. At the HAFM server, open the *HAFM* application. The **Products View** page displays.
 - b. Double-click the icon representing the director for which the configuration file will be backed up. The **Hardware View** page for the selected director displays.
 - c. Choose **Maintenance > Backup & Restore Configuration**. The **Backup and Restore Configuration** dialog box displays, as shown in [Figure 4-5](#).

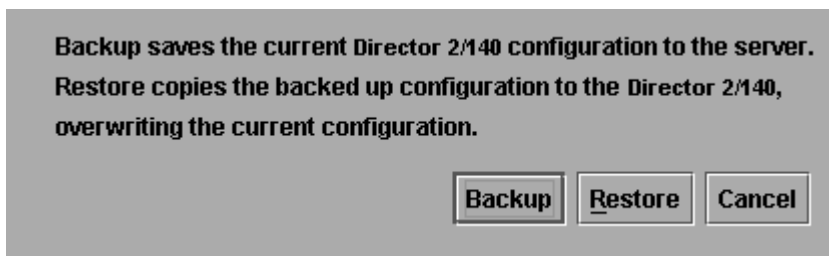


Figure 4-5: Backup and Restore Configuration dialog box

- d. Click **Backup**. When the backup process finishes, the **Backup Complete** dialog box displays.
 - e. Click **OK** to close the dialog box and return to the **Hardware View** page.
5. Choose **Maintenance > Firmware Library**. The **Director Firmware Library** dialog box displays, as shown in [Figure 4-1](#).

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, refer to the *hp StorageWorks director 2/140 service manual* for specific information on isolating the problem. If no error occurs, the **Send Firmware** confirmation box displays, as shown in [Figure 4-6](#).

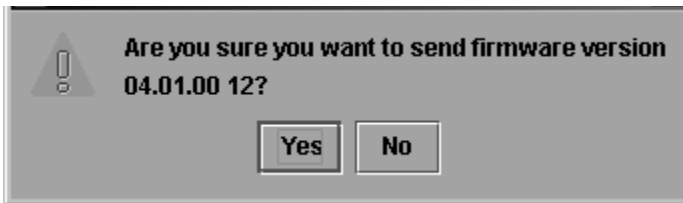


Figure 4-6: Send Firmware confirmation box

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 Initial Program Load (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 **Status** table turns yellow, the **Status** field displays **No Link**, and the **State** field displays a reason message.
- The alert panel at the bottom of the navigation control panel displays a grey square, indicating director status is unknown.
- Illustrated FRUs in the **Hardware View** page are removed, and then displayed again as the connection is re-established.

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.

8. Click **Close** to close the dialog box.
9. Click **Close** to close the **Director Firmware Library** dialog box and return to the **Hardware View** page.

Back Up the Director’s Configuration

Use these steps to back up the configuration file to the HAFM server.

1. At the HAFM server, open the *HAFM* application. The **Products View** displays.
2. Select the icon representing the director for which the configuration file will be backed up. The **Hardware View** page for the selected director displays.
3. Choose **Maintenance > Backup & Restore Configuration**. The **Backup and Restore Configuration** dialog box displays, as shown in [Figure 4–5](#).
4. Click **Backup**. When the backup process finishes, the **Backup Complete** dialog box displays.
5. Click **OK** to close the dialog box and return to the **Hardware View** page.

Regulatory Compliance Notices

This appendix covers the following topics:

- [Regulatory Compliance ID Numbers](#), page A-1
- [Federal Communications Commission Notice](#), page A-2
- [Canadian Notice \(Avis Canadien\)](#), page A-4
- [European Union Notice](#), page A-4
- [Japanese Notice](#), page A-5
- [Taiwanese Notice](#), page A-5
- [Laser Safety](#), page A-6
- [Declaration of Conformity](#), page A-8

Regulatory Compliance ID Numbers

For the purpose of regulatory compliance certifications and identification, your HP StorageWorks Director 2/140 is assigned an HP Regulatory Model Number. The HP Regulatory Model Number for this product is:

RSVLB-0214

The HP StorageWorks Director 2/140 Regulatory Model Number can be found on the product label, along with the required approval markings and information. When requesting certification information for this product, always refer to this Regulatory Model Number. This Regulatory Model Number should not be confused with the marketing name or product number for your HP StorageWorks Director 2/140.

Federal Communications Commission Notice

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

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

Class A Equipment

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

Class B Equipment

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

- Re-orient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio or television technician for help.

Declaration of Conformity for Products Marked with FCC Logo—United States Only

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

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

For questions regarding this FCC declaration, contact:

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

Or call 1-650-857-1501

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

Modifications

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

Network and Serial Cables

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

IEC EMC Statement (Worldwide)

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

Spécification ATI Classe A (France)

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

Canadian Notice (Avis Canadien)

Class A Equipment

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

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

Class B Equipment

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

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

European Union Notice

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

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

- EN55022 1998 (CISPR 22)-Electromagnetic Interference

- EN55024 1998 (IEC61000-4-2, IEC61000-4-3, IEC61000-4-4, IEC61000-4-5, IEC61000-4-6, IEC61000-4-8, IEC61000-4-11)-Electromagnetic Immunity
- EN60950 (IEC60950)-Product Safety
- Power Quality: (IEC61000-3-2)-Harmonics and (IEC61000-3-3)-Voltage Fluctuations and Flicker
- Also approved under UL 1950, 3rd Edition/CSA C22.2 No. 950-95, Safety of Information Technology Equipment

Japanese Notice

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

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

VCCIマークが付いていない場合には、次の点にご注意下さい。

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

Taiwanese Notice

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

Harmonics Conformance (Japan)

高調波ガイドライン適合品

German Noise Declaration

Schalldruckpegel $L_p = 70.3$ dB(A)
Am Arbeitsplatz (operator position)
Normaler Betrieb (normal operation)
Nach ISO 7779:1988 / EN 27779:1991 (Typprüfung)

Laser Safety



WARNING: To reduce the risk of exposure to hazardous radiation:

- Do not try to open the laser device enclosure. There are no user-serviceable components inside.
 - Do not operate controls, make adjustments, or perform procedures to the laser device other than those specified herein.
 - Allow only HP authorized service technicians to repair the laser device.
-

Certification and Classification Information

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

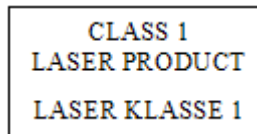
In the USA, the OLM is certified as a Class 1 laser product conforming to the requirements contained in the Department of Health and Human Services (DHHS) regulation 21 CFR, Subchapter J. The certification is indicated by a label on the plastic OLM housing.

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

The OLM includes the following certifications:



- UL Recognized Component (USA)
- CSA Certified Component (Canada)
- TUV Certified Component (European Union)
- CB Certificate (Worldwide)

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



Declaration of Conformity

The Declaration of Conformity is shown on the next page.

	DECLARATION OF CONFORMITY According to IEC/IEC Guide 22 and EN 45014
Manufacturer's Name: Hewlett-Packard Company	
Manufacturer's Address: 11311 Chinden Blvd. Boise, ID 83714 USA	
Declares, that the product	
Product Name: hp StorageWorks director 2/140	
Product Number: 316093-B21, DS-DMGGD-CA, and ED-6140	
Regulatory Model Number: RSVLB-0214	
Product Options: All	
Conforms to the following Product Specifications:	
Safety:	IEC 60950:1991+A1+A2+A3+A4 / EN 60950:1992+A1+A2+A3+A4+A11 GB 4943:1995 IEC 60825-1:1993 / EN 60825-1:1994 +A11, Class 1 (Laser/LED)
EMC:	CISPR 22:1997+A1 / EN 55022:1998 +A1 Class A GB 9254:1998 CISPR 24:1997 / EN 55024:1998 IEC 61000-3-2:1995 / EN 61000-3-2:1995 + A14 IEC 61000-3-3:1994 / EN 61000-3-3:1995
Supplementary Information: The product herewith complies with the requirements of the Low Voltage Directive /3/23/EEC and the EMC Directive 89/325/EEC and carries the CE-marking accordingly.	
1) The Product was tested in a worst-case configuration which maximizes RFI emissions.	
Boise, ID USA November 18, 2002	 George E. Barrett, Regulatory Mgr.
<small>European contact for regulatory topics only: Hewlett-Packard GmbH, HD-TRG, Hertenbergstr. 5/10, D-10245 Böblingen (FAX: +49-7031-14-0143)</small>	

Technical Specifications

This appendix contains the following information:

- [Physical Dimensions](#), page B-1
- [Environmental Specifications](#), page B-2
- [Power Requirements](#), page B-2
- [Operating Tolerances](#), page B-3
- [Laser Information](#), page B-3

Physical Dimensions

[Table B-1](#) lists Director 2/140 dimensions.

Table B-1: Dimensions

Dimension	Size
Height	52.7 cm (20.9 in)
Width	44.1 cm (17.5 in)
Depth	61.0 cm (24.2 in)
Weight	75.9 kg (167 lb)
Shipping Weight	102.1 kg (225 lb)

Environmental Specifications

Figure B-2 lists environmental ranges for shipping, storing, and operating the HP StorageWorks Director 2/140.

Table B-2: Environmental Specifications

Specification	Shipping	Storage	Operating
Weight	102.1 kg (225 lb)	75.9 kg (167 lb)	75.9 kg (167 lb)
Temperature	-40°F to 140°F (-40°C to 60 °C)	34°F to 140°F (1°C to 60 °C)	40°F to 104°F (4°C to 40 °C)
Humidity	5% to 100%	5% to 80%	8% to 80%
Maximum wet-bulb temperature	84°F (29°C)	84°F (29°C)	81°F (27°C)
Altitude	40,000 ft (12,192 m)	40,000 ft (12,192 m)	10,000 ft (3,048 m)

Power Requirements

Table B-3 lists Director 2/140 power requirements.

Table B-3: Power Requirements

Specification	Value
Input voltage	180 to 264 VAC
Input Current	4.66 amps at 180 VAC
Input Power	842 watts
Input frequency	47/63 Hz

Operating Tolerances

Table B-4 lists heating and cooling specifications, shock tolerances, vibration, acoustical noise and inclination.

Table B-4: Operating Tolerances

Specification	Value
Heat dissipation	842W (2,873 BTU/hr)
Cooling airflow clearances	Right and left sides: 2.5 cm (1.0 in) Front and rear: 7.6 cm (3.0 in) Top and bottom: No clearance required
Shock and vibration tolerance	60 Gs for 10 milliseconds without nonrecoverable errors
Acoustical noise	7.0 Bels "A" scale
Inclination	10° maximum

Laser Information

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

Table B-5: Laser Specs—2 Gb

Part Number	Transceivers on UPM Card	Wave Length	Media/Distance	Standard
300836-B21 Long wave - 35 Km	4 Extended Long wave	1310 nm	9/125 µm Single-mode: 1 m–35 Km	100-SM-LL-L
300835-B21 Long wave - 10 Km	4 Long wave	1310 nm	9/125 µm Single-mode: 1 m–10 Km	100-SM-LL-L

Part Number	Transceivers on UPM Card	Wave Length	Media/Distance	Standard
300834-B21 Short wave	4 Short wave	850 nm	50/125 μm multi-mode: 2 m–500 m 62.5/125 μm multi-mode: 1 m–200 m	100-M5-SN-I

Electrostatic Discharge

This appendix contains the following information:

- [Precautions Against Electrostatic Discharge](#)
- [Grounding Methods](#)

Precautions Against Electrostatic Discharge

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

To prevent electrostatic damage, observe the following precautions:

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

Grounding Methods

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

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

- Use heel straps, toe straps, or boot straps at standing workstations. Wear the straps on both feet when standing on conductive floors or dissipating floor mats.
- Use conductive field service tools.
- Use a portable field service kit with a folding static-dissipating work mat.

If you do not have any of the suggested equipment for proper grounding, have an HP authorized service provider install the part.

NOTE: For more information on static electricity, or for assistance with product installation, contact an HP authorized service provider.

Glossary

This glossary defines terms used in this guide or in other guides in this series, and is not a comprehensive glossary of computer terms.

The following cross-references are used in this glossary:

Contrast with. This refers to a term that has an opposite or substantively different meaning.

See. This refers the reader to another keyword or phrase for the same term.

See also. This refers the reader to additional information contained in another entry.

access control

List of all devices that can access other devices across the network and the permissions associated with that access.

See also persistent binding and zoning.

active FRU

A field-replaceable unit that is currently operating as the active and not the 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

SNMP message notifying an operator of a network or device problem.

alias server

Fabric software facility that supports multicast group management.

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.

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 will cause LEDs to flash for selected components.

BB_Credit

Also known as Buffer-to-Buffer Credit. Indicates the maximum number of frames a port can transmit without receiving a receive ready signal from the receiving device.

ber

See bit error rate.

bidirectional

In Fibre Channel, the capability to simultaneously communicate at maximum speeds (100 Mbps) in both directions over a link.

bit error rate

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.

broadcast frames

Data packet, also known as a broadcast packet, whose destination address specifies all computers on a network.

See also multicast.

buffer

Storage area for data in transit. Buffers compensate for differences in processing speeds between devices.

See also BB_Credit.

CHPID

See channel path identifier.

call-home

Product feature which enables the HAFM server to automatically 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 subsystem, 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 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 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, while a hardware product is operating.

configuration data

Configuration data includes: identification data, port configuration data, operating parameters, SNMP configuration, and zoning configuration. A configuration backup file is required to restore configuration data if the CTP card in a non-redundant director is removed and replaced.

connectionless

Non-dedicated link. Typically used to describe a link between nodes which allows the switch to forward Class 2 or Class 3 frames as resources (ports) allow. Contrast this to the dedicated bandwidth that is required in a Class 1 Fibre Channel Service point-to-point link.

connector

See optical fiber connector.

control processor card

Circuit card that contains the director microprocessor. The CTP card also initializes hardware components of the system after power-on. A 10 Mbps RJ-45 twisted pair connector is located on the CTP card to connect to the Ethernet LAN and communicate with the HAFM server or a specific management station.

control unit

A hardware unit that controls the reading, writing, or displaying of data at one or more input/output units.

control unit port

An internal director port on the CTP card that communicates with the attached processor channels to report error conditions and link initialization.

CRC

See cyclic redundancy check.

CTP

See control processor card.

CUP

See control unit port.

cyclic redundancy check

System of error checking performed at both the sending and receiving station using the value of a particular character generated by a cyclic algorithm. When the values generated at each station are identical, data integrity is confirmed.

DASD

Direct access storage device such as a disk drive.

datagram

See Class 3 Fibre Channel service.

default

Pertaining to an attribute, value, or option that is assumed when none is explicitly specified.

default zone

Contains all attached devices that are not members of a separate zone.

destination address

Address identifier that indicates the targeted destination of a data frame.

device

Product, connected to a managed director, that is not controlled directly by the Product Manager.

See also node.

diagnostics

Procedures used by computer users and service personnel to diagnose hardware or software error conditions.

dialog box

Dialog box is a window containing informational messages or data fields to be modified or filled in with desired options.

D_ID

See destination address.

director

An intelligent Fibre Channel switching device providing any-to-any port connectivity between nodes (end devices) on a switched fabric. The director sends data transmissions (data frames) between nodes in accordance with the address information present in the frame headers of those transmissions.

DNS name

Domain name system or domain name service. Host or node name for a device or managed product that is translated to an IP address through a domain name server.

domain ID

Number (1 through 31) that uniquely identifies a switch in a multi-switch fabric. A distinct domain ID is automatically allocated to each switch in the fabric by the principal switch.

E_Port

See expansion port.

E_D_TOV

See error-detect time-out value.

Embedded Web Server

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 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 defines the time the switch waits for an expected response before declaring an error condition.

error message

Indication that an error has been detected.

See also information message and warning message.

Ethernet

A widely implemented local area network (LAN) protocol that uses a bus or star topology and served as the basis for the IEEE 802.3 standard, which specifies the physical and software layers. Baseband LAN allows multiple station access to the transmission medium at will without prior coordination and which avoids or resolves contention.

Ethernet hub

A device used to connect the EFM Server and the directors it manages.

event code

Code that provides the operator with information concerning events.

event log

Record of significant events that have occurred on the director, such as FRU failures, degraded operation, and port problems.

expansion port

Physical interface on a Fibre Channel switch within a fabric, that attaches to an expansion port (E_Port) on another Fibre Channel switch to form a multi-switch fabric.

See also segmented E_Port.

explicit fabric login

Data field size, supported by an F_Port, that is agreed upon during fabric login.

fabric

Entity that interconnects N_Ports and is capable of routing (switching) Fibre Channel frames using the destination ID information in the Fibre Channel frame header accompanying the frames.

fabric element

Any active director or node in a switched fabric.

fabric port

Physical interface within the fabric that connects to an N_Port through a point-to-point full duplex connection.

failover

Automatic and non-disruptive transition of functions from an active FRU that has failed to a backup FRU.

FCC-IOC

See Fibre Channel I/O controller.

FE-MIB

See Fibre Channel fabric element.

fiber

Physical media types supported by the Fibre Channel specification, such as optical fiber, 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 card

Each fiber port module card provides four Fibre Channel connections through duplex small form factor (SFF) pluggable fiber-optic transceivers.

Fibre Channel

Integrated set of standards recognized by ANSI which defines specific protocols for flexible information transfer. Logically, a point-to-point serial data channel, structured for high performance.

Fibre Channel fabric element

Any device linked to a fabric. Information about these devices is recorded in a management information base (MIB) which can be accessed by fabric management software.

Fibre Channel I/O controller

A device that controls the embedded Fibre Channel port and configures the ports' ASICs.

field-replaceable unit

Assembly removed and replaced in its entirety when any one of its components fails.

firmware

Embedded program code that resides and executes on the director.

FPM

See fiber port module card.

F_Port

See fabric 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.xxx.xxx.xxx) that identifies a gateway on the network.

generic port

Also known as G_Port. Physical interface on a director that can function either as a fabric port (F_Port) or an extension port (E_Port) depending on the port type to which it connects.

G_Port

See generic port.

HA-Fabric Manager

A Java-based graphical user interface (GUI) that enables the user to manage users and products, monitor products, and open Product Managers. See also HAFM.

hardware log

Record of FRU insertions and removals in the director.

hardware management console

The console runs the *Hardware Management Console* application (HWMCA), and is the operations and management PC platform for 2/Series servers.

HAFM

See also HA-Fiber Manager.

HBA

See host bus adapter.

high availability

A performance feature characterized by hardware component redundancy (enabling non-disruptive maintenance). High-availability systems maximize system uptime while providing superior reliability, availability, and serviceability.

hop

Data transfer from one node to another node.

homogeneous fabric

A fabric consisting of only HP products.

hop count

The number of hops a unit of information traverses in a fabric.

host bus adapter

Logic card that provides a link between the server and storage subsystem, and that integrates the operating systems and I/O protocols to ensure interoperability.

hot-swapping

Removing and replacing a device's components while the device continues to operate normally.

hub

In Fibre Channel, a device that connects nodes into a logical loop by using a physical star topology.

IML

See initial machine load.

inband management

Management of the director through a Fibre Channel connection to a port card.

information message

Message telling a user that a function is performing normally or has completed normally. *See also* error message and warning message.

initial machine load

Also known as IML. Hardware reset for 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

Process of initializing the device and causing the operating system to start. Initiated through a menu in the Product Manager, this option performs a hardware reset on the active CTP only.

interface

Hardware, software, or both, linking systems, programs, or devices.

Internet protocol address

Unique string of numbers (in the format xxx.xxx.xxx.xxx) that identifies a device on a network.

interoperability

Ability to communicate, execute programs or transfer data between various functional units over a network.

interswitch link

Also known as ISL. Physical E_Port connection between two directors in a fabric.

IOCDs

A data set that contains an I/O configuration definition built by the IOCP.

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 on a switched fabric.

link incident

Interruption to link due to loss of light or other causes.

load balancing

Ability to evenly distribute traffic over multiple interswitch links within a fabric. Load balancing on a director occurs automatically.

logical unit number

Also known as LUN. In Fibre Channel addressing, a logical unit number is a number assigned to a storage device which, in combination with the storage device's node port's world wide name, represents a unique identifier for a logical device on a storage area network.

loopback plug

In a fiber optic environment, a type of duplex connector used to wrap the optical output signal of a device directly to the optical input.

loopback test

Test that checks attachment or control unit circuitry, without checking the mechanism itself, by returning the output of the mechanism as input.

LUN

See logical unit number.

MAC address

See media access control address.

maintenance port

Connector on the 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 HAFM. For example, the Director 2/140 is a managed product.

See also device.

management information base

Related set of software objects (variables) containing information about a managed device and accessed via SNMP from a network management station.

management session

Management session exists when a user logs onto the HAFM server. HAFM can support multiple concurrent management sessions. The user must specify the network address of the Server at logon time.

Media Access Control address

Hardware address of a node (device) connected to a network.

MIB

See management information base.

multicast

Delivery of a single transmission to multiple destination N_Ports. Can be one to many or many to many. All members of the group are identified by one IP address.

multi-switch fabric

Fibre Channel fabric created by linking more than one director or fabric switching device within a fabric.

name server

Program that translates names from one form into another. Domain name servers (DNS) translate domain names into IP addresses.

name server zoning

N_Port access management that allows N_Ports to communicate if and only if they belong to a common name server zone.

network address

Name or address that identifies a managed product on a TCP/IP network. The network address can be either an IP address in dotted-decimal notation containing four three-digit octets in the format xxx.xxx.xxx.xxx), or a domain name (as administered on a customer network).

nickname

Alternate name assigned to a 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

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).

non-disruptive maintenance

Ability to service FRUs (including maintenance, installation, removal and replacement) while normal operations continue without interruption.

See also concurrent maintenance.

N_Port

See node port.

offline sequence

Sequence sent by the transmitting port to indicate that it is attempting to initialize a link and has detected a problem in doing so.

OLS

See offline sequence.

operating state (director)

The 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.

operating state (port)

Valid states include Online, Offline, Testing, Beaconing, Invalid Attachment, Link Incident, No Light, Not Operational, Port Failure, Segmented E_Port.

operating status (director)

The operating status depends on hardware component failures, which are indicated by alert symbols that display in HAFM application views.

Open Systems 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 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 and optical cable.

optical fiber connector

Hardware component that transfers optical power between two optical fibers or bundles and is designed to be repeatedly connected and disconnected.

out-of-band management

Transmission of management information using frequencies or channels other than those routinely used for information transfer.

packet

Logical unit of information (usually in the form of a data frame) transmitted on a network. It contains a header (with all relevant addressing and timing information), the actual data, and a trailer (which contains the error checking function, usually in the form of a cyclic redundancy check).

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.

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.

POST

See power-on self test.

power-on self-test

Series of self-tests executed each time the unit is booted or reset.

preferred domain ID

Domain ID that a switch is assigned by the principal switch in a switched fabric. The preferred domain ID becomes the active domain ID except when configured otherwise by the user.

preventive service planning bucket

Collected problems after early ship of an IBM product.

principal switch

The switch that allocates domain IDs to itself and to all other switches in the fabric. There is always one principal switch in a fabric. If a switch is not connected to any other switches, it acts as its own principal switch.

Product Manager

Application that implements the management user interface for the director.

product name

User-configurable identifier assigned to a managed product. Typically, this name is stored on the product itself. For the director, the product name can also be accessed by an SNMP manager as the system name.

PSP bucket

See preventive service planning bucket.

R_A_TOV

See resource allocation time-out value.

redundancy

Performance characteristic of a system or product whose integral components are backed up by identical components to which operations will automatically failover in the event of a component failure. Redundancy is a vital characteristic of virtually all high-availability (24 hr/7 days per week) computer systems and networks.

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, running HAFM Software that can access the HAFM server over a LAN connection.

resource allocation time-out value

R_A_TOV is a value used to time out operations that depend on the maximum possible time that a frame could be delayed in a fabric and still be delivered.

SAN

See storage area network.

SBAR

See serial crossbar assembly.

SC

Subscriber connectors.

segmented E_Port

E_Port that has ceased to function as an E_Port within a multi-switch fabric due to an incompatibility between the fabrics that it joins.

See also expansion port.

SEL

System error light.

serial crossbar assembly

The serial crossbar assembly (SBAR) is responsible for Fibre Channel frame transmission from any director port to any other director port. Connections are established without software intervention.

SNMP

Simple network management protocol. Specifies a mechanism for network management that is complete, yet simple. Information is exchanged between agents, which are the devices on the network being managed, and managers, which are the devices on the network through which the management is done.

SNMP community

Also known as SNMP community string. SNMP community is a cluster of managed products (in SNMP terminology, hosts) to which the server or managed product running the SNMP agent belongs.

SNMP community name

The name assigned to a given SNMP community. Queries from an SNMP management station to a device running an SNMP agent will only elicit a response if those queries are addressed with the correct SNMP community name.

SSP

See system services processor.

storage area network

A high-performance data communications environment that interconnects computing and storage resources so that the resources can be effectively shared and consolidated.

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 services processor

Controls the RS-232 maintenance port, the Ethernet port, and the operator panel of a Fibre Channel director.

topology

Logical and/or physical arrangement of stations on a network.

trap

Unsolicited notification of an event originating from a SNMP managed device and directed to an SNMP network management station.

trap host

SNMP management workstation that is configured to receive traps.

trunk cable

Cable consisting of multiple fiber pairs that do not directly attach to an active device. This cable usually exists between distribution panels.

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 assuming that this is supported by the current zoning configuration.

unicast

Communication between a single sender and a single receiver over a network. Compare to *multicast* and *anycast* (communication between any sender and the nearest of a group of receivers).

universal port module card

Each universal port module (UPM) card provides four Fibre Channel connections through duplex small form factor (SFF) pluggable fiber-optic transceivers. UPM cards allow 1 Gb/sec and 2 Gb/sec operation.

vital product data

System-level data stored by the backplane in the electrically erasable programmable read-only memory. This data includes serial numbers and identifies the manufacturer.

UPM card

See universal port module card.

VPD

See vital product data.

warning message

Indication that a possible error has been detected.

See also error message and information message.

wrap plug

See loopback plug.

world wide name

Eight byte address that uniquely identifies a switch, or a node (end device), even on global networks.

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

A

AC module 1-14

AC system harness 1-14

active=saved 2-49

AIX operating system 2-64

alerts, introduction 1-4

allen wrench, caution 1-15

asynchronous RS-232

 null modem cable 1-16

audience xi

B

backing up director configuration file 4-9

beaconing

 LED 1-9

beaconing, introduction 1-5

C

cables, FCC compliance statement A-3

call-home feature

 introduction 1-5

call-home feature, configuring 2-38

Canadian Notice (Avis Canadien) A-4

CE marking A-4

CFR, laser compliance 1-10

changing the director's IP address 2-10

class 1 laser transceivers 1-10

clear system error light function 1-9

clock speed, processor 2-64

Code of Federal Regulations 1-10

code pages 2-50

COMn properties dialog box 2-12

components of the director 2/140 1-8

configuration data, backing up 2-47

configure director network information 2-9

configure fabric parameters dialog box 2-31,
3-11

configure feature key

 dialog box 2-24

 procedure 2-23

configure FICON management server dialog box
2-51

configure menu

 switch binding 2-56

configure menu, enable Embedded Web Server
2-48

configure menu, enable EWS 2-48

configure menu, enable telnet 2-48

configure open systems management server
dialog box 2-52

configure switch parameters dialog box 2-27

configuring

 fabric operating parameters 2-31, 3-11

configuring, call-home feature 2-38

connecting the director to the LAN segment 2-15

connectivity failures, causes of 1-7

conventions, document xii

CTP2 cards, description 1-12

D

data collection 1-5

declaration of conformity A-3

default IP address 2-10

defaults

 code page 2-50

 switch priority setting 2-33, 3-14

degraded fabric performance, causes of 1-7
diagnostic software, introduction 1-4
dialog boxes
 configure fabric parameters 2-31, 3-11
 configure feature key 2-24
 configure FICON management server 2-51
 configure open systems management server 2-52
 configure switch parameters 2-27
 switch binding membership list 2-56
director
 AC module 1-14
 desktop, installing 2-7
 e_d_tov 1-7
 Fibre Channel addresses 2-29, 3-9
 firmware 4-2
 general description 1-1
 management, overview 1-3
 NV-RAM 2-27, 2-31, 3-11
 r_a_tov 1-7
 tools supplied 1-15
 unpacking, inspecting, installing 2-6
 weight
 caution 2-7
 weight, caution 2-7
director 2/140
 hardware components 1-8
 optional kits 1-17
director 2/140 firmware library dialog box 4-1
director firmware
 adding version 4-2
 deleting a version 4-6
 downloading 4-6
 version 4-1
document conventions xii
documentation, related xi
domain ID 1-7
 insistent 2-29, 3-9
 preferred 2-29, 3-9
domain RSCNs 2-30, 3-10
 enterprise fabric mode 2-60
downloading firmware 4-6

E

e_d_tov 2-32, 3-13
 fabric segmentation 2-32, 3-13
 incompatible parameters 1-7
 less than r_a_tov 2-32, 3-13
 multiswitch fabrics 2-32, 3-13
 rerouting delay 2-30, 3-10
E_port segmentation
 preferred domain ID 2-29, 3-9
e_port segmentation 1-7
 causes of 1-7
e_ports 1-10
EBCDIC code pages 2-50
electrostatic discharge precautions C-1
e-mail notification
 introduction 1-5
Embedded Web Server (EWS) 3-1
Embedded Web Server, enabling 2-48
enable Embedded Web Server 2-48
enable EWS 2-48
enable management server (FICON) 2-49
enable telnet 2-48
enterprise fabric mode 2-59, 2-60
equipment symbols xiii
ESD
 wrist strap 1-17
Ethernet
 hub
 unpacking, inspecting, and installing 2-63
ethernet network adapter 2-64
European Union notice A-4
EWS 3-1
 launching 3-1
 use to configure director ports 3-3
 use to configure network information 3-15
 use to configure SNMP trap messages 3-17
 use to configure user rights 3-19
 use to set date and time 3-5
 use to set director identification 3-4
 use to set operating parameters 3-6
EWS, enabling 2-48

F

f_ports 1–10
fabric binding 2–53
 enterprise fabric mode 2–59
fabric parameters
 e_d_tov 2–32, 3–13
 interop mode 2–33, 3–14
 r_a_tov 2–32, 3–13
 switch priority 2–33, 3–13
fabric segmentation
 e_d_tov 2–32, 3–13
 preferred domain ID 2–29, 3–9
failover, SBAR assembly 1–14
FC fabric element MIB, version 1–5
FCC
 class A compliance notice A–2
 class B compliance notice A–2
FCC compliance statement, cables A–3
feature
 SANtegrity 2–53
feature key 2–24
features of the director 2/140 1–8
Federal Communications Commission (FCC)
 notice A–2
fiber-optic
 cleaning kit 1–17
 protective plug 1–15
Fibre Alliance MIB 1–5
Fibre Channel addresses 2–29, 3–9
Fibre Channel ports
 connecting cables 2–61
FICON management server 2–30, 2–48
 active=saved 2–49
 code page 2–50
 configuring 2–49, 2–51
 enable management server 2–49
 host control 2–49
 installing 2–49
 programmed offline state control 2–49
firmware
 deleting version 4–6
 determining version 4–1

 modifying description 4–5
 release notes 4–2
firmware library 4–1
frames
 routing of 2–30, 3–10
FRUs
 AC module 1–14
FRUs, CTP2 card 1–12

G

g_ports 1–10
 UPM card 1–10
getting help xiv
grounding methods C–1

H

HA PA-RISC processor 2–64
HAFM
 configuring ports 2–34
 configuring SNMP trap message recipients
 2–35
 enabling e-mail notification 2–37
 enabling to manage the director 2–17
 remote location 2–64
 remote location requirements 2–64
 setting offline 2–25
 setting the director online 2–25
HAFM server
 Fibre Alliance MIB 1–5
 recording and verifying restoration
 information 2–17
hard drives, remote workstation 2–64
help, obtaining xiv
Hewlett-Packard
 authorized reseller xv
 technical support xiv
 website xv
hexagonal adapter 1–15
hop counts 2–30, 3–10
host control 2–49
host control prohibited field 2–51, 2–52
HP-UX operating system 2–64
HyperTerminal 1–17, 2–13

I

- inband switch management 2–30
- input filter 1–14
- insistent domain ID 2–29, 3–9
 - enterprise fabric mode 2–61
- installation options 2–4
 - customer-supplied equipment rack 2–4
 - table or desk top 2–4
- Installation Task Summary (table) 2–1
- installation tasks
 - backing-up configuration data 2–47
 - call-home feature, configuring 2–38
 - director
 - unpacking, inspecting, installing 2–6
 - recording and verifying HAFM Server restoration information 2–17
 - summary 2–1
 - unpacking, inspecting, and installing
 - Ethernet hub 2–63
- Intel Pentium processor 2–64
- Internet Explorer 2–64
- interop mode 2–33, 3–14
- interswitch link, g_port 1–10
- IP address 2–9
- ISL, g_port 1–10

L

- languages, code page 2–50
- laser
 - devices A–6
 - information A–8
- laser transceivers 1–10
- LEDs
 - beaconing 1–9
 - power supplies 1–10
 - SBAR assembly 1–14
 - system error 1–9
 - UPM card 1–11
- Linux operating system, version 2–64
- logic card, torque tool, caution 1–15
- logs, introduction 1–4
- long-wave laser transceivers 1–11

- loopback plug
 - multimode 1–15
 - singlemode 1–15

M

- MAC address 2–9
- maintenance port 1–5, 1–14
- management server
 - FICON 2–48
 - configuring 2–49
 - installing 2–49
 - open systems 2–52
 - installing 2–52
- managing
 - director 1–3
- memory, remote workstation 2–64
- MIBs 1–5
- Microsoft Internet Explorer 2–64
- mode
 - enterprise fabric 2–59
 - interop 2–33, 3–14
 - open fabric 1.0 2–34, 3–14
 - open systems 2–31
 - operating 2–30
 - S/390 2–30
- multi-mode fiber-optic cables 1–11
- multiswitch fabric 1–6
 - connectivity failures, causes of 1–7
 - degraded performance, causes of 1–7
 - domain IDs 1–7
 - e_d_tov 2–32, 3–13
 - e_port segmentation
 - causes of 1–7
 - principal switch 2–33, 3–13
 - zoning 1–7
- multiswitch fabric, e_ports 1–10

N

- n_ports 1–10
- Netscape Navigator 2–64
- network addresses
 - changing 2–10
 - default settings 2–9

gateway 2-10
 IP address 2-9
 MAC address 2-9
 subnet mask 2-10
 null modem cable 1-16
 NV-RAM 2-27, 2-31, 3-11
O
 OFC class 1 laser transceivers 1-10
 online state, setting 2-25
 open fabric 1.0 2-34, 3-14
 open systems management server 2-52
 configuring 2-52
 installing 2-52
 open systems mode 2-30, 2-31
 operating mode 2-30
 optional features 2-48
 FICON management server 2-48
 open systems management server 2-48
 SANtegrity feature 2-53
 optional kits
 8-port module kit 1-17
 combination long-wave/short-wave port
 module kit 1-18
 short-wave port module kits 1-17
P
 port loopback diagnostic tests, fiber-optic
 loopback plug 1-15
 POST 2-9
 power supplies 1-10
 power supply requirements B-2
 power switch 1-14
 POWER3 microprocessor 2-64
 power-on self test 2-9
 PowerPC microprocessor 2-64
 precautions against electrostatic discharge C-1
 preferred domain ID 2-29, 3-9
 multiswitch fabric 2-28, 3-8
 principal switch, determining 2-33, 3-13
 ProComm Plus 1-17
 product manager
 non-English language support 2-50

SNMP agent 1-3
 programmed offline state control 2-49
 protective plug 1-15

R

r_a_tov 2-32, 3-13
 greater than e_d_tov 2-32, 3-13
 incompatible parameters 1-7
 rack stability, warning xiv
 Regulatory Compliance identification numbers
 A-1
 regulatory compliance notices A-1
 related documentation xi
 release notes 4-2
 rerouting delay
 enterprise fabric mode 2-60
 RFC 1213
 definition 1-5

S

S/390 mode 2-30
 FICON management server 2-30
 safety
 ESD grounding cable with wrist strap 1-17
 fiber-optic protective plug 1-15
 SANtegrity feature 2-53
 fabric binding 2-53
 SANtegrity features
 switch binding 2-54
 SBAR assembly 1-14
 segmentation
 causes of 1-7
 serviceability features 1-4
 set director date and time manually 2-21
 setting, online state 2-25
 shortwave laser transceivers 1-11
 single-mode fiber-optic cables 1-11
 site plan 2-4
 SNMP agent
 general description 1-3
 SNMP trap messages
 maximum recipients 1-5
 Solaris operating system 2-64

- summary of installation tasks 2-1
- SunOS operating system 2-64
- switch
 - error-detection, reporting, and serviceability features 1-4
 - multiswitch fabric 1-6
- switch binding 2-54, 2-60
 - configuring 2-23
 - membership list 2-56
 - online state functions 2-58
 - zoning function 2-59
- switch binding membership list dialog box 2-56
- switch clock alert mode 2-49
- switch clock alert mode field 2-51
- switch parameters
 - domain RSCNs 2-30, 3-10
 - insistent domain ID 2-29, 3-9
 - NV-RAM storage 2-27, 2-31, 3-11
 - operating mode 2-30
 - preferred domain ID 2-29, 3-9
- switch priority 2-33, 3-13
 - related number codes 2-33, 3-14
- switch priority setting 2-33, 3-14
- switches, principal, determining 2-33, 3-13
- symbols on equipment xiii
- synchronize date and time 2-22
- system error LED 1-9

T

- TCP/IP MIB-II
 - definition 1-5
- technical specifications, power requirements B-2
- technical support, Hewlett-Packard xiv
- telnet, enabling 2-48
- tools
 - supplied by service personnel 1-16
 - supplied with director 1-15
- torque tool 1-15
 - caution 1-15
- trap messages
 - maximum recipients 1-5

U

- UltraSPARC-II processor 2-64
- United States/Canada 00037 code page 2-50
- UNIX workstation, specifications 2-64
- UPM cards 1-10

V

- versions
 - AIX operating system 2-64
 - Director 2/140 firmware 1-3
 - FC fabric element MIB 1-5
 - firmware
 - deleting 4-6
 - determining 4-1
 - modifying description 4-5
 - HP-UX operating system 2-64
 - Internet Explorer 2-64
 - Linux operating system 2-64
 - Netscape Navigator 2-64
 - Solaris operating system 2-64
 - SunOS operating system 2-64
 - Windows operating systems 1-17, 2-64
- video card, remote workstation 2-64
- voltage
 - AC power connectors 1-14
 - voltage, AC power connectors 1-14

W

- warning, rack stability xiv
- web server, overview 1-3
- websites
 - Hewlett-Packard xiv
 - Hewlett-Packard locations and phone numbers xv
 - Hewlett-Packard storage xv
 - Hewlett-Packard support xiv
- weight, director
 - caution 2-7
- Windows operating systems, versions 1-17, 2-64
- workstation, UNIX 2-64
- WWN

principal switch 2-33, 3-13

Z

zone set, description of 1-6

zoning

joining, rules of 1-7

