hp StorageWorks

embedded web server user guide

Part Number: AA–RTDRA–TE

First Edition (January 2003)

This guide describes the HP StorageWorks Embedded Web Server (EWS), its features, and how to use it to configure, operate, and monitor a Storage Area Network (SAN).

Printed in the U.S.A.

embedded web server user guide
First Edition (January 2003)
Part Number: AA–RTDRA–TE

Contents

2 Configuring the Product

3 Configuring Zones

4 Viewing Product and Fabric Data

5 Monitoring Products

6 Operating and Managing Products and Parts

A Error Messages

Glossary

Index

Figures

Tables

About this Guide

This publication is part of a document suite that supports the Hewlett-Packard (HP) StorageWorks Director 2/64, Director 2/140, Edge Switch 2/16, Edge Switch 2/32, Edge Switch 2/24, and the *Embedded Web Server (EWS)* application.

Intended Audience

This book is intended for use by data center administrators, LAN administrators, operations personnel, and customer support personnel who administer user access to this application and monitor and manage product operation.

Related Documentation

For a list of corresponding documentation, see the Related Documents section of the Release Notes that came with the product.

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

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

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

Document Conventions

The conventions included in Table 1 apply.

Table 1: Document Conventions

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

Symbols in Text

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

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

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

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

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

Symbols on Equipment

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

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

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

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

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

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

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

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

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

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

Rack Stability

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

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

Getting Help

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

HP Technical Support

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

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

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

Be sure to have the following information available before calling:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Applicable error messages
- Operating system type and revision level
- Detailed, specific questions.

HP Website

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

HP Authorized Reseller

For the name of your nearest HP Authorized Reseller:

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

1

Introduction

Overview

The Embedded Web Server (EWS) is a web-based graphical user interface (GUI), based on HTML, that enables the user to administer products, monitor products and ports, and perform tasks to manage a simple Storage Area Network (SAN). You can also use EWS to perform troubleshooting tasks and upgrade product firmware.

With product firmware 04.00.00 (or later) installed, administrators or operators with a browser-capable PC and an Internet connection can monitor and manage the product through the EWS interface.

The EWS interface supports product configuration, statistics monitoring, and basic operation. The EWS interface neither replaces nor offers all of the management capability of the High Availability Fabric Manager (HAFM) and its Product Manager applications (for example, the EWS interface does not support all product maintenance functions).

In addition, EWS provides hyperlink access to other products in a fabric, which means those products can also be managed.

Using EWS to Perform Tasks

Users can perform the following tasks using EWS:

- Display the properties and operational status of the product, FRUs, and Fibre Channel ports; display product operating parameters; and display fabric parameters.
- Configure the Director or Edge Switch, including:
  - — Fibre Channel port parameters, port types, and data transmission speeds.
  - — Product identification, date and time, operating domain parameters, fabric parameters, and network addresses.

  - — Parameters for product management through Simple Network Management Protocol (SNMP), the Command Line Interface (CLI), the Open System Management Server (OSMS) feature, or the Fibre Connection (FICON) management server (FMS) feature.

NOTE: The Edge Switch 2/24 does not support out-of-band management through FMS. However, the Edge Switch 2/24 does support transmission of FICON frames.

  - — Zones and zone sets.
  - — User rights (administrator and operator).
- Monitor ports and port statistics, and display the event log and node list.
- Perform product operations and maintenance tasks, including:
  - — Enable unit beaconing, set the product online or offline, and perform a configuration reset.
  - — Enable port beaconing, perform port diagnostics, and reset ports.
  - — Retrieve dump files and retrieve product information files.
  - — Install optional feature keys.
  - — Configure product Internet Protocol (IP) addresses, names, and SNMP settings.
  - — Install new versions of product firmware.
  - — Manage user access to features.
  - — Control product ports on an individual basis.
  - — Troubleshoot problems using event log and error status indicators. Administrators and operators can access real-time information about the product and fabric.

The EWS interface can be opened from a standard web browser running Netscape Navigator 4.6 or higher or Microsoft Internet Explorer 4.0 or higher. At the web browser, the user enters the IP address of the product as the Internet uniform resource locator (URL). When prompted at a login screen, the user enters a user name and password.

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

Viewing the User Interface

When the EWS interface opens, the default display is the **View** page. Figure 1–1 shows an example EWS view with labels for the various parts of the image. This example shows the **Configure > Switch > Identification** screen for the Edge Switch 2/24. For other products, the corresponding page looks very similar.

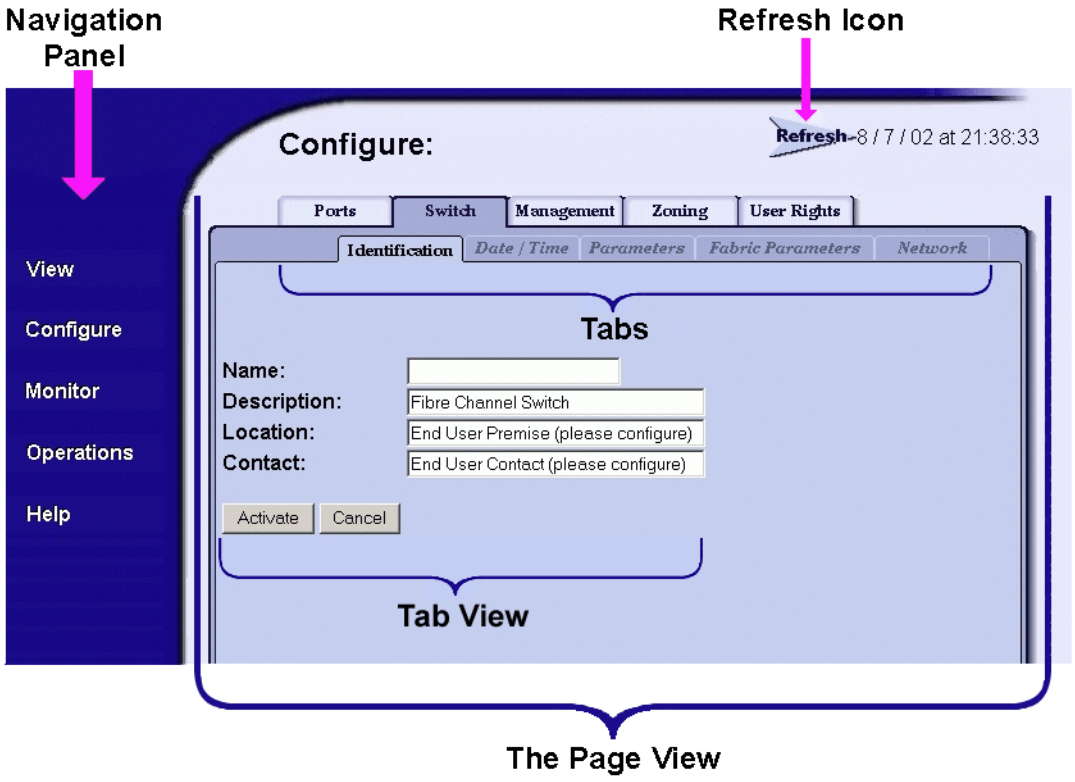

Figure 1–1: Example Embedded Web Server page for Edge Switch 2/24

As shown in Figure 1–1, particular terms are used when describing the EWS interface:

- **Navigation panel** — at the left of the screen is a menu of the various primary views available on the screen. The navigation panel options include:
  - **View** — At the **View** page, the **Director** or **Switch** (default), **Port Properties**, **FRU Properties**, **Unit Properties**, **Operating Parameters**, and **Fabric** task selection tabs display.

  - — **Configure** — At the **Configure** page, the **Ports** (default), **Director** or **Switch**, **Management**, **Zoning**, and **User Rights** task selection tabs display.
  - — **Monitor** — At the **Monitor** page, the **Port List** (default), **Port Stats**, **Log**, and **Node List** task selection tabs display.
  - — **Operations** — At the **Operations** page, the **Director** or **Switch** (default), **Port**, **Maintenance**, and **Feature Installation** task selection tabs display.
  - — **Help** — The **Help** option opens online user documentation that supports the EWS interface. This manual supplements the online help that is included with the EWS interface.

- **Page** — describes the entire screen except the navigation panel. When you choose an item from the navigation panel, the corresponding page view displays. For example, choose **Configure** from the navigation panel to view the **Configure** page.
- **Tab** — describes a label for a viewing option on a page, such as the **Switch** and **Identification** tabs shown in Figure 1–1. Task selection tabs display at the top of the page. The task selection tabs allow users to perform Director- or Switch-specific tasks.
- **Tab view** — describes the information that displays when you choose a tab.
- **Refresh icon** — a button in the top right of the screen. Click the button to refresh the tab view with current information.

Benefits

The EWS interface provides the following benefits:

- Enables a single product to be managed from a single point of access.
- Allows an administrator to manage a product from any location (such as their office, a raised floor area, or a conference room) within the company's public/private networks.
- Enables an administrator to view the most current information about a product upon accessing the product.

  (This easy access provides a single point of product administration that is not limited to the location of an application or special hardware.)

- Protects the authorized rights of users to perform tasks through roles defined as operators and administrators.

  (This protection enables companies to decide who should perform everyday tasks, such as monitoring product status, and sensitive tasks, such as installing firmware updates. This flexible approach enables companies to define roles within their organization while providing a level of security against unauthorized access.)

- Enables users to simply start a web browser, enter the network address of the product, and log in to start using EWS.

  (No additional installation is required. EWS is ready and available to perform administration tasks once the hardware is installed and connected to the Ethernet network.)

- Allows users to utilize a familiar web browser-based graphical user interface that uses standard web browser applications for access.
- Allows users to obtain assistance in performing tasks through online help.

Key Terms

This section provides key terms that will help you perform tasks, especially tasks such as zoning.

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.

Storage Area Network (SAN)

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

Zone (Zoning)

A zone is a group of devices or zone members in a SAN that can communicate and access each other. Communication is only allowed between devices in the same zone. A device can be in multiple zones so that shared resources can be accessed by many devices. Because SANs connect many types of devices that may carry different protocols, separating an entire fabric into zones can control access between specific devices. Zone (or zoning) is an efficient method of managing, partitioning, and controlling access to SAN devices. Zoning maximizes resources while maintaining data security and enabling heterogeneous systems and products to operate in the same SAN.

Zone Member

Specification (definition) of a device that belongs to a zone. A zone member can be identified by the port number of the device to which it is attached or by its device or host bus adapter or World Wide Name (WWN). In multiswitch fabrics, identification of end-devices and nodes by WWN is preferable.

Zone Set

A zone set is composed of one or more zones. When a zone set is activated, all zones in the set are activated at the same time. Only one zone set can be active in the fabric at one time, and that zone set is referred to as the active zone set.

Suggested Reading

A book that can help you to prepare to install products and configure a SAN is the *hp StorageWorks SAN high availability planning guide (620-000124/AA-RS2DB-TE).* You can obtain this book from the Hewlett-Packard website ((http://thenew.hp.com) or from the CD shipped with the Hewlett-Packard product you purchased.

Another publication you may want to read is *Compaq StorageWorks SAN Switch Zoning Reference Guide*, which is a white paper on zoning fundamentals. It is available online from the Hewlett-Packard website ((http://thenew.hp.com).

Where to Start

Depending upon whether the Hewlett-Packard product you purchased has already been installed, you may need to go to a specific chapter. If the product has not been installed, you should start at Chapter 2, Configuring the Product.

If the product was installed, then many of the configuration tasks were probably already completed. In that case, you may need to configure a zone. Configuring (including adding, deleting, and changing) zones is described in Chapter 3, Configuring Zones.

If the products have been configured and you have a functioning SAN, then you most likely will be interested in performing system administration tasks. Those tasks are described in Chapter 4, Viewing Product and Fabric Data; Chapter 5, Monitoring Products; and Chapter 6, Operating and Managing Products and Parts.

If you need to perform troubleshooting, then you will want to review Chapter 5, Monitoring Products, and Chapter 6, Operating and Managing Products and Parts.

Starting EWS

Open the EWS interface as follows:

1. Ensure the workstation (or device you use to launch the web browser) and the Ethernet LAN segment containing the product, such as Edge Switch 2/24, are attached and connected through the Internet.

NOTE: You must be able to make a connection between the web browser and the product in order to login to the product.

2. Launch the web browser application (such as Netscape Navigator, version 4.6 or higher, or Microsoft Internet Explorer, version 4.0 or higher).
3. At the web browser, enter the IP address of the product as the Internet uniform resource locator (URL) such as `http://10.1.1.11`.

NOTE: If the product has not been installed, refer to the product's installation and service manual for the appropriate IP address, login ID, and password that is initially used when you install and configure the product.

4. After a connection is made between the web browser and the product, the **Enter Network Password** dialog box displays as shown in Figure 1–2.

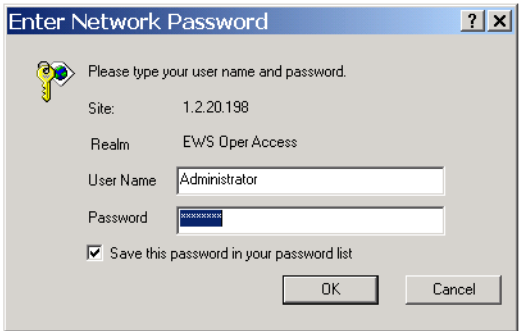

Figure 1–2: Enter Network Password dialog box

5. Type the user name and password.

NOTE: The default user name is available from the installation and service guide that was shipped with the product. The user name and password are case-sensitive. Also, during installation, the default values may have been changed. If defaults have changed, contact your system administrator for the valid user names and passwords.

6. Click **mode**. The EWS interface opens with the **View** page displayed as shown in Figure 1–1 on page 1-3.

2

Configuring the Product

This chapter describes how to configure an HP product using the EWS interface. These procedures can be used to configure a product after installation and as changes are needed. You can use the tabs of the **Configure** page to configure the following aspects of a Director or Edge Switch:

Factory Default Values

HP products on a SAN have preset, default configuration values that were set in the factory. The items that have factory-set default values are:

- Passwords (customer and maintenance-level)
- Internet Protocol (IP) address
- Subnet mask
- Gateway address

The specific default values associated with a particular HP product are documented in the installation and service manual for the product.

Configuring Ports

Perform procedures in this section to configure names and operating characteristics for Fibre Channel ports. To configure one or more ports:

1. If you are going to change the **Speed** parameter on an Director 2/64, set the product offline as follows:
   a. Choose **Operations** from the navigation panel. The **Operations** page displays.
   b. Click the **Online State** tab, then click **Set Offline**. The message `Your operations changes have been successfully activated` displays.
2. At the EWS screen, choose **Configure** from the navigation panel. The **Configure** page and the **Ports** tab view display (Figure 2–1 on page 2-3).

NOTE: Because the Director 2/140 has many ports, the listing of ports is divided into separate displays, which are accessed by clicking the hyperlinks **1-31**, **32-63**, **64-95**, **96-127**, and **132-143**. If you make any changes to a particular list of ports, click **Activate** before selecting another list of ports. If you do not click **Activate**, changes are not implemented on the Director.

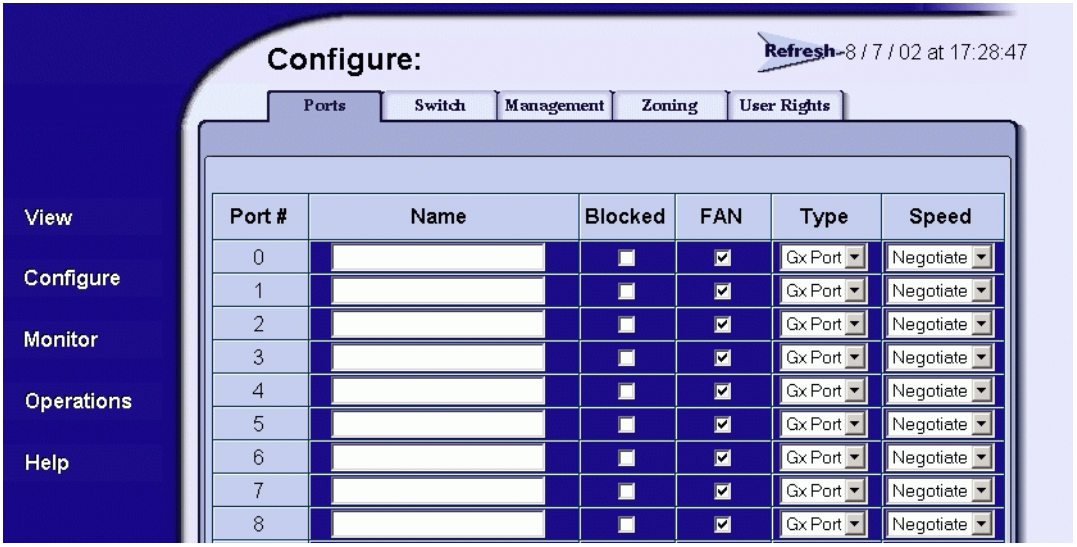

Figure 2–1: Configure Ports tab view

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

NOTE: When naming ports, you may want to name each port based on the device attached to the port. For example, if the port is attached to an e-mail server, you might name the port `email1 server port 2`. The important point is to relate the name of the port to the device that is attached to the port. If you have an installation with many products, you can have a large number of ports. Thus, it is helpful to give each port a name that you relate to the device connected to the port, which can help in isolating problems.

b. Click a check box in the **Blocked** column to block or unblock a port (default is unblocked). A check mark in the box indicates a port is blocked. Blocking a port prevents the attached devices or HP products in the fabric from communicating. A blocked port continuously transmits the offline sequence (OLS).

c. Click the check box in the **FAN** column to enable or disable the fabric address notification (FAN) feature (default is enabled). (The **FAN** column is available only on the Edge Switch 2/24.) A check mark in the box indicates FAN is enabled. When the feature is enabled, the port transmits a FAN frame after loop initialization to verify that Fibre Channel Arbitrated Loop (FC-AL) devices are still logged in. It is recommended this option be enabled for ports configured for loop operation.

d. Click a check box in the **10-100 km** column to define extended distance buffering. (This column is not available on the Edge Switch 2/24.) A check mark in the box indicates extended distance buffering is enabled. You can enable extended distance for a port even if it is not an extended distance port. However, enabling extended distance buffering for a port disables the ability of the port to send broadcast traffic. When you choose this option, the port can support up to 60 buffer-to-buffer credits (BB_Credits) to handle link distances up to 100 km. This enables the port to process 2K frames from attached devices. If this option is not enabled, the port uses the BB_Credit value.

NOTE: If a device is connected and logged in to the fabric when extended distance is enabled or disabled on the corresponding port, the HP product sends OLS for 5 milliseconds to force the device to log in again and obtain the new BB_Credit value set for the port.

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

— **G_Port** — Generic port.

— **F_Port** — Fabric port.

— **E_Port** — Expansion port.

— **GX_Port** — Generic mixed port. Use this selection to configure a port as a generic loop port (GL_Port). The port automatically negotiates any connection type (Edge Switch 2/24 only).

— **FX_Port** — Fabric mixed port. Use this selection to configure a port as a fabric loop port (FL_Port). The port automatically negotiates F_Port and FL_Port connections only (Edge Switch 2/24 only).

f. Choose from the drop-down list in the **Speed** column to configure the port transmission rate. Available selections are:

— **Negotiate** — Auto-negotiate between 1.0625 and 2.125 gigabits per second (Gbps) operation. This is valid only on products that are capable of 2 Gb/sec operation.

— **1 Gb/sec** — 1.0625 Gbps operation.

— **2 Gb/sec** — 2.125 Gbps operation.

3. Click **Activate** to save and activate the changes. The message `Your changes to the port configuration have been successfully activated` displays.

4. If the product is offline, set the product online as follows:
   a. Choose **Operations** from the navigation panel. The **Operations** page displays.
   b. Click the **Online State** tab, then click **Set Online**. The message `Your operations changes have been successfully activated` displays.

Configuring Product Identification

Perform this procedure to configure the HP product's name, description, location, and contact person. The **Name**, **Location**, and **Contact** variables configured here correspond respectively to the SNMP variables **sysName**, **sysLocation**, and **sysContact**. These variables are used by SNMP management workstations when obtaining data from managed Edge Switches or Directors. To configure identification:

1. Choose **Configure** from the navigation panel. Choose the **Switch** or **Director** tab, as appropriate. The **Switch** or **Director** tab displays with the **Identification** tab view (Figure 2–2).

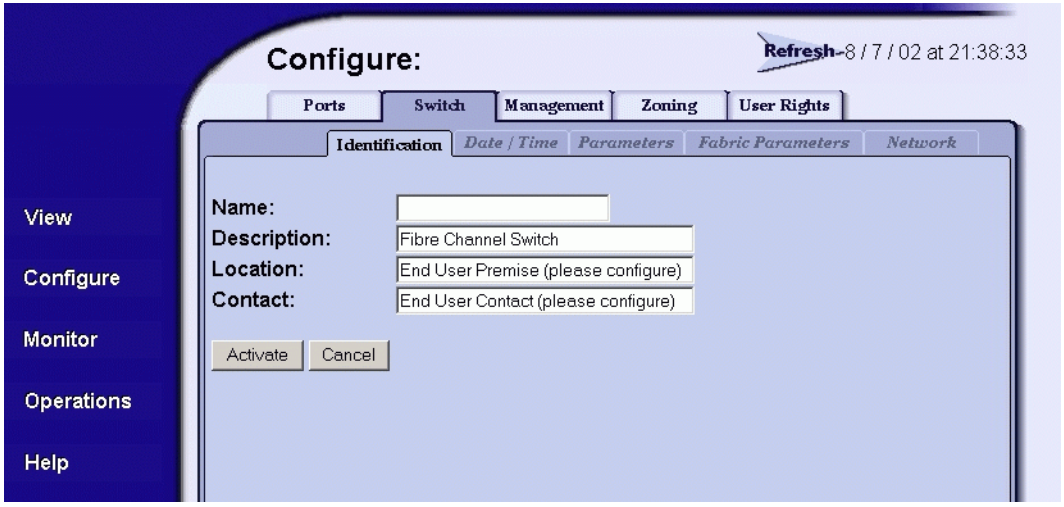

Figure 2–2: Configure product Identification tab view

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

If the product is installed on a public LAN, it is recommended that the name reflect the product's Ethernet network domain name system (DNS) host name. For example, if the DNS host name is `edgeswitch224.hp.com`, the name entered in this dialog box should be `edgeswitch224`.

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

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

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

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

Configuring Date and Time

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

1. Choose **Configure** from the navigation panel. Choose the **Switch** or **Director** tab, as appropriate. Click the **Date/Time** tab to display the **Date/Time** tab view (Figure 2–3 on page 2-7).

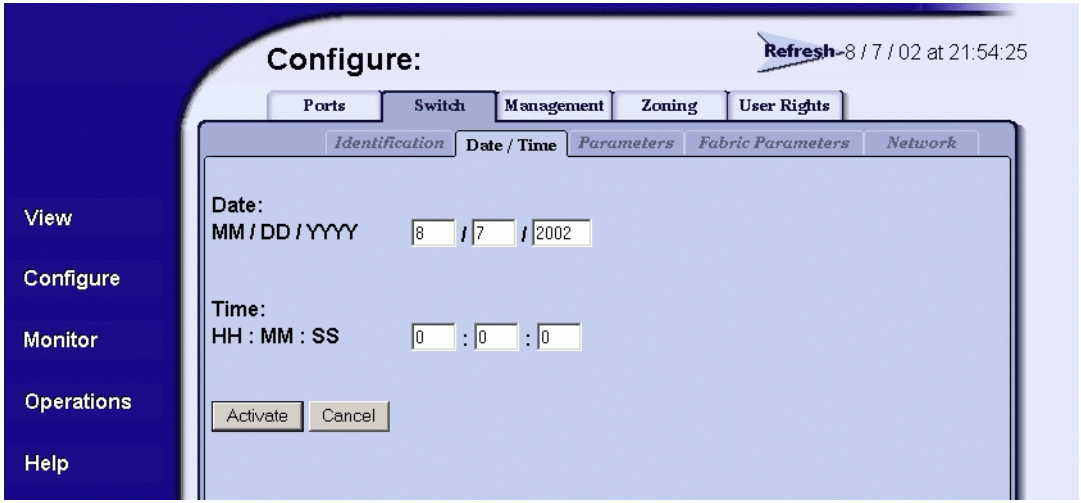

Figure 2–3: Configure date and time tab view

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

   — Month (**MM**): **1** through **12**.

   — Day (**DD**): **1** through **31**.

   — Year (**YYYY**): greater than **1980**.

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

   — Hour (**HH**): **0** through **23**.

   — Minute (**MM**): **0** through **59**.

   — Second (**SS**): **0** through **59**.

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

Configuring Operating Parameters

Perform this procedure to configure the product's preferred domain ID, insistent domain ID, rerouting delay, and domain registered state change notifications (RSCNs). The product must be set offline to configure the preferred domain ID. To configure parameters:

1. Set the product offline as follows:
   a. Choose **Operations** from the navigation panel. The **Operations** page displays.
   b. Click the **Online State** tab, then click **Set Offline**. The message `Your operations changes have been successfully activated` displays.
2. Choose **Configure** from the navigation panel. The **Configure** page displays.
3. Click the **Switch** or **Director** tab, as appropriate. Click the **Parameters** tab to display the **Parameters** tab view (Figure 2–4).

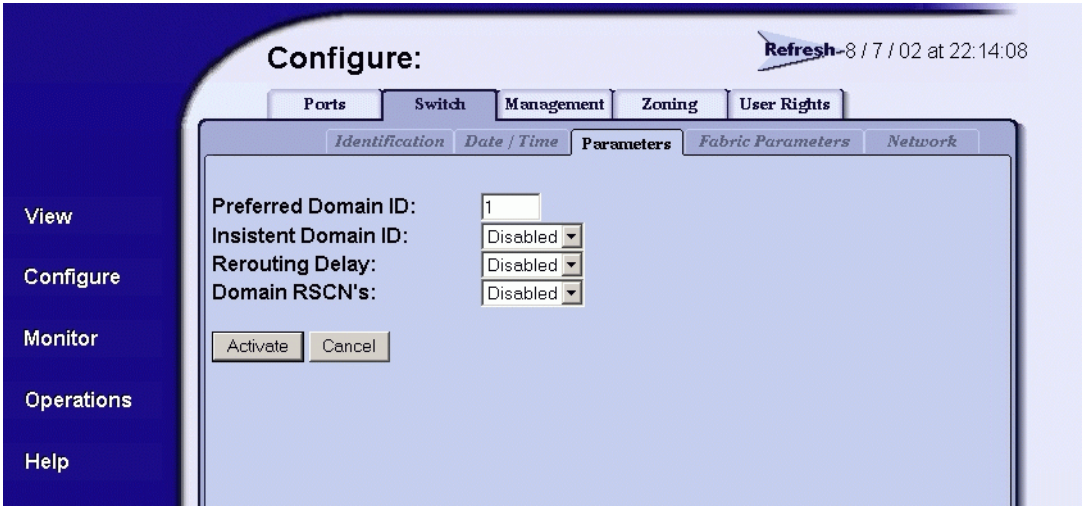

Figure 2–4: Configure product parameters tab view

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

NOTE: If the product is attached to a fabric element, the product and element must have unique domain IDs. If the values are not unique, the E_Port connection to the element cannot carry traffic and the product cannot communicate with the fabric.

b. At the **Insistent Domain ID** field, choose **Enabled** or **Disabled**. When this parameter is enabled, the domain ID configured in the **Preferred Domain ID** field becomes the active domain identification when the fabric initializes.

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

d. At the **Domain RSCNs** field, choose **Enabled** or **Disabled**. When this parameter is enabled, messages can be sent between end devices in a fabric to provide additional connection information to host bus adapters (HBA) and storage devices.

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

5. If fabric parameters require configuration, go to Configuring Fabric Parameters on page 2-9. If the configuration is complete, set the product online as follows:

   a. Choose **Operations** from the navigation panel. The **Operations** page displays.

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

Configuring Fabric Parameters

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

1. If product is online, set the product offline as follows:

   a. Choose **Operations** from the navigation panel. The **Operations** page displays.

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

2. Choose **Configure** from the navigation panel.
3. Click the **Switch** or **Director** tab (as appropriate), then click the **Fabric Parameters** tab. The **Fabric Parameters** tab view displays (Figure 2–5).

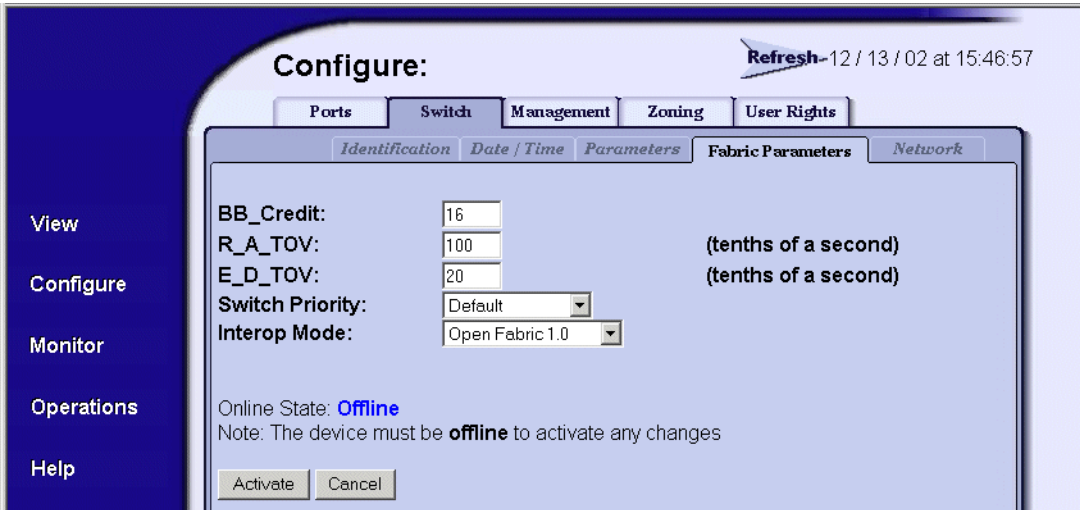

Figure 2–5: Fabric parameters tab view

a. At the BB_Credit field, type a value between **1** and **60**. (This field is not available for the Edge Switch 2/24.) Configure the product 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 industry specification, *Fibre Channel Physical and Signaling Interface*.

b. At the **R_A_TOV** field, type a value between **10** through **1200** tenths of a second (1 through 120 seconds). (The R_A_TOV value must be greater than the E_D_TOV value.)

NOTE: If the product is attached to a fabric element, the product and element must be set to the same R_A_TOV value. If the values are not identical, the E_Port connection to the element fails and the product cannot communicate with the fabric.

c. At the **E_D_TOV** field, type a value between **2** through **600** tenths of a second (0.2 through 60 seconds). (The E_D_TOV value must be less than the R_A_TOV value.)

NOTE: If the product is attached to a fabric element, the product and fabric element must be set to the same E_D_TOV value. If the values are not identical, the E_Port connection to the element fails and the product cannot communicate with the fabric.

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

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

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

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

e. Choose from the **Interop Mode** drop-down list to set the product operating mode. This option does not display if the Operation mode is S/390. (S/390 mode is not supported with the Edge Switch 2/24.) This setting only affects the mode used to manage the product; it does not affect port operation. Available selections are:

— **Homogenous Fabric** — Choose this option if the product is fabric-attached only to other HP Directors or Switches operating in Homogenous Fabric mode.

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

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

5. Set the product online as follows:

a. Choose **Operations** from the navigation panel. The **Operations** page opens.

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

Configuring Network Information

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

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

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

1. Choose **Configure** from the navigation panel.
2. Click the **Switch** or **Director** tab, then click the **Network** tab to display the **Network** tab view (Figure 2–6).

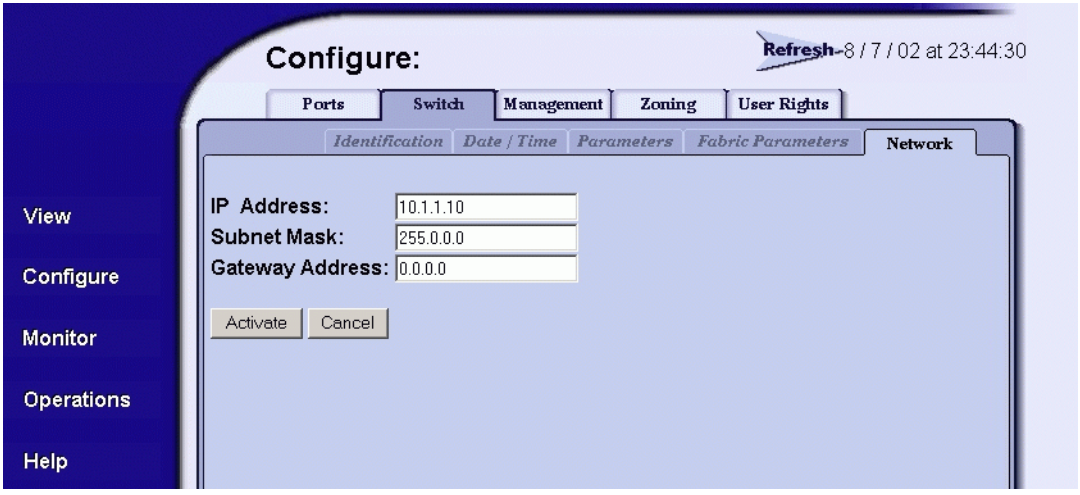

Figure 2–6: Configuring network parameters tab view

a. At the **IP Address** field, type the new value specified by the customer's network administrator (default is **10.1.1.10**).

b. At the **Subnet Mask** field, type the new value specified by the customer's network administrator (default is **255.0.0.0**).

c. At the **Gateway Address** field, type the new value specified by the customer's network administrator (default is **0.0.0.0**).

3. Click **Activate** to save and activate the changes. The following message box displays (Figure 2–7).

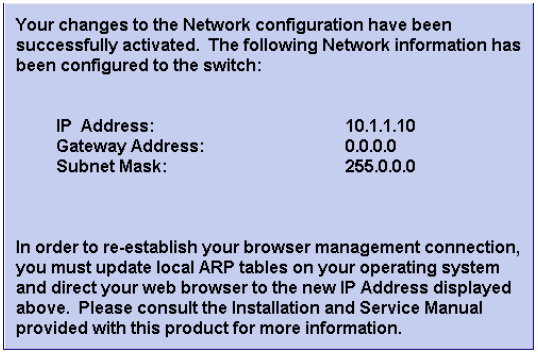

Figure 2–7: Network information message box

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

a. Choose the **Exit** option from the **File** menu to close the Embedded Web Server and browser applications. The Windows desktop displays.

b. At the Windows desktop, click **Start** at the left side of the task bar. The **Windows Workstation** menu displays.

c. At the **Windows Workstation** menu, sequentially choose the **Programs** and **Command Prompt** options. (Depending on which Windows operating system is used, you may need additional steps to access the Command Prompt.) A disk operating system (DOS) window displays.

d. Delete the product'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 product.

e. Click close (**X**) at the upper right corner of the DOS window to close the window and return to the Windows desktop.

5. At the PC, launch the browser application (Netscape Navigator or Internet Explorer).
6. At the browser, enter the product's **new** IP address as the Internet URL. The **Enter Network Password** dialog box displays.

7. Type the user name and password.

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

8. Click **OK**. The EWS interface opens with the **View** page open and the **Switch** or **Director** page displayed.

Configuring SNMP

Perform this procedure to configure community names, write authorizations, network addresses, and user datagram protocol (UDP) port numbers for up to six SNMP trap message recipients. A trap recipient is a management workstation that receives notification (through SNMP) if a switch event occurs. To configure SNMP trap recipients:

1. Choose **Configure** from the navigation panel.
2. Choose the **Management** tab. The **Management** and **SNMP** tab views display (Figure 2–8).

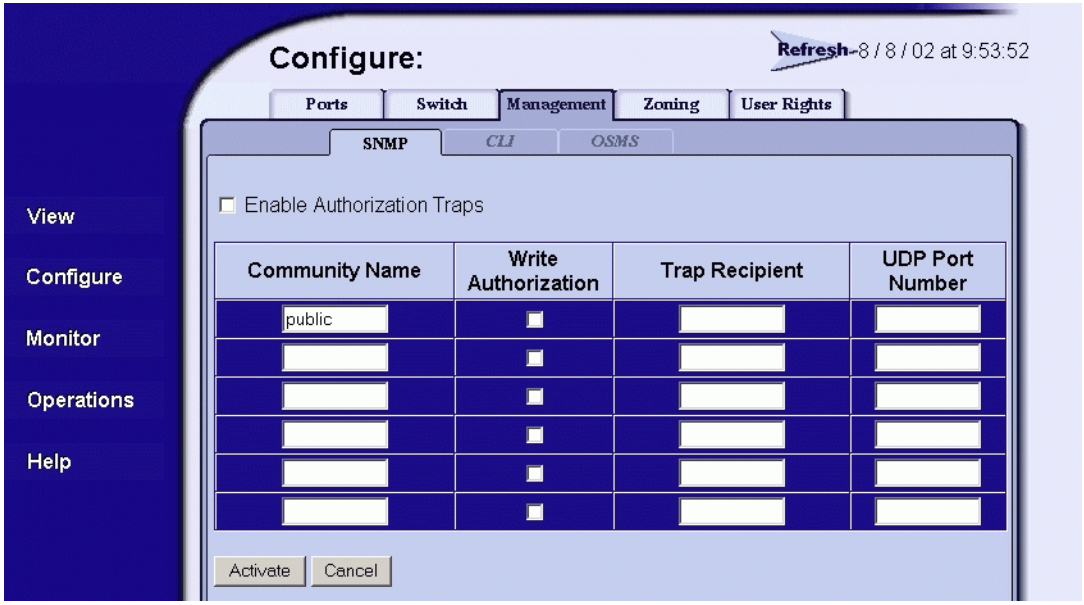

Figure 2–8: Configure SNMP parameters tab view

a. Click the **Enable Authorization Traps** field to enable authorization trap messages to be sent to SNMP management stations when unauthorized stations try to access SNMP information from the product.

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

c. 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 indicates write authorization is enabled. When the feature is enabled, a management workstation user can change **sysContact**, **sysName**, and **sysLocation** SNMP variables.

d. Type the IP address or DNS host name of the trap recipient (SNMP management workstation) in the **Trap Recipient** field in four-byte, dotted-decimal format. It is recommended the IP address be used.

e. The default UDP port number for trap recipients is **162**. Type a decimal port number in the **UDP Port Number** field to override the default value.

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

Enabling or Disabling the CLI

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

1. Choose **Configure** from the navigation panel.
2. Click the **Management** tab and the **CLI** tab. The **CLI** tab view displays (Figure 2–9).

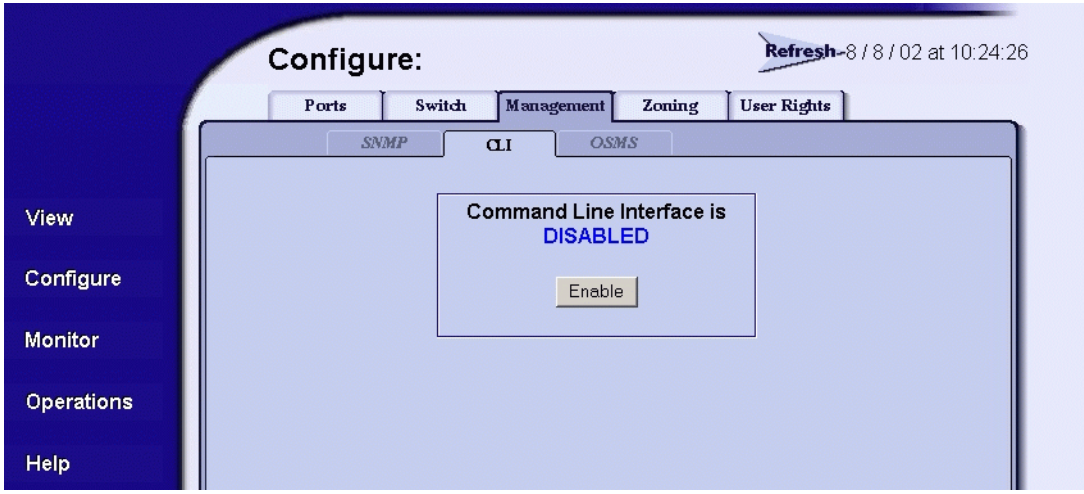

Figure 2–9: Disabling the CLI

3. Perform one of the following steps as required:
   a. Click **Enable** to activate the CLI. The message `Your changes to the CLI enable state have been successfully activated` displays.
   b. Click **Disable** to deactivate the CLI. The message `Your changes to the CLI enable state have been successfully activated` displays.

Enabling or Disabling Host Control

Perform this procedure to enable or disable host control of the product through the OSMS. The OSMS feature must be installed to access this control. Refer to Installing Feature Keys on page 2-22 for instructions. If the feature is not installed, the message `Feature not installed` displays. To enable or disable host control:

1. Choose **Configure** from the navigation panel.
2. Choose the **Management** tab and the **OSMS** tab. The **OSMS** tab view displays (Figure 2–10).

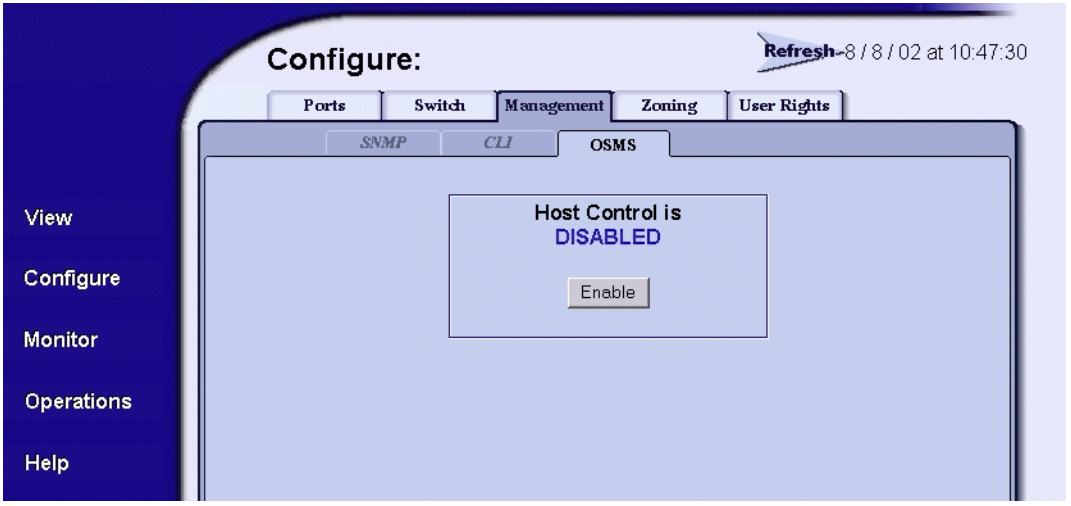

Figure 2–10: Enabling OSMS host control

3. Perform one of the following steps as required:
   a. Click **Enable** to activate the OSMS. The message `Your changes to the host control enable state have been successfully activated` displays.
   b. Click **Disable** to deactivate the OSMS. The message `Your changes to the host control enable state have been successfully activated` displays.

Zoning Tab View

The functionality provided by the **Zoning** tab view is described in Chapter 3, Configuring Zones.

Configuring User Rights

EWS has two login IDs, the administrator-level ID and the operator-level ID. These user names and passwords are used to access the EWS interface through the **Enter Network Password** dialog box. (For a listing of user rights availability for the Administrator and Operator, see User Rights Settings on page 2-20.)

The default administrator-level user name is **Administrator** and the default password is **password**. The default operator-level user name is **Operator** and the default password is **password**. All user names and passwords are case-sensitive.

To configure user names and passwords:

1. Choose **Configure** from the navigation panel.
2. Choose the **User Rights** tab. The **User Rights** tab view displays (Figure 2–11) showing the Administrator and Operator user access levels.

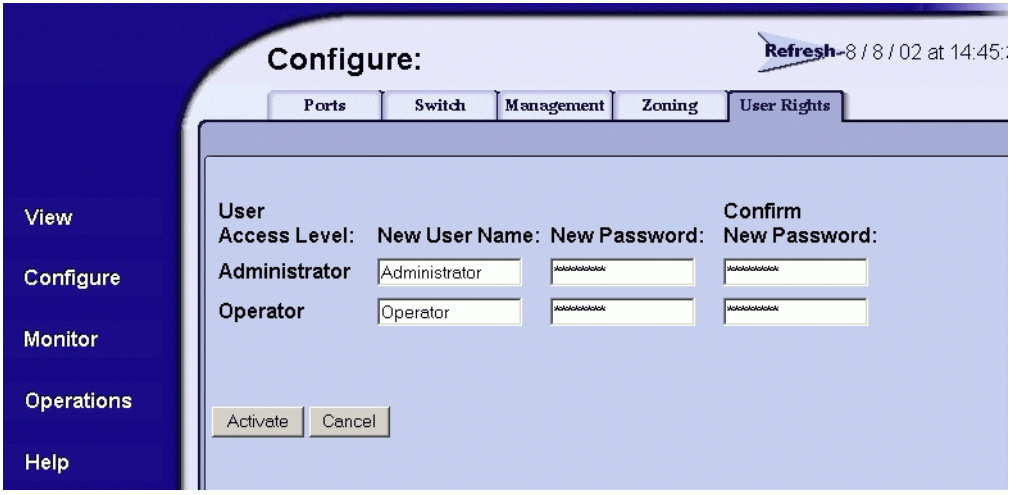

Figure 2–11: Configuring user IDs

3. For the **Administrator** set of data fields:
   a. Type the administrator user name (as specified by the customer's network administrator) in the **New User Name** field. Use 16 alphanumeric characters or less.
   b. Type the administrator password (as specified by the customer's network administrator) in the **New Password** field. Use 16 alphanumeric characters or less.
   c. Type the administrator password again in the **Confirm New Password** field.
4. For the **Operator** set of data fields:
   a. Type the operator user name (as specified by the customer's network administrator) in the **New User Name** field. Use 16 alphanumeric characters or less.
   b. Type the operator password (as specified by the customer's network administrator) in the **New Password** field. Use 16 alphanumeric characters or less.
   c. Type the operator password again in the **Confirm New Password** field.
5. Click **Activate**. The **User Rights** tab redisplays with the message `Your changes to the User Rights configuration have been successfully activated. Login may be required` displays. The new settings for user name and password are implemented.

NOTE: In some cases, you may need to log into EWS again to continue using EWS.

User Rights Settings

Table 2–1: lists the management functions provided by EWS along with the access permissions for each function. If a user lacks the rights to access a specific function, they will receive a login password dialog box indicating the rights (either administrator or operator) required to access the function.

Table 2–1: User Rights Levels

Functionality	Administrator Rights	Operator Rights
View: Unit	Available	Available
View: Port Properties	Available	Available

Table 2–1: User Rights Levels (Continued)

Functionality	Administrator Rights	Operator Rights
View: FRU Properties	Available	Available
View: Unit Properties	Available	Available
View: Fabric	Available	Available
View: Operating Parameters	Available	Available
Configure: Ports	Available	Available
Configure: Switch Identification	Available	Unavailable
Configure: Switch Date/Time	Available	Unavailable
Configure: Switch Operating Parameters	Available	Unavailable
Configure: Switch Network	Available	Unavailable
Configure: Management SNMP	Available	Unavailable
Configure: Management CLI	Available	Unavailable
Configure: Management OSMS	Available	Unavailable
Configure: Zone Set	Available	Unavailable
Configure: Zones	Available	Unavailable
Configure: Modify Zone	Available	Unavailable
Configure: User Rights	Available	Unavailable
Monitor: Port List	Available	Available
Monitor: Port Stats	Available	Available
Monitor: Event Log	Available	Available
Monitor: Node List	Available	Available
Operations: Switch Beacon	Available	Available
Operations: Switch Online State	Available	Unavailable
Operations: Switch Reset Config	Available	Unavailable
Operations: Port Beacon	Available	Available
Operations: Port Reset	Available	Available
Operations: Port Diagnostics	Available	Unavailable
Operations: Maintenance Dump Retrieval	Available	Unavailable

Table 2–1: User Rights Levels (Continued)

Functionality	Administrator Rights	Operator Rights
Operations: Maintenance Product Info	Available	Unavailable
Operations: Maintenance Firmware Upgrade	Available	Unavailable
Operations: Feature Enablement/Installation	Available	Unavailable
Help	Available	Available

Installing Feature Keys

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

- **OSMS** — This feature allows open systems host control of the product.
- **Flexport** — A Flexport switch is delivered at a discount with only a portion of the switch's ports enabled. When additional port capacity is required, the remaining ports are enabled (in eight-port increments) through purchase of this feature.
- **SANtegrity** — This feature enhances security in SANs, which is valuable in SANs that contain a large or heterogeneous group of fabrics and attached devices.

After purchasing a feature, obtain the required feature key from the website to which the feature documentation directs you. A feature key is an alphanumeric string consisting of both uppercase and lowercase characters. The total number of characters may vary depending on keys and serial number. The feature key is case sensitive and must be entered exactly, including dashes.

Feature keys use a format similar to the following:

XxXx-XXxX-xxXX-xX.

NOTE: You must be logged in with Administrator-level rights to install feature keys.

NOTE: With firmware 03.00.00 or earlier, the product must be offline before a feature can be enabled. Also, if the new feature key removes existing functionality, the product must be offline during this process. See Setting Product Online or Offline on page 6-3 for instructions.

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

1. Choose **Operations** from the navigation panel. The **Operations** page opens.
2. Click the **Feature Installation** tab. The **Feature Installation** tab view displays (Figure 2–12).

Figure 2–12: Feature installation tab view

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

NOTE: When **Activate** is selected, all current features are removed and replaced with the features specified in the feature key. Features not included in the new feature key are no longer available on the system. Because of this, it is important to verify that the feature key enables all desired features.

4. Click **Activate** to activate the new feature key.
5. If you receive an error message, `Error 238, Invalid Key`, this means that either the feature key was entered incorrectly or the feature key is not a valid key for that feature. Re-enter the feature key. If you continue to have problems, contact technical support.

3

Configuring Zones

Understanding Zoning

Designing zoning can be a complex task, especially for multiswitch fabrics. Consult with your managed product vendor's professional services organization before configuring zoning.

This section is designed to help you understand the following concepts so that you can more efficiently use Embedded Web Server features to configure and manage zones across a multiswitch fabric:

- Benefits of zoning.
- How zoning works to control access to storage devices and servers across a fabric.
- Other methods of controlling access at the switch and at the server and device, such as binding.
- Merging zoned fabrics.
- Basic concepts of zoning that you must deal with in configuring zoning such as zones, zone sets, active zones, and default zones.

Controlling Access Across a Fabric

Embedded Web Server zoning features enable you to establish zoning across a fabric of devices attached to Switches and Directors by partitioning these devices into groups called zones. A zone is comprised of devices that can access each other through port-to-port connections. Devices in the same zone can recognize and communicate with each other; devices in different zones cannot.

System administrators create zones to increase security measures and prevent data loss or corruption by controlling access between devices (such as servers and data storage units), or between separate user groups (such as engineering or human resources).

Zoning allows an administrator to:

- Establish barriers between devices that use different operating systems. For example, it is often critical to separate servers and storage devices with different operating systems because accidental transfer of information from one to another can delete or corrupt data. Zoning prevents this by grouping devices that use the same operating systems into zones.
- Create logical subsets of closed user groups. Administrators can authorize access rights to specific zones for specific user groups, thereby protecting confidential data from unauthorized access.
- Create groups of devices that are separate from devices in the rest of a fabric. Zoning allows certain processes (such as maintenance or testing) to be performed on devices in one group without interrupting devices in other groups.
- Allow temporary access between devices for specific purposes. Administrators can remove zoning restrictions temporarily (for example, to perform nightly data backup), then restore zoning restrictions to perform normal processes.

Figure 3–1 illustrates three zones established on a single managed product with four devices in each zone. Devices in each zone can communicate with and access devices only in their respective zones.

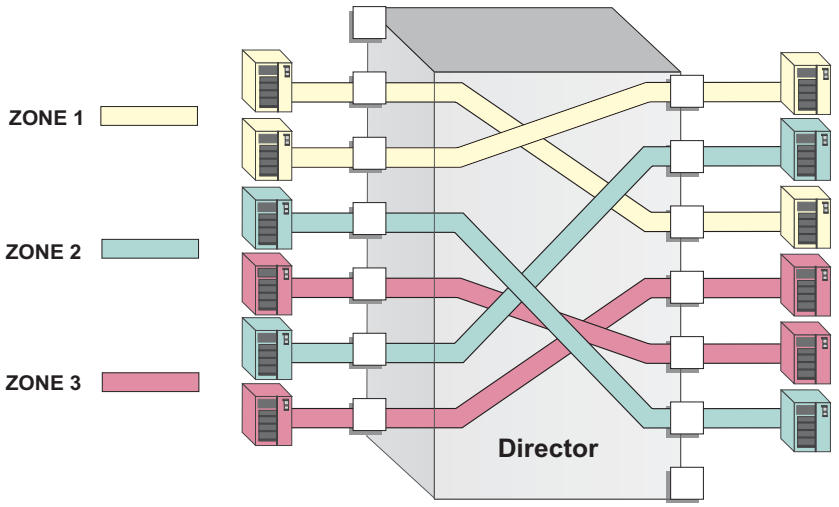

Figure 3–1: Zoning through a single Fibre Channel managed product

Figure 3–2 illustrates how zones can consist of ports and/or devices installed on ports in three managed products in a multiswitch fabric.

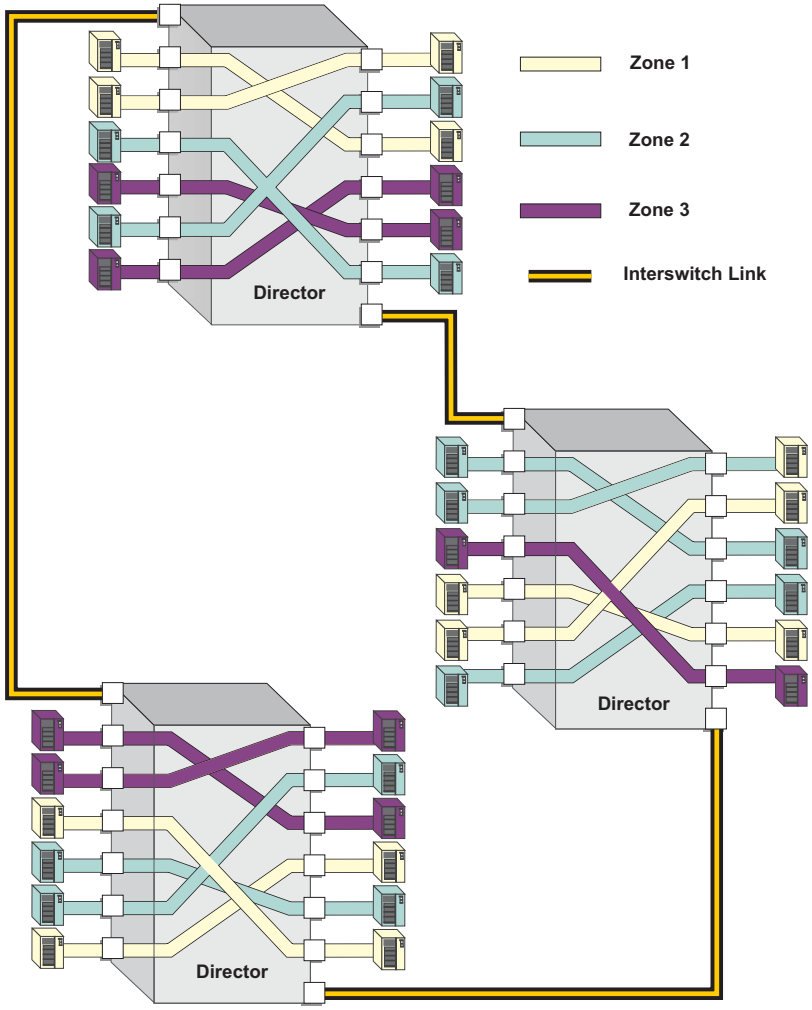

Figure 3–2: Zoning through a multiswitch fabric

Controlling Access at the Switch

A World Wide Name (WWN) binding feature is available on Switches and Directors that allows you to "bind" a specific Switch or Director port to the WWN of an attached device for exclusive communication.

NOTE: This **WWN Binding** feature can be configured through the HP HAFM Product Manager but not through the EWS.

Controlling Access at the Server or Storage Device

Features available at the server or storage device can add methods, beyond zoning, to increase network security measures, differentiate between operating systems, and prevent data loss or corruption by controlling access between devices or between separate user groups (such as engineering or human resources).

Server-level access control is called persistent binding. Persistent binding uses configuration information stored on the server and is implemented through the server's host bus adapter (HBA) driver. The process binds a server device name to a specific Fibre Channel storage volume or logical unit number (LUN), through a specific HBA and storage port WWN. In essence, this feature creates a reliable route across the fabric that sustains the small computer system interface (SCSI) connection between a server and storage device.

For persistent binding:

- Each server HBA is explicitly bound to a storage volume or LUN, and access is explicitly authorized (access is blocked by default).
- The process is compatible with open system interconnection (OSI) standards. The following are transparently supported:
  - — Different operating systems and applications.
  - — Different storage volume managers and file systems.
  - — Different fabric devices, including disk drives, tape drives, and tape libraries.
- If the server is rebooted, the server-to-storage connection is automatically re-established.
- The connection is bound to a storage port WWN. If the fiber-optic cable is disconnected from the storage port, the server-to-storage connection is automatically re-established when the port cable is reconnected. The connection is also automatically re-established if the storage port is cabled through a different managed product port.

Access can also be controlled at the storage device as an addition or enhancement to redundant array of independent disks (RAID) controller software. Data access is controlled within the storage device, and server HBA access to each LUN is explicitly limited (access is blocked by default). Storage-level access control:

- Provides control at the storage port and LUN level, and does not require configuration at the server.
- Is typically proprietary and protects only a specific vendor's storage devices. Storage-level access control may not be available for many legacy devices.

Consult with your managed product vendor's professional services organization before establishing persistent binding.

Consult with your managed product vendor's professional services organization when establishing access control features at the storage device.

This chapter provides instructions for configuring zoning for single and multiple HP HAFM Directors and Switches in a multiswitch fabric.

Zoning Concepts

Zoning is configured by authorizing or restricting access to name server information associated with device ports that attach to product ports. A zone member is specified by the number of the product port to which a device is attached, or by the 8-byte WWN assigned to the host bus adapter or Fibre Channel interface installed in a device. A device port can belong to multiple zones.

Zoning concepts include:

- Zones
- Default Zone
- Zone Sets
- Active Zone Set

Naming Conventions for Zones and Zone Sets

The following naming conventions apply to zones and zone sets:

- All names must be unique and may not differ by case only. For example, myzone and MyZone are both valid individually, but they are not unique.
- The first character of a zone set name must be a letter (A-Z, a-z).
- A zone set name cannot contain spaces.
- Valid characters are a-z, A-Z, 0-9, ^, -, _, and $.
- A zone set name can have a maximum of 64 characters.

Zones

A zone comprises a set of members that can access each other. Refer to Table 3–1 on page 3-10 for details on the number of members that you can configure in a zone and the number of zones that you can configure with the EWS Configure Zone functions.

A zone member can be a Switch or Director port or the WWN of the device. Ports and devices spread throughout multiple managed products in a multiswitch fabric may be grouped into the same zone. Members of a zone can see each other; members in different zones cannot. The number of members that you can configure for a zone varies according to the number of zones in the zone set, the length of the zone names, and other factors, but is essentially bounded by the available nonvolatile random-access memory (NVRAM) in the managed product.

NOTE: Port numbers cannot be used for zone members if the interoperability mode for the Switch or Director is set to Open Fabric 1.0 mode. In this case, you must use node WWNs as zone members.

The type of zone members identified for a zone may be mixed and matched. For example, two members may be specified by a port number and the third member by the WWN of the device.

Using WWNs

To identify a zone member by WWN, use the 16-digit WWN of the device. For example:

10:00:08:00:88:40:C0:D4

In EWS the WWN displays with the Switch or Director manufacturer's name before the WWN. The WWN is assigned to the Fibre Channel interface or HBA installed in devices such as servers or storage devices. Although the device may also have a node WWN, this WWN is not used for zoning identification.

NOTE: Nicknames can be assigned to the WWN using the HAFM Product Manager, not EWS.

The advantage of identifying a zone member as the WWN of the attached device is that the identification will not change if fiber cable connections to ports are rearranged. This is especially important if you are using spare ports. You can simply move the fiber cable to a spare port from a failed port and still maintain the zoning configuration.

The disadvantage of identifying a zone member by the WWN is that 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.

Using Port Numbers

To identify a zone member by port number, use the domain identification number of the managed product and the port number on that managed product. For example:

Domain 1, Port 1

NOTE: Port numbers cannot be used for zone members if the interoperability mode for the Switch or Director is set to Open Fabric 1.0 mode.

Port numbers can be 0 through *n*, with *n* representing the number of ports on the managed product minus one. When you define a zone member by a port number, any device attached through that port is included in the zone. A port number that you assign as a zone member is automatically prefixed with the domain identification number of the managed product.

The advantage of identifying a zone member by port number is that if the HBA on an attached device fails, you don't have to identify the member with the WWN of the replacement HBA.

A disadvantage of port zoning is that someone may rearrange cable connections to ports (because of port failures or other reasons) and inadvertently allow devices to communicate that should not have access to each other.

NOTE: If a managed product's Domain ID changes, you must reconfigure all zones that contained the managed product's port as a zone member. We recommend assigning unique Preferred Domain IDs to each switch in the fabric using the EWS **Configure** page**, Switch**, **Parameters** tabs to change the Preferred Domain IDs.

Default Zone

A default zone consists of all devices that have not been configured as members of a zone in a currently-active zone set. Here are some important points to remember about zone sets:

- You can enable or disable the default zone separately from the active zone set by choosing the **Zoning** option from the **Configure** menu. Enabling the default zone allows all devices and ports not configured as members of the active zone set to communicate. If the default zone is disabled, these ports and devices cannot communicate.
- When no zone set is activated, then all devices are considered to be in the default zone.
- If a zone set is active, then all connected devices that are not included as a members of a zone in the active zone set are included in the default zone.

Zone Sets

A zone set is a group of zones that you can activate or deactivate as a single entity across all managed products in either a single switch or a multiswitch fabric. Only one zone set can be active at one time. Devices that are members of zones in the zone set can only communicate with members of zones in the same zone set. However, devices can be included as members of more than one zone set. By activating a zone set, you are making all zones in the set active.

Refer to Table 3–1 on page 3-10 for details on the number of zones and zone members that you can configure in a zone set and the number of zone sets that you can configure.

Here are some important points to remember about zone sets:

- If no zone set is active, and the default zone is disabled, then no devices can communicate.

- If you activate a zone set when there is already an active zone set, that set will replace the currently-active zone set.
- If you deactivate the current active zone set, then all devices connected in the fabric become members of the default zone.

Active Zone Set

An active zone set is a zone set that is currently active on a single-switch fabric or across all managed products in a multiswitch fabric. At any time, you can disable zoning by deactivating the active zone set and enabling the default zone, or you can enable zoning by activating a zone set. When a zone set is active, all zones that are members of that zone set are active. Only one zone set can be active for the fabric at one time. If no zones are active, then all devices are considered to be in the default zone.

Merging Zoned Fabrics

Managed products are linked through Interswitch Links (ISLs) to form multiswitch fabrics. In a multiswitch fabric, the active zoning configuration applies to the entire fabric. Any change to the configuration applies to all switches in the fabric.

When fabrics join through an ISL, adjacent managed products exchange active zone configurations and determine if the configurations are compatible and can merge. Zoning configurations are compatible if the active zone names in each fabric are unique. If there are identical zone names in each fabric, then the zones must have identical members for the fabrics to join.

If the configurations can merge, the fabrics join. The resulting configuration will be a single zone set containing zone definitions from each fabric.

If configurations cannot merge, the expansion ports (E_Ports) on each product become segmented. Segmented E_Ports cannot carry traffic from attached devices (class 2 or 3 traffic), but can carry management and control traffic (class F traffic) between managed products.

Rules for Merging Zoned Fabrics

Certain rules are enforced to ensure that zoning is consistent across the fabric. Table 3–1 summarizes rules for joining two fabrics through an ISL. The following terms are used in the table:

- Not zoned — No zone set is active in the fabric and the default zone is enabled. In other words, all devices in the fabric are visible to all other devices in the fabric.

- Zoned — A zone set is active in the fabric and/or the default zone is disabled. In this case, devices can discover other devices that are members of the same zone.
- Zoning configuration — Combination of the active zone set definition and the default zone state (enabled or disabled).

Table 3–1: Merging Zones

Fabric A	Fabric B	Result
Not zoned	Not zoned	Fabrics join successfully. The new fabric remains not zoned.
Not zoned	Zoned	Fabrics join successfully and the active zone set will propagate across the fabric. Fabric A inherits zoning configuration from Fabric B.
Zoned	Not zoned	Fabrics join successfully and the active zone set will propagate across the fabric. Fabric B inherits zoning configuration from Fabric A.
Zoned	Zoned	Fabrics can merge if the zone names in each fabric are unique. The resulting active zone set is a union of the zones from each fabric. Once you have merged the two zoned fabrics, click the **Save active zone set as** button in the **Zoning view** to save the active zone set. If there is a zone name conflict (the same zone name in each fabric) then the zones must have identical members for the fabrics to join. If the two zones have the same name but contain different members, then the E_Ports will segment and the fabrics will not join.

NOTE: If merging zones will result in segmented E_Ports and the fabrics will not join, you can join the fabrics by deactivating the active zone set on one of the fabrics (default zone is enabled). This eliminates any conflicts because the fabrics will then join using only the active zone set. After the fabrics join, you can make adjustments to zoning configurations as you desire.

Configuring, Adding, or Deleting Zones

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

CAUTION: If, in your business practices, zoning tasks are performed using both the Command Line Interface (CLI) and EWS, you risk potential conflicts in the configuration and functionality could be lost.

To configure zones:

1. Choose **Configure** from the navigation panel.
2. At the **Configure** page, choose the **Zoning** tab and the **Zones** tab. The **Zones** tab view displays as shown in Figure 3–3.

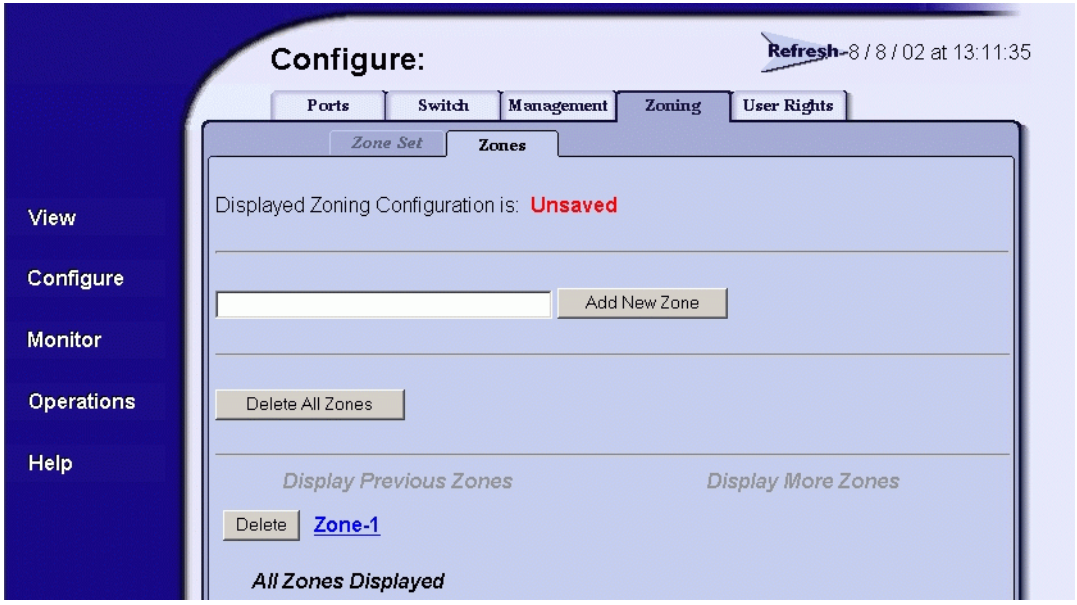

Figure 3–3: Configuring zones

3. To configure a zone, first add the zone name to the product configuration. The following naming conventions apply to zones and zone sets:

- All names must be unique and may not differ by case only. For example, **zone-1** and **Zone-1** are both valid individually, but are not considered unique.
- The first character of a zone set name must be a letter (**A** through **Z** or **a** through **z**).
- A zone set name cannot contain spaces.
- Valid characters are alphanumerics and the caret (**^**), hyphen (**-**), underscore (**_**), or dollar (**$**) symbols.
- A zone set name can have a maximum of 64 characters.

4. Type the zone name and click **Add New Zone**. After the name is validated, the new zone name (**Zone-1**) and an associated **Delete** button display at the bottom of the page. Note the following:
   - **Save and activate the zone** — Changes to a zone or zoning configuration are not saved and activated on the product until saved as part of a zone set. Go to Configuring Zone Sets on page 3-14 to perform this function.
   - **Delete all zones** — To delete all configured zones and zone members, click **Delete All Zones**. A confirmation dialog box displays. Click **OK** to delete all zones.
   - **Delete a single zone** — To delete a single zone and its zone members, click the **Delete** button adjacent to the zone name. A confirmation dialog box displays. Click **OK** to delete the zone.
   - **Display more zones** — If a zone set contains more than 64 zones, the **Display More Zones** link activates to display subsequent pages. In addition, the **Display Previous Zones** link activates on subsequent displayed pages.
5. To add devices (members) to the zone, click the zone name (**Zone-1**). The **Modify Zone** tab view displays (Figure 3–4 on page 3-13).
   - **Rename the zone** — To rename a configured zone, type the new name in the **Zone** field and click **Rename Zone**. After the name is validated, the zone name is changed.

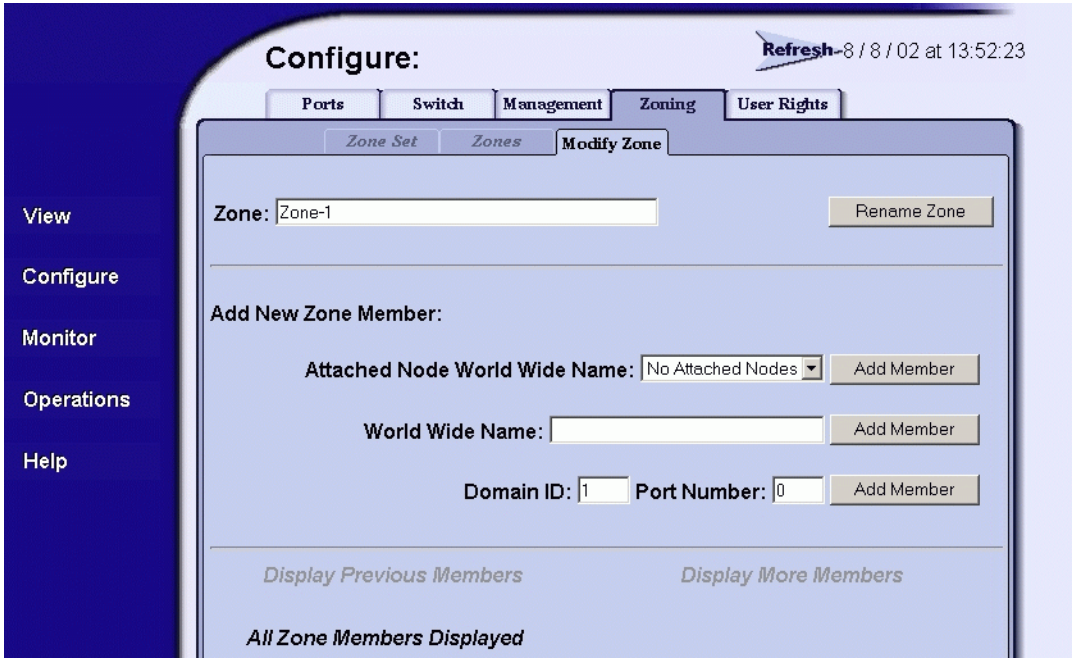

Figure 3–4: Modify Zone tab view

6. Add or delete zone members as follows:

   - **Add member by attached node WWN** — Choose the WWN of an attached device (node) from the **Attached Node World Wide Name** drop-down list and click the adjacent **Add Member** button. The device is added to the zone. (This option is valid for local devices only.)
   - **Add member by WWN** — Type the WWN of a device in the **World Wide Name** field and click the adjacent **Add Member** button. The device is added to the zone.

- **Add member by domain ID and port number** — Type the domain ID (**1** through **31**) of the switch in the **Domain ID** field, type the switch port number to which a device is attached, and click the adjacent **Add Member** button. The device attached to that port is added to the zone.
- **Delete a member** — To delete a zone member, click the **Delete** button adjacent to the configured zone member (WWN or domain ID and port number) at the bottom of the page. A confirmation dialog box displays. Click **OK** to delete the zone member.

7. Changes to a zone, zoning configuration, or zone member are not saved and activated on the switch until saved as part of a zone set. Go to Configuring Zone Sets below to perform this function.
8. Up to 64 zones may be displayed on a single page. If a zone set has more than 64 zones defined, you can display additional pages by choosing **Display Previous Zones** or **Display More Zones**. These fields are grayed out if there are 64 or fewer zones defined for a zone set.

Configuring Zone Sets

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

1. Choose **Configure** from the navigation panel.
2. Choose the **Zoning** tab and the **Zone Set** tab. The **Zone Set** tab view displays (Figure 3–5 on page 3-15).

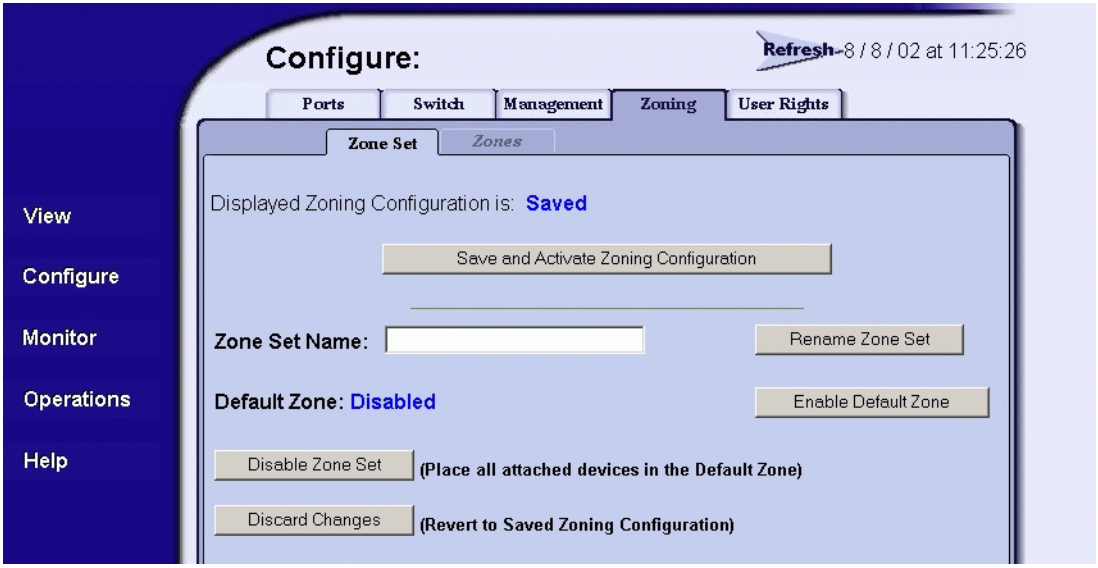

Figure 3–5: Zone Set tab view

3. Click **Save and Activate Zoning Configuration**. After the zone set name is validated, a confirmation dialog box displays.
4. Click **OK** to save and activate the new zone set. The message `Your changes to the Zoning configuration have been successfully activated` displays. Note the following:
   - **Rename zone set** — To rename a zone set, type the new name in the **Zone Set Name** field. Click **Rename Zone Set**. The new zone set name is validated and changed.
   - **Enable or disable default zone** — To toggle (enable or disable) the default zone state, click **Enable Default Zone** or **Disable Default Zone**. Depending on the toggle state, the **Default Zone** field changes to **Enabled** or **Disabled**.
   - **Disable zone set** — To disable the active zone set and place all attached devices in the default zone, click **Disable Zone Set**. A confirmation dialog box displays. Click **OK** to disable the active zone set.
   - **Discard changes** — To discard unsaved changes made to a zone set configuration and revert to a saved zoning configuration, click **Discard Changes**. A confirmation dialog box displays. Click **OK** to discard the changes.

4

Viewing Product and Fabric Data

This chapter describes how to use the Embedded Web Server to view information related to the configuration, status, and communications of a product using the **View** page. You can use EWS to view configuration information for the product and the fabric in which the product participates.

This chapter has been subdivided as follows:

Viewing Product Information

The **View** panel of the EWS interface enables you to see a representation of the physical product, whether a Director or Switch, and view the various IDs and configuration items for the product.

Viewing a Representation of the Product

To view the representation of the product, choose **View** from the navigation panel. The **View** page opens displaying the **Switch** or **Director** tab view, as appropriate for the product (Figure 4–1).

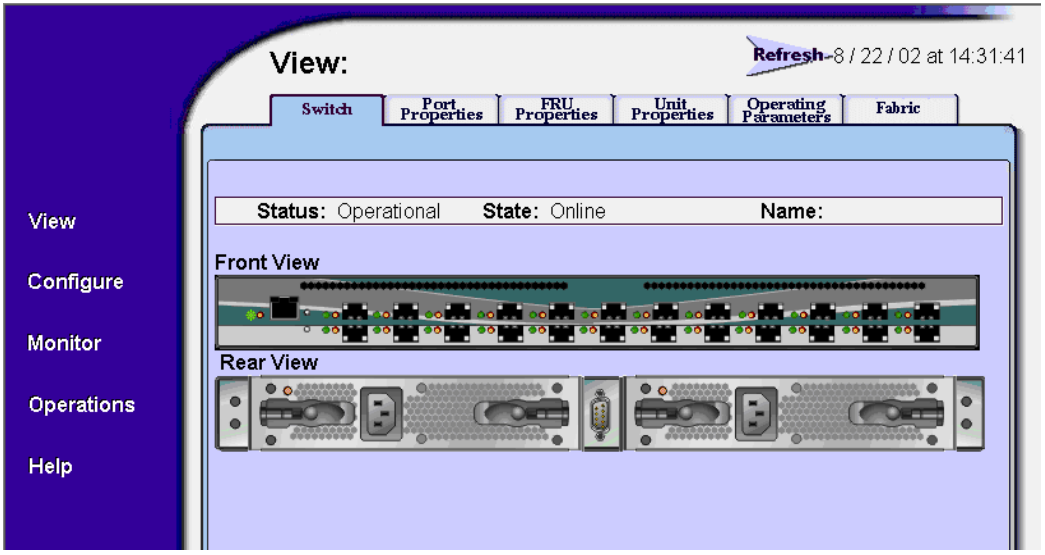

Figure 4–1: Switch tab view for a Edge Switch 2/24

This page shows the following:

- **Status** — The product's operational status. Possible statuses are: **Operational**, **Degraded**, and **Failed**.
- **State** — The product's operational state. Possible states are defined in Table 4–1 on page 4-3

Table 4–1: State Definitions

State	Description
OFFLINE	When the product is OFFLINE, all ports are offline. The ports cannot accept a login from an attached device and cannot connect to other switches. You can configure this state through the **Set Online State** dialog box. Refer to step 5 on page 2-11 for instructions.
Online	All unblocked ports are able to connect with devices. You can configure this state through the **Set Online State** dialog box. Refer to step 5 on page 2-11 for instructions. Note that the product automatically goes online after a power-up, an initial machine load (IML), or initial program load (IPL).

- **Name** — The user-defined name or description assigned to the product.
- **Front View and Rear View** — Using this graphical view of the product, you can view status symbols and simulated light emitting diode (LED) indicators, display data, or use mouse functions to monitor status and obtain vital product information for the product and its hardware components.

  Move the cursor over parts of the graphics to display labels identifying each hardware component or port and its slot position in the chassis relative to identical components installed in the product. Choose a port to view the corresponding **Port Properties** tab for the port. Choose a FRU to view the **FRU Properties** tab for the FRU.

Colored indicators reflect the status of actual LEDs on the product's components. Table 4–2 describes the port operational states and the LED and attention indicators that display on the **Switch** or **Director** page.

Table 4–2: Status Indicators

View	LED Name	Color	Behavior
Front	System Power	Green	• Off when the link is down. • On when the link is up.
	System Error Light (SEL)	Amber	• Off when the SEL is off. • On when the SEL is on.
	Port Online	Green/Blue	• Off when port status is anything but Online. • On Green when port status is Online and the operating speed is 1 Gbps. • On Blue when port status is Online and the operating speed is 2 Gbps (Edge Switch 2/24 only).
	Port Service Required	Amber	• Off when port status is anything but Failed or Service Required. • On when port status is Failed or Service Required.
Rear	FRU Service Required	Amber	• Off when FRU status is Active. • On when FRU status is Failed.

Viewing Port Properties

To view the properties of a port on a product, perform the following procedure:

1. Choose **View** from the navigation panel.
2. Choose the **Port Properties** tab. The **Port Properties** tab view displays (Figure 4–2) showing the properties for only one port.

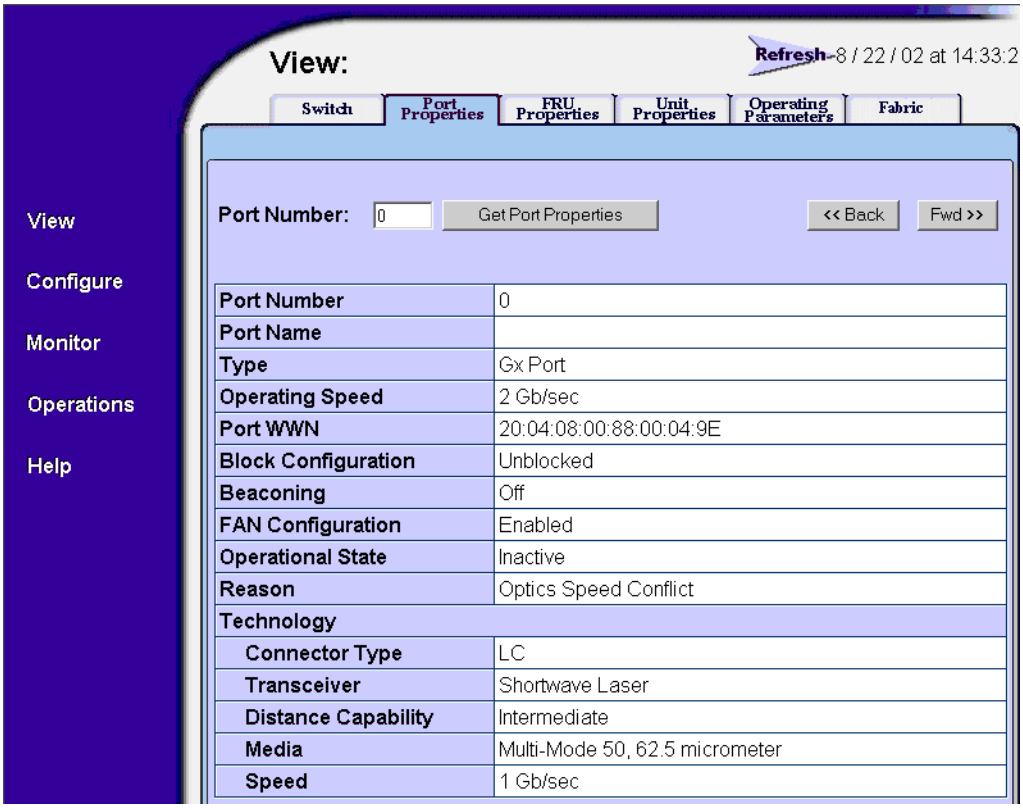

Figure 4–2: Port Properties tab view

3. To display properties for a specific port, insert the port's number in the **Port Number** field and click the **Get Port Properties** button. (You can also use the **<<Back** and **Fwd>>** buttons to view port information incrementally, one at a time.)

The **Port Properties** page provides the following information:

- **Port Number** — The physical port number.
- **Port Name** — User-defined port name or description.
- **Type**
  - — `G_port` — Displays if nothing is logged into the port.
  - — `F_Port` — Displays if a device is logged into the port.
  - — `E_Port` — Displays if the port is connected to another switch's E_Port through an ISL.
  - — `GX_Port` — Valid only on the Edge Switch 2/24; allows a port to operate as either a Fabric Loop Port, Fabric Port, or an Expansion Port.
  - — `FX_Port` — Valid only on the Edge Switch 2/24; restricts a port to operate as either a Fabric Loop Port or a Fabric Port.
- **Operating Speed** — This field displays the current data speed for the port as **1 Gb/sec**, **2 Gb/sec**, or **Not Established**. **Not Established** displays if **Negotiate** is defined as the operating speed and the data speed has not been resolved between the port and the attached device, or if the port and device are not communicating. Note that **2 Gb/sec** and **Not Established** can display only on machines that support 2 Gbps speeds.
- **Port WWN** — The port's 16-digit WWN.
- **Attached Port WWN** — Fibre Channel WWN identifier of the device attached to the port.
- **Block Configuration** — Indicates whether the port is blocked or unblocked.
- **Beaconing** — This field indicates the beaconing status for the port.
- **FAN Configuration** — This field indicates the FAN status for the port. This field is valid only on the Edge Switch 2/24.
- **Operational State** — Inactive, invalid attachment, link incident, no light, not operational, online, offline, port failure, segmented E_Port, testing, or not installed.

- **Reason** — When the port operating state is **Segmented E_Port**, **Invalid Attachment**, or **Inactive**, this field displays the reason for that state. When an E_Port is segmented, two fabrics are prevented from joining. This only occurs when the switch is connected to another switch. Reasons and probable causes are as follows:
  - If Operational State is **Segmented E Port**:
    - Segment Not Defined
    - Incompatible Operating Parameters
    - Duplicate Domain ID(s)
    - Incompatible Zoning Configurations
    - Build Fabric Protocol Error
    - No Principal Switch
    - No Response from Attached Switch
    - ELP Retransmission Failure Timeout
  - If Operational State is **Invalid Attachment**:
    - Unknown
    - ISL connection not allowed on this port
    - ELP rejected by the attached switch
    - Incompatible switch at other end of the ISL
    - External loopback adapter connected to the port
    - N_Port connection not allowed on this port
    - Non-HP high availability fabric switch or compatible switch at other end of the ISL
    - ISL connection not allowed to external Fabrics
    - Port binding violation — unauthorized WWN
    - Unresponsive node connected to Port

— If Operational State is **Inactive**:

— No Serial Number

— No Key Enabled

— Switch Speed Conflict

— Optics Speed Conflict (Director 2/64 and Director 2/140 only)

— No SBAR Support

- **Technology**

  Identifies the technology used for the following aspects of the port:

  — **Connector Type** — The type of connector: LC, MT_RJ, MU, Unknown, or Internal Port.

  — **Transceiver** — The type of transceiver: Longwave Laser (LC), Shortwave Laser, Shortwave Laser with OFC, Longwave Laser (LL), Long Distance Laser, Unknown, or None.

  — **Distance Capability** — General distance range for port transmission: Short, Intermediate, Long, Very Long, or Unknown.

  — **Media** — The Fibre Channel mode and optic size: Single-Mode, Multi-Mode 50 micrometer, Multi-Mode 62.5 micrometer, Multi-Mode 50, 62.5 micrometer, or Unknown.

  — **Speed** — The port speed, either 1 Gbps, 2 Gbps, 4 Gbps, or Unknown.

Viewing FRU Properties

To view the properties of a FRU on a product, perform the following procedure:

1. Choose **View** from the navigation panel.
2. Choose the **FRU Properties** tab. The **FRU Properties** tab view displays (Figure 4–3 on page 4-9) showing each FRU on the product.

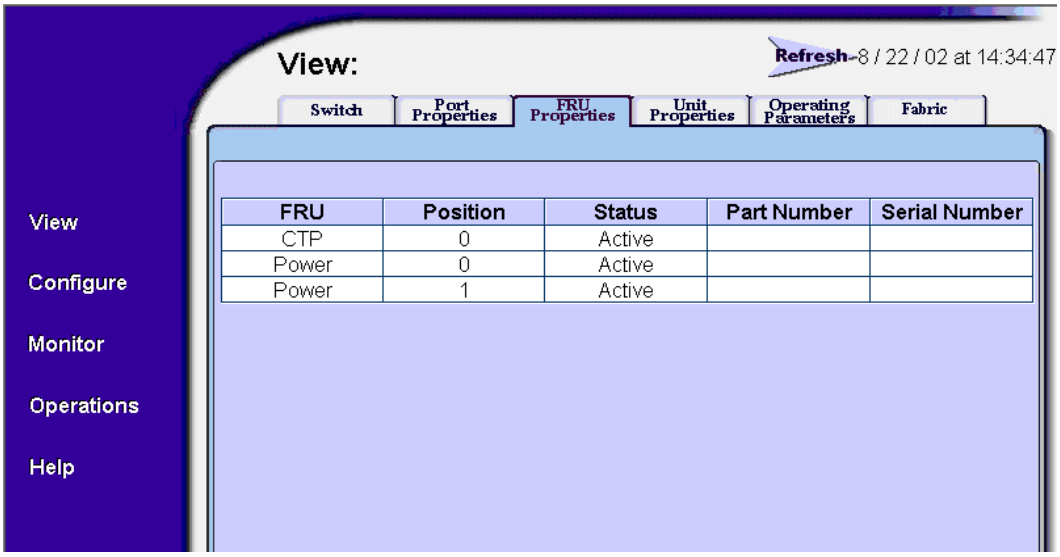

Figure 4–3: FRU Properties tab view

This page shows the following information for the FRUs:

- **FRU —** Name of the FRU.
- **Position —** Slot position relative to identical FRUs installed in the chassis.
- **Status —** Active, backup, or failed state. (On the Edge Switch 2/24, **Not Installed** status indicates the FRU is not present.)
- **Part number —** The OEM part number, as set in non-volatile memory of the FRU (if applicable).
- **Serial number —** Serial number of the FRU, as set in its non-volatile memory (if applicable).

Viewing Unit Properties

To view the unit properties of a product, perform the following procedure:

1. Choose **View** from the navigation panel.
2. Choose the **Unit Properties** tab. The **Unit Properties** tab view displays (Figure 4–4 on page 4-10) showing each FRU on the product.

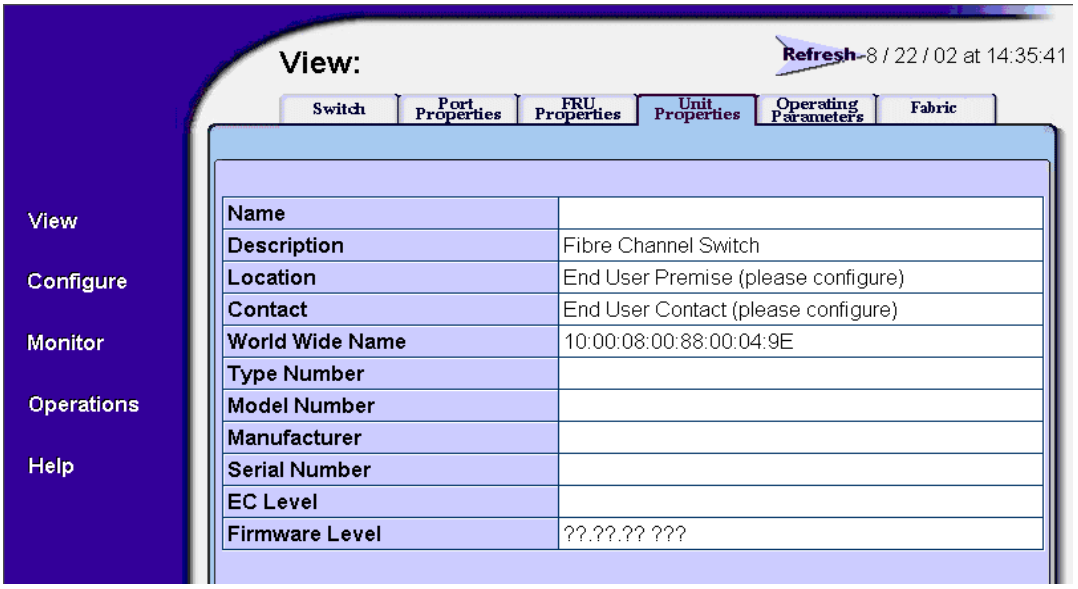

Figure 4–4: Unit Properties tab view

This page shows the following information for the product:

- **Name —** The name configured for the port.
- **Description —** A configurable description of the product functionality.
- **Location —** Location of the product.
- **Contact —** Name of the product's point of contact.
- **WWN —** Fibre Channel WWN address.
- **Type Number —** Type Number of the product (such as 6064 for the Director 2/64).
- **Model Number —** Model Number of the product.
- **Manufacturer —** Three-letter identifier of the product's manufacturer.
- **Serial Number —** Product serial number.
- **EC Level —** Current engineering change (EC) level.
- **Firmware Level —** Release number of the firmware that is currently installed.

Viewing Operating Parameters for the Product

To view the Operating Parameters of a product, perform the following procedure:

1. Choose **View** from the navigation panel.
2. Choose the **Operating Parameters** tab. The **Operating Parameters** tab view displays (Figure 4–5) showing **Switch Parameters** and **Fabric Parameters**.

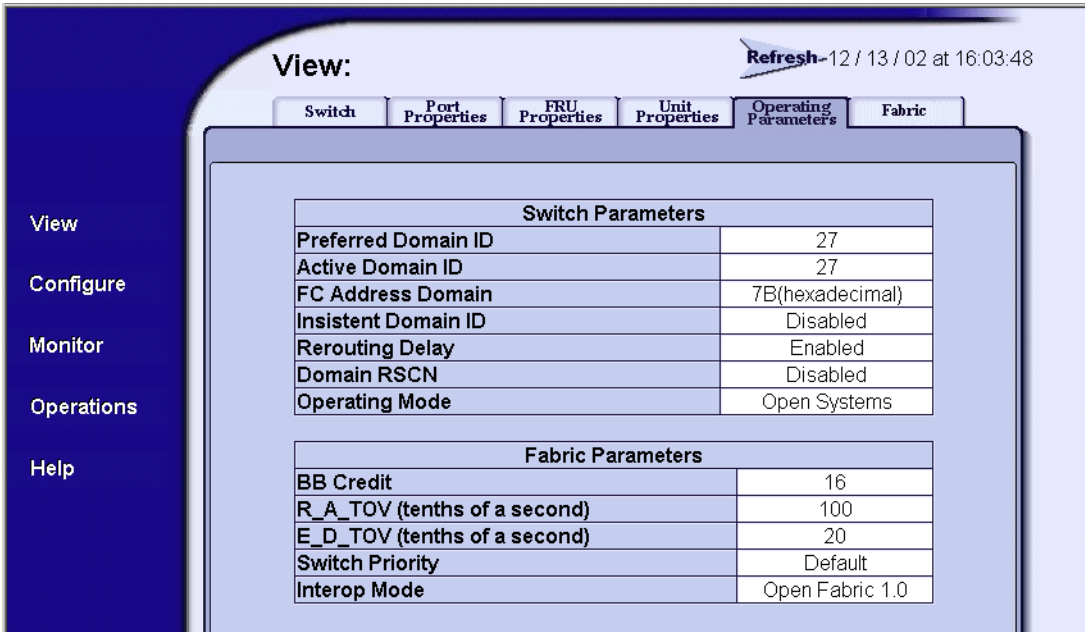

Figure 4–5: Operating Parameters tab view

This page shows the following **Switch Parameters** information for the product:

- **Preferred Domain ID —** The ID to be used if the product participates in a multiswitch fabric. The preferred domain ID must be unique for each Director and Switch in a fabric.
- **Active Domain ID —** The domain ID assigned to the switch.
- **FC Address Domain ID —** The Fibre Channel domain ID.
- **Insistent Domain ID —** Indicates whether the domain ID is enabled to be insistent. The Insistent Domain ID cannot be enabled unless the SANtegrity feature is installed.

- **Rerouting Delay —** Indicates whether rerouting delay is enabled. Enabling the rerouting delay ensures that frames are delivered in order through the fabric to their destination.
- **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. This option is required if Enterprise Fabric mode (an optional SANtegrity feature) is enabled.
- **Operating Mode —** Indicates whether the operation mode is S/390 mode or Open Systems mode. (S/390 mode is not supported with the Edge Switch 2/24.)
- **Director Speed —** speed of communications on the product. Values can be **1 Gbps** or **2 Gbps**. Valid on the Director 2/64 only.

Viewing Fabric Information

Options on the **View** panel of the EWS interface enables you to see information about the fabric in which a product participates. You can view each of the following:

- Operating parameters for a fabric.
- Information about each of the devices that make up the fabric.
- Topology of the fabric.

Viewing Operating Parameters for a Fabric

To view the Operating Parameters of a product, perform the following procedure:

1. Choose **View** from the navigation panel.
2. Choose the **Operating Parameters** tab. The **Operating Parameters** tab view displays (Figure 4–5 on page 4-11) showing the operating function of the product showing **Switch Parameters** and **Fabric Parameters**.

This view shows the following **Switch Parameters** information for the product:

- **BB Credit —** the BB_Credit value for the fabric (not available on the Edge Switch 2/24).
- **R_A_TOV —** Resource Allocation Time Out Value (R_A_TOV) used by the fabric. Specified in tenths of a second.
- **E_D_TOV —** Error Detection Time Out Value (E_D_TOV) value used by the fabric. Specified in tenths of a second.

- **Switch Priority —** Priority value of the switch. Values can be **Default**, **Principal**, and **Never Principal.**
- **Interop Mode —** Interoperability mode of the fabric. Values can be **Homogenous Fabric** and **Open Fabric 1.0**. (This field is not valid if the product's Operation Mode is **S/390**.)

Viewing Fabric Directors and Switches

To view information about the HP high availability fabric Directors and Switches on a menu, perform the following procedure:

1. Choose **View** from the navigation panel.
2. Choose the **Fabric** tab and the **Products** tab. The **Products** tab view displays (Figure 4–6).

NOTE: The page may take some time to display. If the message `Attempting to Collect Data` displays in a product cell, you may want to refresh the image to load data that has been collected. Click the **Refresh** icon at the top right of the window.

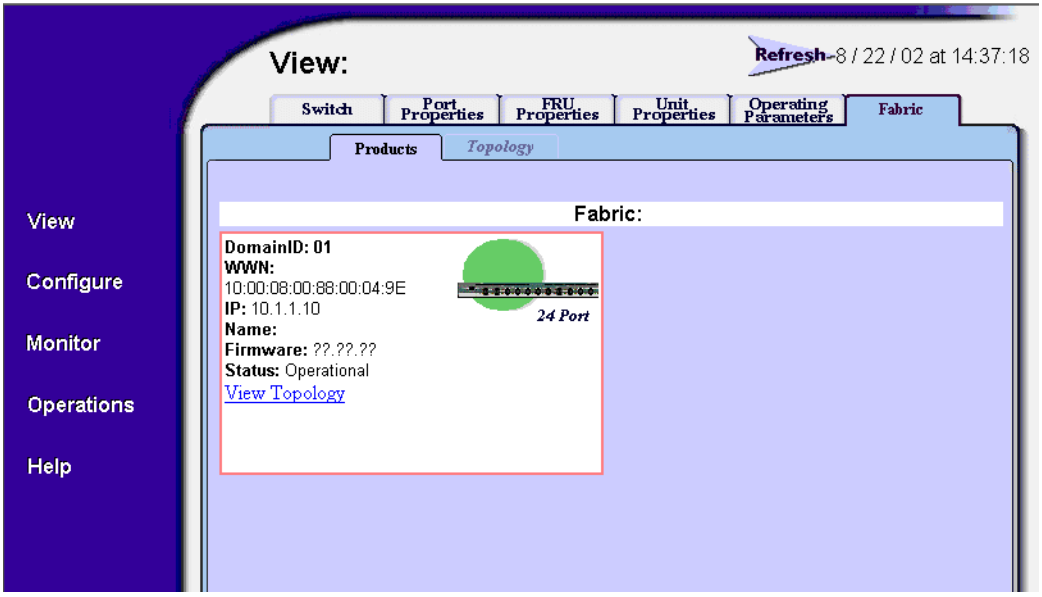

Figure 4–6: Fabric tab with Products tab view

The **Products** page provides the user a quick glance at the devices in the fabric, as well as direct hyperlink access to fabric participants that support the EWS interface. The devices are shown in separate product cells organized by domain ID in numerical order.

NOTE: EWS utilizes embedded OSMS functionality to gain information about other switches in the fabric through in-band (FC) based requests. None of the devices in the fabric (neither the hosting device nor the queried devices) require feature-key enablement of OSMS to utilize this capability.

Each device on the fabric is shown in a separate box called a product cell. The boxes consist of a list of properties for the device, and a graphic showing the product and a symbol that represents the status of the product.

The information shown in the product cells reflects the state of devices as recorded before the information displayed. This information does not update automatically. You must refresh the screen manually to see the most recent information. Click the **Refresh** icon at the top right of the window.

NOTE: If the message `Attempting to Collect Data` displays in a product cell, you may want to reload the page, because it will not update automatically after the initial view is loaded.

Parts of the Product Cell

The product cell has the following parts:

- A graphic representation of the device and its status. For more information, see Parts of the Product Graphic on page 4-16.
- Information about the device. For more information, see the next section, Product Cell Information.
- **View Topology** text that acts as a hyperlink to the **Topology** page for the fabric (firmware 04.00.00 and higher only). Choose this hyperlink to view the **Topology** page. (The hyperlink is found only on the Edge Switch 2/16, Edge Switch 2/32, Edge Switch 2/24, Director 2/64, and Director 2/140.) Other HP high availability fabric Directors and Switches and non-HP products do not have this hyperlink.

Product Cell Information

Each product cell provides information about a device on the fabric as described in Table 4–3:

Table 4–3: Information on the Product Cell

Information	Description	Availability
Domain ID	Domain ID of the product used in the fabric.	Available for any product.
WWN	WWN of the product used in the fabric.	Available for any product.
IP	IP addresses of the product.	HP high availability fabric Directors and Switches only.
Name	Nickname assigned to the product.	HP high availability fabric Directors and Switches only.
Firmware	Level of firmware used by the product.	HP high availability fabric Directors and Switches only.
Status	Status of the product, which can be **Operational**, **Degraded**, **Failed**, or **Unknown**.	The following HP high availability fabric Directors and Switches only: • Edge Switch 2/16 • Edge Switch 2/32 • Edge Switch 2/24 • Director 2/64 • Director 2/140

Parts of the Product Graphic

The product graphic provides the following information:

- The maximum number of ports on the product.
- A graphic representing the status of the product.
- An icon representing the appearance of the product. If the product shown in the graphic is one of the following HP high availability fabric Directors and Switches, the graphic shows an icon that represents the actual product. You can click the graphic to view these devices' Default Pages:
  - Edge Switch 2/16
  - Edge Switch 2/32
  - Edge Switch 2/24
  - Director 2/64
  - Director 2/140
  - Generic product. All other HP Directors and Switches in the fabric have a generic product graphic. The generic product graphic does not provide a link to the device's Default Page.

The symbols that display behind the product graphic indicate the status of the product. The meaning of each symbol is explained in Table 4–4.

Table 4–4: Operating-Status Symbols

Symbol	Symbol Name	Status	Meaning
	Green Circle	Fully Operational	All components and installed ports are operational; no failures.
	Yellow Triangle	Redundant Failure	A redundant component has failed, such as a power supply, and the backup component has taken over operation.
		Minor Failure	A failure occurred that has decreased the product's operational ability. Normal switching operations are not affected. • One or more ports failed, but at least one port is still operational. • A fan has failed or is not rotating sufficiently.
	Red Diamond	NOT OPERATIONAL	A critical failure prevents the product from performing fundamental operations. • All fans failed. • All installed ports failed. • Both power supplies failed.

Viewing Fabric Topology

The topology of a fabric is a high-level view of the routing and pathways on the fabric. To view the fabric topology from the viewpoint of the hosting machine, perform the following procedure:

1. Choose **View** from the navigation panel.
2. Choose the **Fabric** tab and the **Topology** tab. The **Topology** tab view displays (.

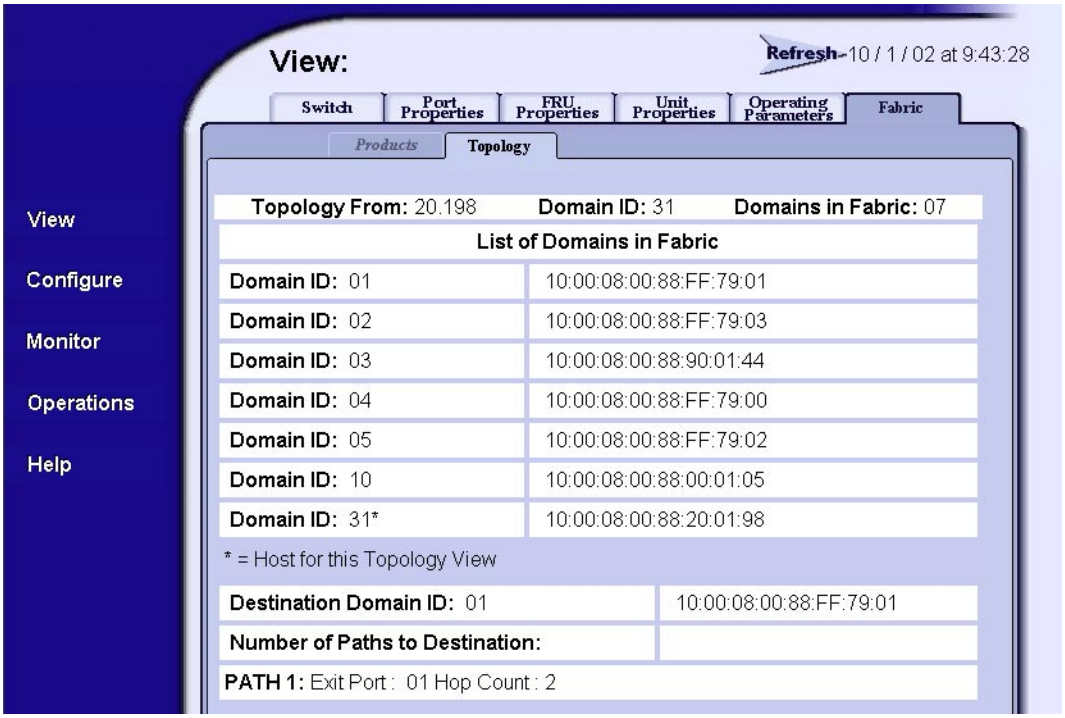

Figure 4–7: Fabric tab with Topology tab view

NOTE: If you attempt to access this page during a fabric build, or any other instance in which the fabric is not operational, only the top line of the page displays, with the message `Fabric Not Operational`.

3. The **Topology** page provides the following information:

Table 4–5: Components of the Topology Page

Part of Page	Component	Description
Host Information	Topology From	Identifies the host product that is providing the fabric topology information. All information on the page is provided from the point of view of the host machine.
	Domain ID	Domain ID of the host product.
	Domains in Fabric	The total number of domains in the fabric.
List of Domains in Fabric	Domain ID	Domain IDs of each device in the fabric. (The ID number that is followed by an asterisk is the ID for the host product.)
	WWN	WWN of the device that corresponds to the Domain ID next to the WWN.
Destination Description	Destination Domain ID	The Domain ID of the destination device. The destination device is described from the point of view of the host product.
	WWN	WWN of the destination device.
	Number of Paths to Destination	Total paths that can be used by the host product to communicate with the destination device.
	List of Paths	A list of each path used by the host product to communicate with the destination device. The details include the Exit Port used for the path and the number of hops needed to reach the destination fabric device.

5

Monitoring Products

The **Monitor** page is used to access information about the product including port and node information as well as critical information about performance. Key tasks you can perform to troubleshoot problems from the **Monitor** page are:

- Monitoring Ports on page 5-1
- Accessing Port Statistics on page 5-3
- Reviewing the Event Log on page 5-8
- Viewing Node List on page 5-10.

Monitoring Ports

You can obtain information about ports from the **Port List** and **Port Stats** tab views.

Port List

Choose **Monitor** on the navigation panel. The **Port List** tab view displays (Figure 5–1). The **Port List** tab view provides the following information including information on the port state:

- **Port # —** The number of the port.
- **Name —** Displays the port name as configured through the **Configure Ports** tab.
- **Block Configuration —** Indicates the blocked or unblocked configuration of the port:
  - — `Blocked` **—** Devices communicating with the port are prevented from logging into the product or communicating with other devices attached to product ports.
  - — `Unblocked` **—** Devices communicating with the port can log in to the product and communicate with devices attached to any other unblocked port in the same zone.

- **State —** See Port Operational States in the next section for an explanation of the states that are displayed.
- **Type —** The type of port that varies by product.

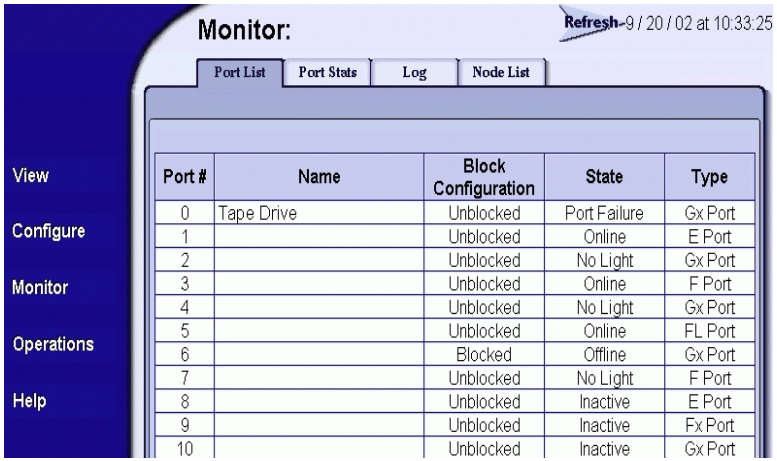

Figure 5–1: Port List tab view

Port Operational States

The **State** column of the **Port List** tab view displays one of the following operational states:

- `Beaconing` — The port is beaconing, which means that a light is flashing on the hardware.
- `Inactive` — The switch port is in an inactive state. Reasons for this state display in the **Reason** field of the **Port Properties** page. (You can find more information at Viewing Port Properties on page 4-5.)

NOTE: Note that if port optics have also failed, the amber LED will be on.

- `Invalid Attachment` — The switch port is in an invalid attachment state.
- `Link Incident` — A link incident occurred on one of the ports.
- `Link Reset` — The switch and the attached device are performing a link reset operation to recover the link connection. Ordinarily, this is a transient state that should not persist.

- `No Light` — No signal (light) is being received on the switch port. This is a normal condition when there is no cable plugged into the port or when the power of the device attached to the other end of the link is off.
- `Not installed` — The port optics are not installed or the feature that provides additional port function is not enabled.
- `Not Operational` — The switch port is receiving the Fibre Channel not operational sequence (NOS) indicating that the attached device is not operational.
- `Online` — The attached device has successfully connected to the switch and is ready to communicate or is in the process of communicating with other attached devices.
- `Offline` — The switch port was configured as "blocked" and is transmitting the Fibre Channel OLS to the attached device.
- `Port Failure` — The switch port has failed and requires service.
- `Segmented E_Port` — The E_Port is segmented preventing the two fabrics from joining (this only occurs when two switches are connected to each other).
- `Testing` — Port is executing an internal loopback test.

Accessing Port Statistics

Choose **Monitor** on the navigation panel. Choose the **Port Stats** tab; the **Port Stats** tab view displays (Figure 5–2: on page -4).

To display port statistics for a selected port, enter a port number in the **Port Number** field and choose **Get Port Statistics**. (You can also choose the **Back** or **Fwd** buttons to view the previous or next port.) The Port Statistics are divided into Traffic Statistics, Error Statistics, Class Two Statistics, and Class Three Statistics.

The information that displays is current as of the time when the view displays. The information does not update automatically.

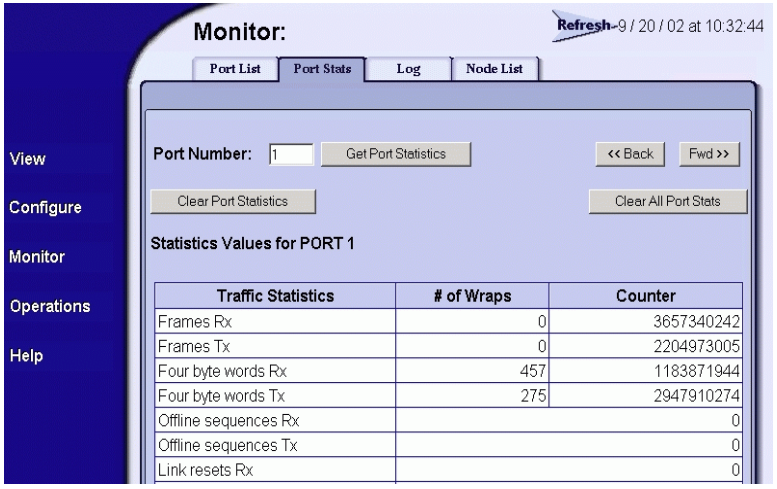

Figure 5–2: Port Statistics tab view

Troubleshooting Tip for Port Stats

As a general rule, you should clear all the counters by choosing **Clear Port Stats** or **Clear All Port Stats** after you have resolved a problem. When troubleshooting, keep track of the time interval when errors accumulate to judge the presence and severity of a problem. (There is a link recovery hierarchy implemented in Fibre Channel to handle some level of "expected anomalies.") For troubleshooting purposes, you want to focus on when the errors, as displayed in the **Counter** column, increment very quickly.

Parts of Statistics Tables

The tables of statistics contain the following columns:

- **Statistics** — Type of statistic being tracked.
- **# of Wraps** — Number of times the **Counter** value wraps, for statistics that grow rapidly. The maximum value that either the **Counter** or the **# of Wraps** can hold is 2^{32}, or 4,294,967,296. Each time the **Counter** field reaches the maximum value of 2^{32}, the wrap count is incremented by 1.
- **Counter** — Number of instances of the tracked item recorded since system initialization or the last time the counters were cleared.

Traffic Transmit and Receive Statistics

The Traffic Statistics include these transmit and receive values.

- **Frames Rx** — Number of frames that the port has received.
- **Frames Tx** — Number of frames that the port has transmitted.
- **Four byte words Rx** — Number of words that the port has received.
- **Four byte words Tx** — Number of words that the port has transmitted.
- **Offline sequences Rx** — Number of offline sequences (OLS) received by this port.
- **Offline sequences TX** — Number of offline sequences (OLS) transmitted by this port.
- **Link resets Rx** — Number of link reset protocol frames received by this port from the attached N_Port.
- **Link resets TX** — Number of link reset protocol frames transmitted by this port to the attached N_Port.
- **Link utilization % Rx** — Current link utilization for the port expressed as a percentage. On 1 Gbps links, ports can transmit or receive data at 100 MB per second. On 2 Gbps links, ports can transmit or receive data at 200 MB per second. Link utilization is calculated over one-second intervals.
- **Link utilization % TX** — Current link utilization for the port expressed as a percentage. On 1 Gpbs links, ports can transmit or receive data at 100 MB per second. On 2 Gbps links, ports can transmit or receive data at 200 MB per second. Link utilization is calculated over one-second intervals.

For the Edge Switch 2/24, the following statistics are also shown:

- **LIPs Detected** — A loop initialization primitive (LIP) was detected, which means the loop was completed.
- **LIPs Generated** — A loop initialization primitive was created to initialize a loop.

Class 2 Statistics

The Class 2 Statistics include these transmit and receive values:

- **Received Frames** — Number of Class 2 frames received by this F_Port from its attached N_Port.
- **Transmitted Frames** — Number of Class 2 frames transmitted by this F_Port to its attached N_Port.
- **Busied Frames** — Number of F_BSY frames generated by this F_Port against Class 2 frames.
- **Rejected Frames** — Number of F_RJT frames generated by this F_Port against Class 2 frames.
- **4-byte words Rx** — Number of Class 2, 4-byte words received by the port.
- **4-byte words TX** — Number of Class 2, 4-byte words transmitted by the port.

Class 3 Statistics

The Class 3 Statistics include these transmit and receive values:

- **Received Frames** — Number of Class 3 frames received by the F_Port from its attached N_Port.
- **Transmitted Frames** — Number of Class 3 frames transmitted by this F_Port to its attached N_Port.
- **Discarded Frames** — Number of Class 3 frames discarded (including multicast frames with bad Domain IDs).
- **4-byte words Rx** — Number of Class 3, 4-byte words received by the port.
- **4-byte words TX** — Number of Class 3, 4-byte words transmitted by the port.

Error Statistics

The Error Statistics include these transmit and receive values:

- **Link failures** — Number of link failures recorded because a not operational sequence (NOS), protocol timeout, or port failure was detected.
- **Sync losses** — Number of loss-of-synchronizations detected because an attached device was reset or disconnected from the port.
- **Signal losses** — Number of loss-of-signal errors detected because the attached device was reset or disconnected from the port.

- **Primitive sequence errors** — Number of primitive sequence protocol errors received from an attached device, which indicates a Fibre Channel link-level protocol violation.
- **Discarded frames** — A received frame could not be routed and was discarded because the frame timed out due to an insufficient buffer-to-buffer credit, or the destination device was not logged into the product.
- **Invalid transmission words** — Number of invalid transmission words from an attached device. This indicates that a frame or primitive sequence arrived at the port corrupted.
- **CRC errors** — A received frame failed a cyclic redundancy check (CRC) validation, indicating the frame arrived at the port corrupted. Frame corruption may be caused by device disconnection, an optical transceiver failure at the device, a bad fiber-optic cable, or a poor cable connection.
- **Delimiter errors** — Number of times that the switch detected an unrecognized start-of-frame (SOF), an unrecognized end-of-frame (EOF) delimiter, or an invalid class of service. This indicates that the frame arrived at the switch's port corrupted. This corruption can be due to plugging/unplugging the link, bad optics at either end of the cable, bad cable, or dirty or poor connections. Moving the connection around or replacing cables can isolate the problem.
- **Address ID errors** — A received frame had an unavailable or invalid Fibre Channel destination address, or an invalid Fibre Channel source address. This typically indicates the destination device is unavailable.
- **Frames too short** — A received frame exceeded the Fibre Channel frame maximum size or was less than the Fibre Channel minimum size, indicating the frame arrived at the switch's port corrupted. Frame corruption may be caused by device disconnection, an optical transceiver failure at the device, a bad fiber-optic cable, or a poor cable connection.

Reviewing the Event Log

Choose **Monitor** on the navigation panel. Choose the **Log** tab; the **Log** tab view displays (Figure 5–3). This log displays a record of significant events that have occurred on the product, such as degraded operation, FRU failures, and port problems. The event log is an important tool you can use to monitor and troubleshoot the products in the SAN. Information contained in the event log may also be used by customer support and service personnel to help resolve problems.

The event log displays the date and time of the event, a unique error event code, event severity level, and additional event data in hexadecimal format.

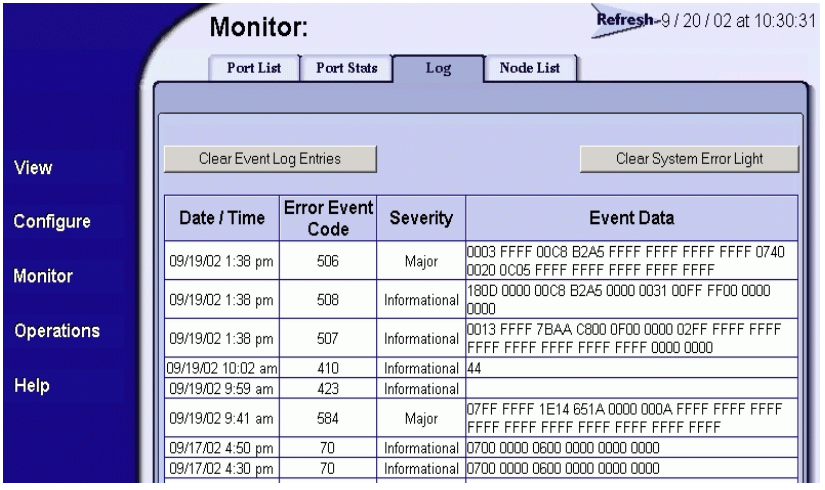

Figure 5–3: Log tab view

Severity Levels

Severity levels are:

- Informational
- Minor
- Major
- Severe (not operational)

Error Event Code Categories

Error Event Codes define event categories; the categories and events vary by product. Below is a list of event codes:

- 1xx-system events
- 2xx-power supply events
- 3xx-fan events
- 4xx-control processor card events
- 5xx-port or universal port module card events
- 6xx-serial crossbar assembly (SBAR) events
- 8xx-thermal incident events

For detailed information on event codes and isolating problems from events and record event data, see the product installation and service manual.

NOTE: In addition to the event log, another method to obtain operation information about the status of the product is from the Fabric Tab. See Chapter 4, Viewing Product and Fabric Data.

There are two options available that you can use to clear either event logs or the system error light. These options are described below.

Clearing Event Log Entries

NOTE: Before clearing the event logs, make sure the logs are not needed for troubleshooting. Once the event log is cleared, the data cannot be retrieved.

To access this option, choose **Monitor** and choose the **Log** tab. Choose **Clear Event Log Entries** to clear the event logs for the product. A message displays stating that the operation has been performed successfully.

Clearing the System (Product) Error Light

To access this option, choose **Monitor**, and then choose the **Log** tab. Click **Clear System Error Light** to clear the ERR (error) LED on the product's front panel. (The ERR LED remains illuminated as long as an event like a FRU failure is active.) A message displays stating that the operation has been performed successfully.

Viewing Node List

Choose **Monitor** on the navigation panel. Choose the **Node List** tab; the **Node List** tab view displays (Figure 5–4). The **Node List** tab view displays information about all node attachments or N_Ports that have logged into existing F_Ports on the product. All data is dynamically updated as the nodes log in and log out.

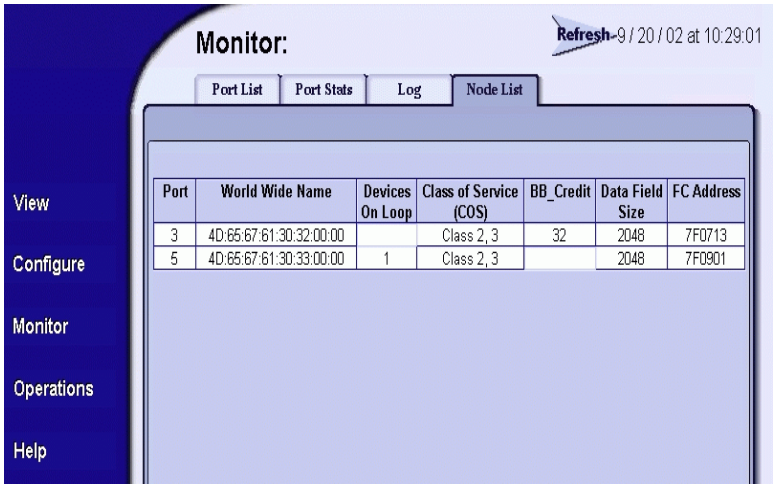

Figure 5–4: Node List tab view

Information displayed for each node includes:

- **Port** — Port number.
- **World Wide Name** — The 16-digit WWN assigned to the attached node.
- **Class of Service (COS)** — Class 2 and/or Class 3 service.
- **BB_Credit** — Buffer-to-buffer credit the attached node has available.
- **Data Field Size** — Largest Fibre Channel frame the node can process.
- **FC Address** — Fibre Channel address, which is shown only if there is a single attached device on the loop. Otherwise, all Fibre Channel address information is displayed on the port-specific page.

For the Edge Switch 2/24, this value is also displayed:

- **Devices on Loop** — Number (device count) of public and private loop-attached devices. This field entry contains a hyperlink to a screen that shows a list of devices on a loop for the port. This tab view shows the **FC Address**, **WWN**, **COS**, and **Data Field Size** for each device in the loop.

6

Operating and Managing Products and Parts

Key Tasks

The **Operations** page is used to manage the product and ports as well as perform maintenance tasks such as port diagnostics. If you or service personnel need to perform troubleshooting, you will access most of the information and tools you need from the **Operations** page.

Setting Product Beaconing On or Off

Choose **Operations** from the navigation panel. The **Switch** or **Director** tab displays, depending on the type of product. Choose the **Beacon** tab; the **Beacon** tab view displays (Figure 6–1).

Using this view, you can enable or disable beaconing on the product. The current state of beaconing for the unit, which is either on or off, is displayed by a flashing LED. Beaconing is useful in helping to isolate problems and locate the product, especially when there are multiple HP high availability fabric Directors and Switches stacked together, such as in a rack-mount cabinet.

You can change the beaconing state from on or off by choosing **Activate**. For example, if the page displays **Unit beaconing is Off**, choosing **Activate** will turn beaconing on. After you refresh the web browser, by choosing the **Beacon** tab, the page will then display **Unit Beaconing is On**.

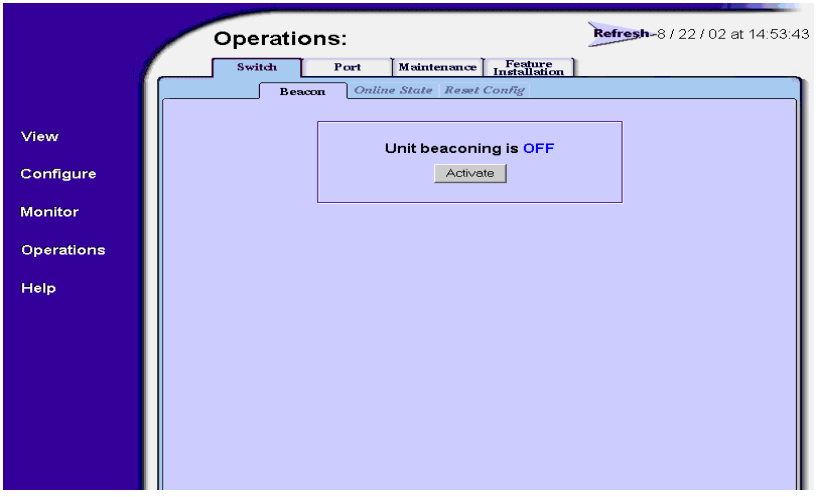

Figure 6–1: Setting product beaconing

Setting Product Online or Offline

Choose **Operations** from the navigation panel. Choose the **Switch** or **Director** tab as appropriate. Choose the **Online State** tab; the **Online State** tab view displays (Figure 6–2). Use this screen to set product online or offline. A box displays with the current online state and a button that is selected to change the state of the product from offline to online or online to offline. If your changes are successful a message displays stating that your changes have been successfully activated. You can refresh the web browser to verify the change has been made.

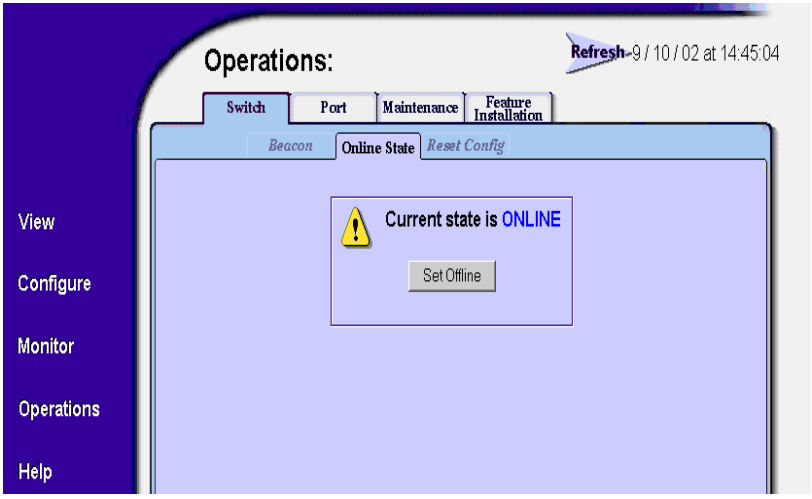

Figure 6–2: Setting product online or offline

Resetting Product Configuration to Default Values

Choose **Operations** from the navigation panel. Choose the **Switch** or **Director** tab as appropriate. Choose the **Reset Config** tab; the **Reset Config** tab view displays (Figure 6–3). You can use this view to reset product configuration values. This enables you to reset all configuration data and nonvolatile settings to the factory default values including any data that was created from the **Configure** page and associated tabs.

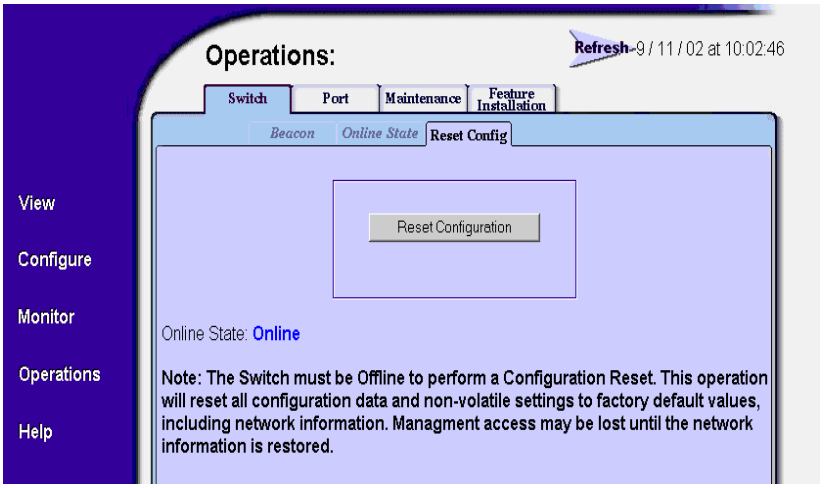

Figure 6–3: Resetting product to default values

NOTE: You may be asked to perform this operation by service personnel; it is important to review the information in this section before performing this operation.

For a list of factory default values, refer to the product's installation and service manual.

CAUTION: This operation will reset all configuration data and non-volatile settings to the factory default values. All optional features will also be disabled. You will need to activate optional features after completing the product reset.

NOTE: Before resetting the product, you may want to review the kinds of data that will be reset by browsing through the **Configure** page and associated tabs.

If the product configuration is reset, management access of the product may be lost until the network information is restored. The product must be offline before the configuration can be reset. See Installing Feature Keys on page 2-22 for instructions.

NOTE: Since the current IP address for the product may not match the factory default values, the Ethernet link between the product and the service processor may drop and not reset. Make sure you record the product's current IP address as you will want to enter that value in the IP Address, under the **Configure** page, **Switch** or **Director** tab as appropriate, and **Network** tab. See Configuring Network Information on page 2-12 for instructions.

NOTE: After you reset the product configuration, you should view the product information page as described in Obtaining Product Information on page 6-13. Save the product information page to a file or print the page to verify the changes you made and to identify the default values.

Set Individual Port Beaconing On or Off

Choose **Operations** from the navigation panel. Choose the **Port** tab and the **Beacon** tab; the **Beacon** tab view displays (Figure 6–4 on page 6-6). Use this view enable or disable beaconing for individual ports. Enabling beaconing helps you to locate a specific port for troubleshooting purposes by the use of flashing port LED. When there are multiple products stacked together, such as in a rack-mount cabinet, beaconing is useful to help locate a specific port by turning beaconing on for only that port.

The first column shows the port number, the second column contains the port name, as configured in the **Ports** tab view on the **Configure** page, and the third column contains check boxes to enable/disable beaconing.

A checked box indicates beaconing is active, an empty box indicates beaconing is not active for the port. To change the state click once inside the box. When finished, click **Activate** to enable the new configuration, or **Cancel** to return to previous configuration. If your changes are successful, a message displays stating that your changes to the configuration have been successfully activated.

NOTE: For the Director 2/140, the ports are displayed through several pages in groups of 32. To configure the port beaconing, make sure you go through each set of ports.

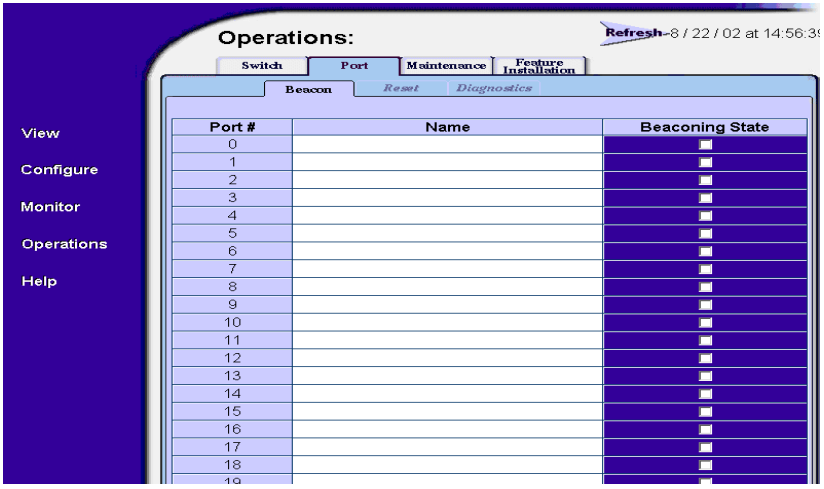

Figure 6–4: Setting individual port beaconing on or off

Resetting Ports

Choose **Operations** from the navigation panel. Choose the **Port** tab and the **Reset** tab; the **Reset** tab view displays (Figure 6–5 on page 6-7). Use this page to reset ports. If a product is attached to the port and is online, this operation sends a link reset to the attached product; otherwise, this action disables port beaconing on the port. If the port is in a failed state, such as after failing a loopback test, the reset restores the port to an operational state and clears the service required (amber) LED. The reset does not affect other ports in the product.

To reset a port, click once in the box for that port's row, so that a check mark displays. When you have selected all ports to reset, click **Activate**. A message displays confirming that the operation has completed. For the Director 2/140, the ports are displayed through several pages in groups of 32. To reset the ports, make sure you go through each set of ports.

Figure 6–5: Resetting ports

Performing Diagnostics on Ports

Choose **Operations** from the navigation panel. Choose the **Port** tab and the **Diagnostics** tab; the **Diagnostics** tab view displays (Figure 6–6 on page 6-8). Use this view to run either internal or external loopback diagnostic tests for any port. (Service personnel may request these tests to be conducted to aid in troubleshooting problems.)

- **Internal loopback test -** an internal loopback test checks internal port, serializer, and deserializer circuitry.
- **External loopback test -** an external loopback test checks all port circuitry, including fiber-optic or copper components.

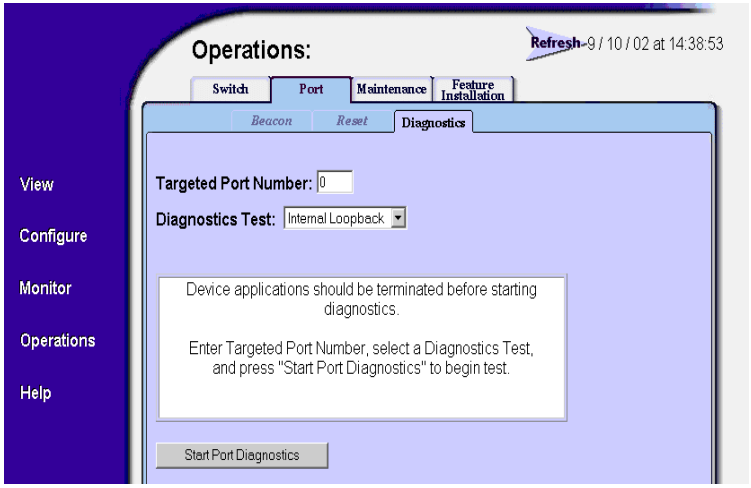

Figure 6–6: Performing diagnostics on ports

To run these tests, make sure that the administrator for any device attached to the ports quiesces Fibre Channel frame traffic through the product and sets the attached devices offline. A message will display in the status area to notify you that device applications should be terminated before starting diagnostics. However, since these tests disrupt port operation, make sure that there are no active nodes connected to the port(s) before starting a test. A loopback plug, furnished with the product, is required for the external loopback test.

NOTE: To identify port numbers on cards that you want to test, drag the mouse cursor across the cards in the **Unit view**. A label displays with the port number.

1. Enter a port number in the **Targeted Port Number** field.
2. Click the arrow on the **Diagnostic Test** drop-down list to display the available tests (**Internal Loopback** and **External Loopback**), then click a test to choose it.

3. Click **Start Port Diagnostics**. Port beaconing automatically initiates on the ports that you choose for loopback diagnostics (Figure 6–7). The test usually lasts 30 seconds as displayed on the page.

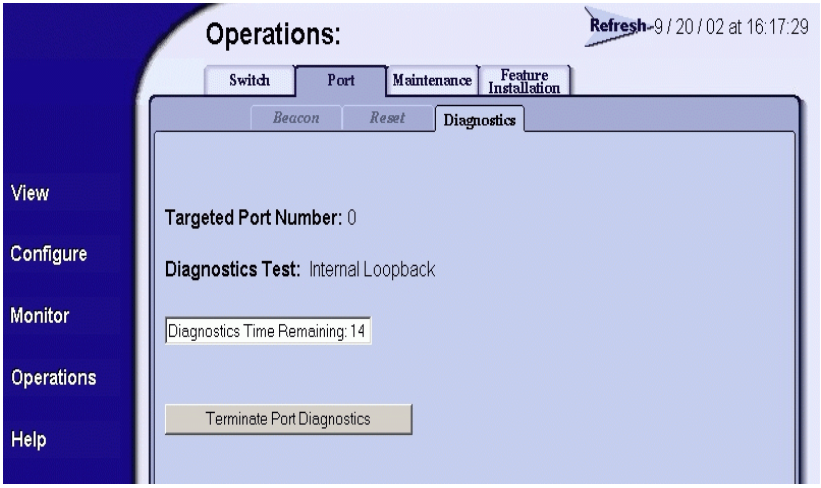

Figure 6–7: Diagnostics test in progress

CAUTION: When disconnecting a fiber optic cable to install an external loopback plug, make sure that you reconnect the cable to the same port after running the external loopback test.

The port's amber LED continues to beacon during the test. If running an internal loopback test, the green LED is off. If running an external loopback test, the green LED is on. Test status displays in the message window and the results display in the status area bar.

4. To stop a test, click **Terminate Port Diagnostics**.

   Beaconing automatically stops when the test completes or is canceled. If the port fails the test, the port's amber LED remains on.

5. Results display when the diagnostics finish or when you terminate the test. If errors occur, record all error information and refer to the product service documentation for problem isolation. See Figure 6–8 for an example of the screen when tests are completed.

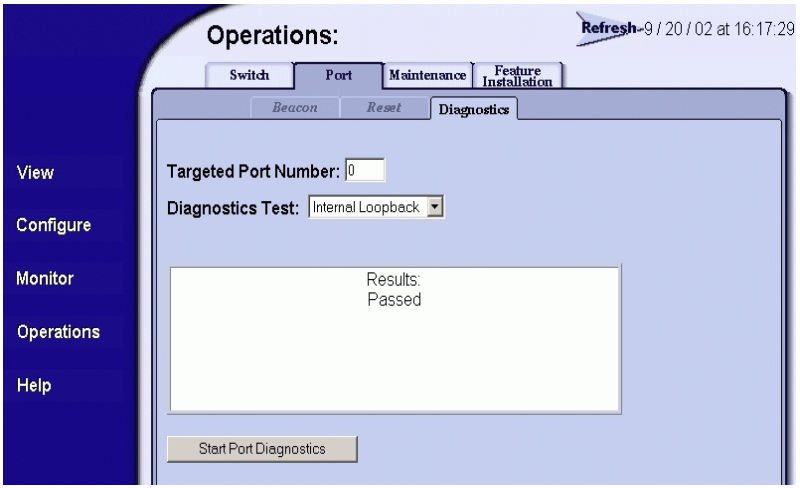

Figure 6–8: Completed diagnostics test

Retrieving Maintenance Information

When the operational firmware detects a critical error, the product automatically copies the contents of dynamic random access memory (DRAM) to a dump area in FLASH memory on the Control Processor (CTP) card; the CTP dump file contains this maintenance information. The CTP dump file will usually be requested by service personnel to aid in troubleshooting.

1. Choose **Operations** from the navigation panel.
2. Choose the **Maintenance** tab and the **Dump Retrieval** tab; the **Dump Retrieval** tab view displays (Figure 6–9).

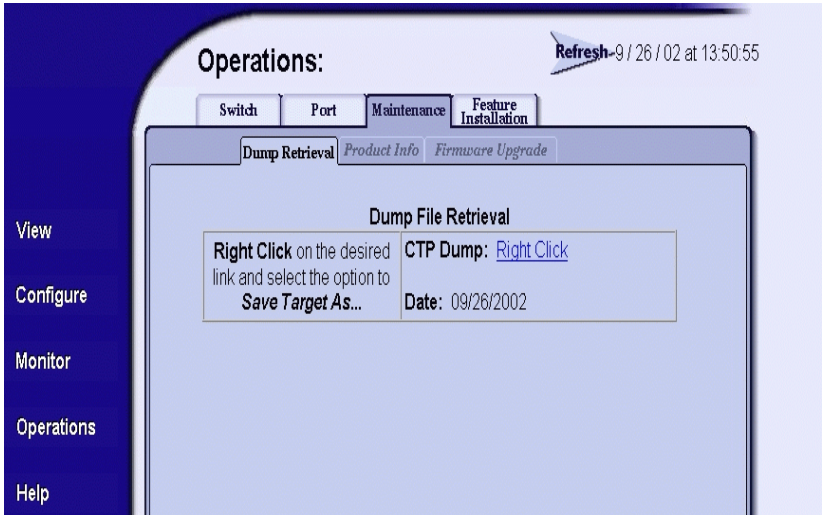

Figure 6–9: Retrieving the CTP maintenance information

3. If no dump file is available, the message **Not Available** displays. If a dump file is available, follow the instructions shown in the tab view.

4. When you have accessed the **Save As** dialog box (Figure 6–10), choose **All Files** from the **Save as type:** field. When naming the file, add a "**.dmp**" extension to the filename.

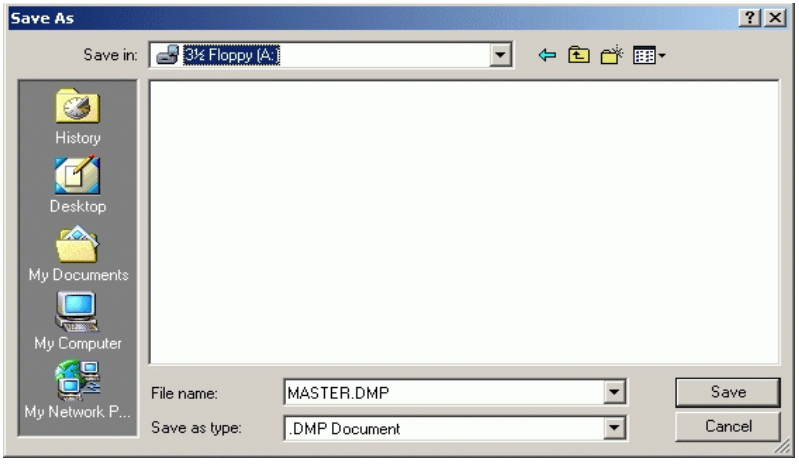

Figure 6–10: Choosing the location to save the CTP maintenance information

5. When the file is completely downloaded, the Download complete screen displays (Figure 6–11). If you encounter any problems during this procedure, contact your service representative.

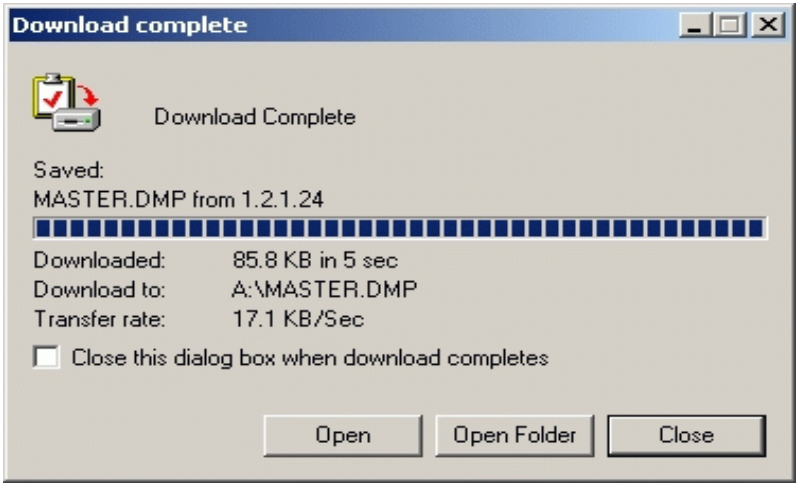

Figure 6–11: Download Complete screen

Obtaining Product Information

To obtain product information, choose the **Operations** page, then the **Maintenance** tab, and then choose **Product Info** tab. The **Product Info** tab view displays (Figure 6–12).

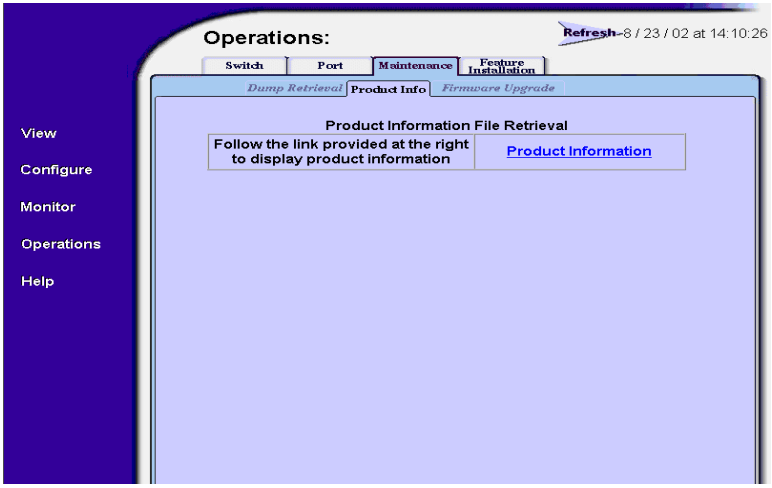

Figure 6–12: Obtaining product information

To view product information, choose the **Product Information** link in the right side of the table. A page with the following information is displayed:

NOTE: You may want to save this page to a file or print this page as the information may be requested by technical support to help resolve technical problems. (You may also want to enter a date in the file you save or on the printed page to note when the product information file was created.)

- Network Information (IP Address, Subnet Mask, Gateway Address)
- Identification Information
- Switch Information
- Operating Parameters
- Port Configurations
- FRU List and Information
- Zoning Information
- Port Data
- Port Technology

- Port Login Data
- E_Port Status
- Switch Status
- Switch Configuration

Upgrading Firmware

Choose the **Maintenance** tab from the **Operations** page, and then choose **Firmware Upgrade** tab to upload and upgrade firmware. The **Firmware Upgrade** tab view displays (Figure 6–13).

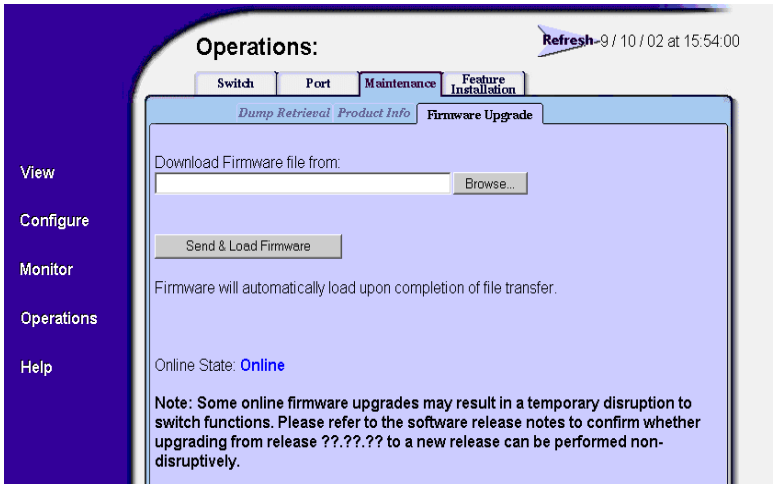

Figure 6–13: Upgrading firmware

The firmware version shipped with the product is provided on the documentation CD-ROM. Information about subsequent firmware versions is provided at HP's website.

Instructions on how to locate and download firmware are provided in the product's installation and service manual. This procedure only describes how to load firmware once you have obtained the version you need for your product.

NOTE: When adding a firmware version, follow all procedural information contained in release notes that accompany the firmware version. That information supplements and supersedes information provided in this manual.

NOTE: Refer to the software release notes on whether the firmware upgrade can be done without causing a disruption as some upgrades may cause a temporary disruption to product function.

Type the drive path and name of the firmware file or click **Browse** to locate the file.

When the correct filename is in the box, click **Send & Load Firmware**. When the firmware has finished transferring, a message displays stating that the new firmware is being activated on the product and the product will be unavailable temporarily. You must reconnect to EWS after this period by logging back into EWS.

NOTE: You can verify the firmware was upgraded by viewing the **Unit Properties** tab under the **View** page. See Viewing Unit Properties on page 4-9.

Activating (Installing) Optional Features

This procedure is described in Installing Feature Keys on page 2-22. Please refer to that procedure for information.

A

Error Messages

This appendix lists and explains error messages for the Embedded Web Server. Any error numbers that are not listed are reserved for future use.

The message that is returned is a string that includes the error number and the text of the message.

Table A–1: High Availability Fabric Manager Messages

Message	Description	Action
Error 08: Invalid Switch Name	The value entered for the switch name is invalid.	The name for the Director or Switch may contain 0–24 characters. Enter a name with 0–24 characters and re-submit. If spaces are used, enclose the name in quotation marks.
Error 09: Invalid Switch Description	The value entered for the switch description is invalid.	The description for the Director or Switch may contain 0–255 characters. Enter a description with 0–255 characters and re-submit. If spaces are used, enclose the description in quotation marks.

Message	Description	Action
Error 10: Invalid Switch Location	The value entered for the switch location is invalid.	The location for the Director or Switch may contain 0–255 characters. Enter a location with 0–255 characters and re-submit. If spaces are used, enclose the location in quotation marks.
Error 11: Invalid Switch Contact	The value entered for the switch contact is invalid.	The contact for the Director or Switch may contain 0–255 characters. Enter a contact with 0–255 characters and re-submit. If spaces are used, enclose the contact in quotation marks.
Error 13: Invalid Port Number	The value entered for the port number is invalid.	Enter a port number within the range supported by your Director or Switch. Valid values are: • 0–15 for the Edge Switch 2/16 • 0-23 for the Edge Switch 2/24 • 0–31 for the Edge Switch 2/32 • 0–63 for the Director 2/64 • 0–127 and 132–144 for the Director 2/140

Message	Description	Action
Error 14: Invalid Port Name	The value entered for the port name is invalid.	The port name for the individual port may contain 0–24 characters. Enter a name with 0–24 characters and re-submit. If spaces are used, enclose the name in quotation marks.
Error 15: Invalid BB Credit	The value entered for the buffer-to-buffer credit is invalid.	The buffer-to-buffer credit must be an integer in the range of 1–60.
Error 16: Invalid R_A_TOV	The value entered for the resource allocation time-out value is invalid.	The R_A_TOV is entered in tenths of a second and must be entered as an integer in the range 10–1200 (1 second to 120 seconds). The R_A_TOV value must be larger than the E_D_TOV value. Check to be sure that all conditions are met and re-submit.
Error 15: Invalid BB Credit	The value entered for the buffer-to-buffer credit is invalid.	The buffer-to-buffer credit must be an integer in the range of 1–60.
Error 16: Invalid R_A_TOV	The value entered for the resource allocation time-out value is invalid.	The R_A_TOV is entered in tenths of a second and must be entered as an integer in the range 10–1200 (1 second to 120 seconds). The R_A_TOV value must be larger than the E_D_TOV value. Check to be sure that all conditions are met and re-submit.

Message	Description	Action
Error 17: Invalid E_D_TOV	The value entered for the error detection time-out value is invalid.	The E_D_TOV is entered in tenths of a second and must be entered as an integer in the range 2–600 (0.2 second to 60 seconds). The E_D_TOV must be smaller than the R_A_TOV. Check to be sure that all conditions are met and re-submit.
Error 18: Invalid TOV	The E_D_TOV and R_A_TOV values are not compatible.	Enter a valid E_D_TOV / R_A_TOV combination. The E_D_TOV must be smaller than the R_A_TOV.
Error 20: Invalid Preferred Domain ID	The value entered for the preferred domain ID for the Director or Switch is invalid.	The preferred domain ID must be an integer in the range 1–31. Enter an appropriate value and re-submit.
Error 21: Invalid Switch Priority	The value entered for the switch priority is invalid.	The switch priority entered for the Director or Switch must be one of the following: **principal**, **never principal**, or **default**. Enter an appropriate value and re-submit.
Error 29: Invalid Gateway Address	The value entered for the gateway address is invalid.	The new gateway address for the Ethernet interface must be entered in dotted decimal format (for example, 0.0.0.0). Enter an appropriate gateway address and re-submit.

Message	Description	Action
Error 30: Invalid IP Address	The value entered for the IP Address is invalid.	The new IP address for the Ethernet interface must be entered in dotted decimal format (for example, 10.0.0.0). Enter an appropriate IP address and re-submit.
Error 31: Invalid Subnet Mask	The value entered for the subnet mask is invalid.	The new subnet mask for the Ethernet interface must be entered in dotted decimal format (for example,. 255.0.0.0). Enter an appropriate subnet mask and re-submit.
Error 32: Invalid SNMP Community Name	The value entered for the SNMP community name is invalid.	The community name must not exceed 32 characters in length. Duplicate community names are allowed, but corresponding write authorizations must match. Enter an appropriate SNMP community name and re-submit.
Error 33: Invalid SNMP Trap Address	The value entered for the SNMP trap address is invalid.	The new SNMP trap address for the SNMP interface must be entered in dotted decimal format (for example, 10.0.0.0). Enter an appropriate SNMP trap address and re-submit.

Message	Description	Action
Error 34: Duplicate Community Names Require Identical Write Authorization	Two or more community names have been recognized as being identical, but their corresponding write authorizations are not identical.	Enter unique SNMP community names or force write authorizations for duplicate community names to be identical and re-submit.
Error 37: Invalid Month	The value of the month entered for the new system date is invalid.	The format of the date parameter must be mm:dd:yyyy or mm/dd/yyyy. The month must contain an integer in the range 1–12. Enter an appropriate date and re-submit.
Error 38: Invalid Day	The value of the day entered for the new system date is invalid.	The format of the date parameter must be mm:dd:yyyy or mm/dd/yyyy. The day must contain an integer in the range 1–31. Enter an appropriate date and re-submit.
Error 39: Invalid Year	The value of the year entered for the new system date is invalid.	The format of the date parameter must be mm:dd:yyyy or mm/dd/yyyy. The year must contain an integer greater than 1980. Enter an appropriate date and re-submit.
Error 40: Invalid Hour	The value of the hour entered for the new system time is invalid.	The format of the time parameter must be hh:mm:ss. The hour can contain an integer in the range 0–23. Enter an appropriate time and re-submit.

Message	Description	Action
Error 41: Invalid Minute	The value of the minute entered for the new system time is invalid.	The format of the time parameter must be hh:mm:ss. The minute can contain an integer in the range 0–59. Enter an appropriate time and re-submit.
Error 42: Invalid Second	The value of the second entered for the new system time is invalid.	The format of the time parameter must be hh:mm:ss. The second can contain an integer in the range 0–59. Enter an appropriate time and re-submit.
Error 44: Max SNMP Communities Defined	A new SNMP community may not be defined without removing an existing community from the list.	A total of 6 communities may be defined for SNMP. A new community can be added only after a current community is removed. Make the appropriate changes and re-submit.
Error 45: Not Allowed While Switch Online	The entered command requires that the Director or Switch be set offline.	Set the switch offline and re-submit the command.
Error 55: Invalid Zone Name	The value entered for the zone name is invalid.	The zone name must be unique and contain 1–64 characters.
Error 57: Duplicate Zone	Two or more zone names in the zone set are identical.	All zone names must be unique. Make the appropriate changes and re-submit.
Error 59: Zone Name in Use	Two or more zone names in the zone set are identical.	All zone names must be unique. Make the appropriate changes and re-submit.

Message	Description	Action
Error 60: Invalid Number of Zone Members	The entered command tried to add more zone members than the zone can hold.	Reduce the number of zone members in the zone and re-submit the command.
Error 61: Invalid Zone Member Type	A zone member was entered that is neither a WWN nor a Domain, Port pair.	Zone members must be expressed in WWN format or as a Domain, Port pair. Make the appropriate changes and re-submit.
Error 62: Invalid Zone Set Name	The value entered for the zone set name is invalid.	The zone set name must be contain 1–64 characters. Make the appropriate changes to the zone set name and re-submit.
Error 69: Duplicate Port Name	Two or more port names are identical.	Port names must be unique. Make appropriate changes and re-submit.
Error 70: Invalid FRU Type	The specified FRU does not exist on this product	Consult the installation/service manual for this product to find appropriate FRU names.
Error 71: FRU Not Installed	The specified FRU is not installed.	Consult the installation/service manual for this product for appropriate action.
Error 72: No Backup FRU	The FRU cannot be swapped because a backup FRU is not installed.	Insert a backup FRU and re-submit the request or consult the installation/service manual for this product for appropriate action.

Message	Description	Action
Error 73: Port Not Installed	The port specified is not installed on this product.	Consult the installation/service manual on installing a port optic.
Error 74: Invalid Number of Zones	The specified zone set contains less than one zone or more than the maximum number of zones allowed for this product.	A zone set must contain at least one zone to be considered valid. Add or remove zones accordingly to meet specified requirements.
Error 75: Invalid Zone Set Size	The zone set entered exceeds switch NVRAM limitations.	Reduce the size of the zone set to meet specified requirements. This can be a reduction in the number of zones in the zone set, a reduction of members in a zone, or a reduction of zone name lengths.
Error 76: Invalid Number of Unique Zone Members	The zone entered contains more than the maximum number of zone members allowed per zone set for this product.	Reduce the number of members in one or more zones and re-submit the command.
Error 77: Not Allowed While Port Is Failed	The port selected is in a failed or inactive state, or is in need of service.	Consult the installation/service manual for appropriate action.
Error 78: System Error Light On	This unit is not able to beacon because the system error light is on.	You must clear the system error light before unit beaconing may be enabled. Consult the installation/service manual for appropriate action.

Message	Description	Action
Error 79: FRU Failed	The specified FRU has failed.	Consult the installation/service manual for appropriate action.
Error 81: Default Zone Enabled	The request cannot be completed because the default zone is enabled	Disable the default zone and re-submit the command.
Error 82: Invalid Interop Mode	The value entered for the interoperability mode is not valid.	The interoperability mode for the Director or Switch must be mcdata (Homogenous Fabric) or open (Open Fabric 1.0). Make the appropriate changes and re-submit the command.
Error 83: Not Allowed in Open Fabric Mode	This request cannot be completed while this switch is operating in Open Fabric 1.0 mode.	Configure the interop mode to Homogenous Fabric mode.
Error 88: Invalid Feature Key Length	The feature key installed is longer than the maximum length allowed.	Be sure that the key has been entered correctly and re-submit. Contact your sales representative with any further problems.
Error 89: Not Allowed in S/390 Mode Without the SANtegrity Feature	Cannot configure port types in S/390 mode without installing SANtegrity.	This command is only supported when the switch is in Open Systems mode or in S/390 with SANtegrity.
Error 90: Invalid Port Type	The port type configured is invalid.	A port may be configured to be an eport, gport, or fport. Be sure the port is configured appropriately and re-submit the command.

Message	Description	Action
Error 91: E_Port Type Configured	Ports are not allowed to be configured as E_Ports in S/390 mode.	Configure the port as either a fport or gport and re-submit the command.
Error 92: Not Allowed While Port Is Unblocked	The port must be blocked to complete this request.	Block the port and re-submit the command.
Error 93: Not Allowed While FICON MS Is Installed	This request cannot be completed because FICON Management Server is installed.	This operation is not supported. No action necessary.
Error 94: Invalid Feature Combination	The features requested cannot be installed at the same time on one Director or Switch.	Contact your sales representative.
Error 99: Preferred Domain ID Cannot Be Zero	This product cannot be configured to have a preferred domain ID equal to zero (0).	Ensure that the ID is expressed as an integer in the range 1–31 and re-submit.
Error 101: Command Not Supported on This Product	This product does not support the requested command.	Command not supported. No action necessary.
Error 102: Switch Not Operational	The request cannot be completed because the switch is not operational.	Consult the installation/service manual and contact your service representative.
Error 115: Invalid Switch Speed	The request cannot be completed because the switch is not capable of operating at the configured speed.	Consult the installation/service manual to determine the speed capabilities of your product.
Error 116: Switch Not Capable of 2 Gb/sec	The request cannot be completed because the switch is not capable of operating at 2 Gbps.	Consult the installation/service manual to determine the speed capabilities of your product.

Message	Description	Action
Error 117: Port Speeds Cannot be Set at Higher Data Rate than Switch Speed	This request cannot be completed because the requested port speed is faster than the currently-configured switch speed.	The switch speed should first be configured to accommodate changes in the configured port speed. The ports can not operate at a faster rate than the switch, itself. Update the switch speed and re-submit the request.
Error 118: Invalid Port Speed	This request cannot be completed because the requested port speed is not recognized for this product.	Port speeds may be set to 1 Gbps or 2 Gbps. Update the port speed and re-submit the request.
Error 119: Switch Speed Not 2 Gb/sec	This request cannot be completed because the switch speed has not been set to 2 Gbps.	The switch speed must be set to 2 Gbps in order to accommodate a port speed of 2 Gbps. Update the switch speed and re-submit the request.
Error 134: Invalid Membership List	Generic message to indicate a problem in either the switch binding or fabric binding membership list.	Be sure that the membership list submitted does not isolate a switch already in the fabric. If this is not the case, the user needs to be aware of all fabric security rules and make sure that the list submitted adheres appropriately.

Message	Description	Action
Error 135: Invalid Number of Fabric Membership List Entries	The number of fabric members submitted exceeds the maximum allowable entries of 31.	The number of entries in the fabric membership list is limited to the total number of domain ID's available to the fabric. Make sure that the list (including the managed switch) contains no more than 31 entries.
Error 136: Invalid Number of Switch Membership List Entries	The number of switch members submitted exceeds the maximum allowable entries of 256.	The number of entries in the switch membership list is limited to 256. Make sure that the list (including the managed switch) contains no more than 256 entries.
Error 137: Invalid Fabric Binding State	The fabric binding state submitted is not recognized by the CLI.	The fabric binding state must be set to either **inactive** or **restrict**.
Error 138: Invalid Switch Binding State	The switch binding state submitted is not recognized by the CLI.	The switch binding state must be set to one of the following: **disable**, **erestrict**, **frestrict**, or **allrestrict**.
Error 139: Insistent Domain ID's Must Be Enabled When Fabric Binding Active	The user attempted to disable insistent domain ID's while fabric binding was active.	Insistent domain ID's must remain enabled while fabric binding is active. If fabric binding is set to inactive, the insistent domain ID state may be changed. It should be noted, however, that this can be disruptive to the fabric.
Error 140: Invalid Insistent Domain ID State	The request cannot be completed because an invalid insistent domain ID state has been submitted.	The insistent domain ID state must be set to either enable or disable.

Message	Description	Action
Error 141: Invalid Enterprise Fabric Mode	The request cannot be completed because an invalid enterprise fabric mode has been submitted.	The enterprise fabric mode must be set to either activate or deactivate.
Error 142: Invalid Domain RSCN State	The request cannot be completed because an invalid domain RSCN state has been submitted.	The domain RSCN state must be set to either enable or disable.
Error 143: Domain RSCNs Must Be Enabled When Enterprise Fabric Mode Active	The user attempted to disable domain RSCN's while enterprise fabric mode was active.	Domain RSCN's must remain enabled while the enterprise fabric mode is active. If enterprise fabric mode is set to inactive, the domain RSCN state may be changed. It should be noted, however, that this can be disruptive to the fabric.
Error 144: The SANtegrity Feature Has Not Been Installed	The user attempted to activate a change to the fabric security configuration without first installing the SANtegrity feature key.	If this key has not been installed, contact your sales representative.
Error 146: Fabric Binding May Not Be Deactivated While Enterprise Fabric Mode Active	The user attempted to deactivate fabric binding while enterprise fabric mode was active.	Fabric binding must be active while operating in enterprise fabric mode. The fabric binding state may be changed if enterprise fabric mode is deactivated. It should be noted, however, that this can be disruptive to the fabric.
Error 148: Not Allowed While Switch Offline	The switch must be online to complete this request.	Change the state of the switch to ONLINE and re-submit the request.

Message	Description	Action
Error 149: Not Allowed While Enterprise Fabric Mode Enabled and Switch Active	The request cannot be completed while the switch is online and enterprise fabric mode is Active.	This operation will be valid if the switch state is set to offline and enterprise fabric mode to inactive. It should be noted, however, that this can be disruptive to the fabric.
Error 151: Invalid Open Systems Management Server State	The request cannot be completed because the OSMS state submitted is invalid.	The OSMS state may be set to either enable or disable.
Error 152: Invalid FICON Management Server State	The request cannot be completed because the FICON MS state submitted is invalid.	The FICON MS state may be set to either enable or disable.
Error 153: Feature Key Not Installed	The request cannot be completed because the required feature key has not been installed to the firmware.	Contact your sales representative.
Error 154: Invalid Membership List WWN	The request cannot be completed because the WWN does not exist in the switch binding membership list.	Make sure that the WWN deleted matches the WWN in the switch membership list. Make appropriate changes and re-submit the request.

Message	Description	Action
Error 155: Cannot Remove Active Member From List	This member cannot be removed from the fabric security list because it is currently logged in.	Fabric security rules prohibit any device or switch from being isolated from the fabric via a membership list change. If it is truly the intention of the user to remove the device in question from the membership list, then there are several approaches to take. This request may be completed most non-disruptively by blocking the port (or physically removing the device from the managed switch) to which this device is attached and re-submitting the request.
Error 156: Cannot Disable Fabric Binding while Switch is Online	The switch must be offline before Fabric Binding can be deactivated.	Deactivating fabric binding is disruptive to Fabric operations. Set the switch offline before deactivating this feature.
Error 201: Change Authorization Request Failed	The switch did not accept the request to make a change to NVRAM.	Be sure all parameters have been entered correctly and re-submit. Contact your service representative with further problems.
Error 202: Invalid Change Authorization ID	The switch will not accept a change request from this particular client.	Be sure all parameters have been entered correctly and re-submit. Contact your service representative with further problems.

Message	Description	Action
Error 203: Another Client Has Change Authorization	Another user is currently making changes to this switch.	Be sure all parameters have been entered correctly and re-submit.
Error 207: Change Request Failed	The switch did not accept the request.	Be sure all parameters have been entered correctly and re-submit. Contact your service representative with further problems.
Error 208: Change Request Timed Out	Authorization time to make NVRAM changes has expired.	Be sure all parameters have been entered correctly and re-submit. Contact your service representative with further problems.
Error 209: Change Request Aborted	The switch did not accept the request.	Be sure all parameters have been entered correctly and re-submit. Contact your service representative with further problems.
Error 210: Busy Processing Another Request	A different switch in the Fabric was busy processing another request and could not complete the command.	Be sure all parameters have been entered correctly and re-submit. Contact your service representative with continued problems.
Error 211: Duplicate Zone	Two or more zone names in the local zone set are identical.	All zone names must be unique. Make the appropriate changes and re-submit.
Error 212: Duplicate Zone Member	A member was added that already exists in the zone.	No action necessary.
Error 213: Number of Zones Is Zero	You are attempting to activate and empty zone set.	The zone set must have at least one zone to be considered valid. Add a valid zone to the zone set and re-submit.

Message	Description	Action
Error 214: A Zone Contains Zero Members	You are attempting to activate a zone set that contains at least one zone with zero members.	Each zone in the zone set must contain at least one member. Add a valid member to the empty zone and re-submit.
Error 215: Zone Set Size Exceeded	The local work area zone set has outgrown the size limitations imposed by the Command Line Interface.	Reduce the size of the zone set to meet CLI requirements. This can be a reduction in the number of zones in the zone set, a reduction of members in a zone, or a reduction of zone name lengths.
Error 218: Invalid Port Number	The value entered for the port number is invalid	Enter a port number within the range supported by your Director or Switch. Valid values are: • 0–15 for the Edge Switch 2/16 • 0-23 for the Edge Switch 2/24 • 0–31 for the Edge Switch 2/32 • 0–63 for the Director 2/64 • 0–127 and 132–144 for the Director 2/140
Error 219: Invalid Port Type	The port type configured is invalid.	A port may be configured to be an eport, gport, or fport. Be sure the port is configured appropriately and re-submit the command. On the Edge Switch 2/24 only, fxport and gxport types are also supported.

Message	Description	Action
Error 222: Invalid SNMP Community Index	The value entered for the SNMP community index is invalid.	The SNMP community index must be an integer in the range 1–6. Make the appropriate changes and re-submit the command.
Error 223: Unknown Error	The switch did not accept the request	Contact your service representative.
Error 224: Invalid Argument	One or more parameters are invalid for this command.	For the appropriate parameters, see the section of the manual that corresponds to the attempted command.
Error 225: Argument Does Not Contain All USASCII Characters	Non-USASCII characters.	For the appropriate parameters, see the section of the manual that corresponds to the attempted command.
Error 226: Argument Is Too Long	One or more parameters are invalid for this command.	For the appropriate parameters, see the section of the manual that corresponds to the attempted command.
Error 227: Invalid SNMP Community Name	The value entered for the SNMP community name is invalid	The community name must not exceed 32 characters in length. Duplicate community names are allowed, but corresponding write authorizations must match. Enter an appropriate SNMP community name and re-submit.
Error 228: Invalid Write Authorization Argument	The write authorization parameter does not contain a valid value.	Parameters must be typed exactly to specification to be recognized correctly.

Message	Description	Action
Error 229: Invalid UDP Port Number	The udpPortNum parameter does not contain a valid value.	Parameters must be typed exactly to specification to be recognized correctly by the CLI.
Error 230: Invalid WWN	The wwn parameter does not contain a valid value.	For the appropriate parameters, see the section of the manual that corresponds to the attempted command.
Error 231: Invalid Port number	The portNum parameter does not contain a valid value.	For the appropriate parameters, see the section of the manual that corresponds to the attempted command.
Error 232: Invalid Domain ID	The domainID parameter does not contain a valid value.	For the appropriate parameters, see the section of the manual that corresponds to the attempted command.
Error 233: Invalid Member	The zone member added is not valid.	For the appropriate parameters, see the section of the manual that corresponds to the attempted command.
Error 234: Invalid Command	The cannot associate an action with the submitted command. The command may be misspelled, required parameters may be missing, or the request may not be applicable.	Consult the documentation for the command to be sure this command was entered correctly, all parameters are valid and present, and that the syntax is correct.

Message	Description	Action
Error 235: Unrecognized Command	Cannot recognize the command and cannot perform the help '?' command as requested.	The entered command is misspelled or the prompt is not positioned at the right place. For the appropriate syntax, see the section of the manual that corresponds to the attempted command.
Error 236: Ambiguous Command	Cannot recognize the command issued.	The command cannot be interpreted because a unique match cannot be identified. For the appropriate syntax, see the section of the manual that corresponds to the attempted command. Enter the complete command and re-submit.
Error 237: Invalid Zoning Database	There was an unidentifiable problem in the local zone set work area.	Verify all parameters are entered correctly and re-submit. Otherwise, the pending zone set should be cleared and reconstructed.
Error 238: Invalid Feature Key	The feature key entered is invalid.	Verify that the feature key was entered correctly and re-submit. Contact your service representative with further difficulties.
Error 239: Fabric binding entry not found	The user requested to remove a fabric binding entry that is not in the pending fabric membership list.	Verify that the correct entry (both WWN and Domain ID) is being requested for removal from the list and re-submit the request.

Message	Description	Action
Error 240: Duplicate fabric binding member	The user requested to add an entry to the fabric binding list that is already a member of the list.	Verify that the correct entry (both **WWN** and **Domain ID**) is being requested for addition to the list and re-submit the request.
Error 241: Comma-delimited mode must be active	Comma-delimited mode must be active to execute this command	Some commands require that comma-delimited mode be active (for example, `show.nameserverExt`) . Enable comma-delimited mode and re-issue the command.
Error 242: Open trunking threshold % value must be 0–99	An invalid threshold percentage has been entered.	The Open trunking threshold must be in the range 0–99. Make sure all values are valid and re-submit the request.
Error 243: Not allowed while S/390 Mode is Enabled	This operation is not allowed while S/390 mode is enabled.	This command is not valid for the S/390 environment.

Glossary

This glossary defines terms used in this guide or related to this product and is not a comprehensive glossary of computer terms. It includes terms from:

American National Standard Dictionary for Information Systems (ANSI X3.172-1990), copyright 1990 by the American National Standards Institute (ANSI). Copies can be purchased from the American National Standards Institute, 25 West 42nd Street, New York, NY 10036. Definitions from this text are identified by (A).

ANSI/EIA Standard - 440A: Fiber Optic Terminology, copyright 1989 by the Electronic Industries Association (EIA). Copies can be purchased from the Electronic Industries Association, 2001 Pennsylvania Avenue N.W., Washington, D.C. 20006. Definitions from this text are identified by (E).

IBM Dictionary of Computing (ZC20-1699). Definitions from this text are identified by (D).

Information Technology Vocabulary, developed by Subcommittee 1 (SC1), Joint Technical Committee 1 (JTC1), of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Definitions of published parts of this vocabulary are identified by (I). Definitions taken from draft international standards, committee drafts, and working papers developed by ISO/IEC SC1/JTC1 are identified by (T), indicating that final agreement has not been reached among the participating national bodies of SC1.

access
The ability and means necessary to store data in, to retrieve data from, to transfer data into, to communicate with, or to make use of any resource of a storage device, a system, or area such as random access memory (RAM) or a register.

access control
A list of all devices that can access other devices across the network and the permissions associated with that access. See also persistent binding; zoning.

active configuration
In S/390 mode, the Director or Switch configuration that is determined by the status of the connectivity attributes.

active field-replaceable unit
Active FRU. An FRU that is currently operating as the active, and not the backup FRU. See also backup field-replaceable unit.

active port address matrix
In S/390 mode, an active port address matrix is the port address matrix that is currently active or operational on an attached Director or Switch. See also connectivity capability.

active zone set
A single zone set that is active in a multiswitch fabric and is created when a specific zone set is enabled. This zone set is compiled by checking for undefined zones or aliases. See also zone; zone set.

address
(1) In data communication, the unique code assigned to each device or workstation connected to a network. (2) The identifier of a location, source, or destination (D).

address name
Synonym for port name.

address resolution protocol
ARP. The protocol by which a host computer maintains a cache of address translations, allowing the physical address of the computer to be derived from the Internet address (D).

alarm
(1) A notification of an abnormal condition within a system that provides an indication of the location or nature of the abnormality to either a local or remote alarm indicator. (2) A simple network management protocol (SNMP) message notifying an operator of a network or device problem.

AL_PA
See arbitrated loop physical address.

American National Standard Code for Information Interchange
ASCII. A standard character set consisting of 7-bit coded characters (8-bit including parity check) used for information exchange between systems and equipment (D).

American National Standards Institute
ANSI. A national organization consisting of producers, consumers, and general interest groups that establishes procedures by which accredited organizations create and maintain industry standards in the United States (A).

application client
The source object of the small computer system interface (SCSI) commands and destination for the command responses.

application program
A program used to connect and communicate with stations in a network, enabling users to perform application-oriented activities (I).

arbitrated loop
One of the three connection topologies offered by Fibre Channel protocol. Up to 126 node ports and one fabric port can communicate without the need for a separate switched fabric. See also point-to-point (point-to-point).

arbitrated loop physical address
AL_PA. A 1-byte value used in the arbitrated loop topology that identifies loop ports (L_Ports). This value then becomes the last byte of the address identified for each public L_Port on the loop.

arbitration
Process of selecting one device from a collection of devices that request service simultaneously.

ARP
See address resolution protocol.

ASCII
See American National Standard Code for Information Interchange.

attribute
In S/390 mode, the connection status of the address on a configuration matrix: allowed, blocked, or prohibited.

backup field-replaceable unit
Backup FRU. When an active FRU fails, an identical backup FRU takes over operation automatically (failover) to maintain Director or Switch and Fibre Channel link operation. See also active field-replaceable unit.

backup FRU
See backup field-replaceable unit.

BB_Credit
See buffer-to-buffer credit.

beaconing
Use of light-emitting diodes (LEDs) on ports, port cards, field-replaceable units (FRUs), and Directors to aid in the fault-isolation process. When enabled, active beaconing will cause LEDs to flash in order for the user to locate field-replaceable units (FRU's), switches, or Directors in cabinets or computer rooms.

blocked connection
In S/390 mode, in a Director or Switch, the attribute that, when set, removes the communication capability of a specific port. A blocked address is disabled so that no other address can be connected to it. A blocked attribute supersedes a dedicated or prohibited attribute on the same address. Contrast with unblocked connection. See also connectivity attribute; dynamic connection; dynamic connectivity.

blocked port
In a Director or Switch, the attribute that when set, removes the communication capability of a specific port. A blocked port continuously transmits the offline sequence.

buffer
Storage area for data in transit. Buffers compensate for differences in processing speeds between devices. See also buffer-to-buffer credit.

buffer-to-buffer credit
BB_Credit. (1) The maximum number of receive buffers allocated to a transmitting node port (N_Port) or fabric port (F_Port). Credit represents the maximum number of outstanding frames that can be transmitted by that N_Port or F_Port without causing a buffer overrun condition at the receiver. (2) The maximum number of frames a port can transmit without receiving a receive ready signal from the receiving device. BB_Credit can be adjustable to provide different levels of compensation.

bus
The path that carries data between the computer (microprocessor) and peripheral devices. An IDE interface cable and a small computer system interface (SCSI) cable are both examples.

bypassed port
If a port is bypassed, all serial channel signals route past the port. A device attached to the port cannot communicate with other devices in the loop.

cascade
Linking two or more Fibre Channel switches to form a larger switch or fabric. The switched link through fiber cables attached between one or more expansion ports (E_Ports). See also expansion port

channel
(1) A system element that controls one channel path, and whose mode of operation depends on the type of hardware attached. Each channel controls an I/O interface between the channel control element and the attached control units (D). (2) Point-to-point link that transports data from one point to the other. (3) A connection or socket on the motherboard to controller card. A motherboard may have only one or two channels (primary and secondary). If a motherboard has only one channel, it may be necessary to add a controller card to create a secondary channel.

channel-attached
(1) Pertaining to direct attachment of devices by data I/O channels to a computer. (2) Pertaining to devices attached to a control unit by cables, not telecommunication lines (D). Synonymous with local.

channel path
CHP. A single interface between a central processor and one or more control units, along which signals and data are sent to perform I/O requests (D).

channel path identifier
CHPID. In a channel subsystem, a value assigned to each channel path of the system that uniquely identifies the path (D). See also channel-to-channel (channel-to-channel) (input/output configuration program).

channel subsystem
CSS. A collection of subchannels that direct the flow of information between I/O devices and main storage, relieve the processor of communication tasks, and perform path management functions (D).

channel-to-channel
CTC. A channel attached to another channel (channel-to-channel) and specifies the I/O mode of operation for the channel path under the I/O configuration program (IOCP) channel path identifier (CHPID) statement 'Type' parameter (D). See also channel path identifier (input/output configuration program).

channel wrap test
A diagnostic procedure that checks S/390 host-to-Director or host-to-Switch connectivity by returning the output of the host as input. The test is host-initiated and transmits Fibre Channel frames to a Director or Switch port. A Director or Switch port enabled for channel wrapping echoes the frame back to the host.

CHP
See channel path.

CHPID
See channel path identifier.

Class 2 Fibre Channel service
Provides a connectionless (not dedicated) service with notification of delivery or nondelivery between two node ports (N_Ports).

Class 3 Fibre Channel service
Provides a connectionless (not dedicated) service without notification of delivery or nondelivery between two node ports (N_Ports).

Class F Fibre Channel service
Used by switches to communicate across interswitch links (ISLs) to configure, control, and coordinate a multiswitch fabric.

Class of Fibre Channel service
Defines the level of connection dedication, acknowledgment, and other characteristics of a connection.

client
A node that requests network services from a server. Typically the node is a personal computer (PC).

client/server computing
Architectural model that functionally divides that execution of a unit of work between activities initiated by an end user or program (client) and those maintaining data (servers). Originally thought to make mainframes obsolete.

cluster
A group of processors interconnected by a high-speed network (typically dedicated) for increased reliability and scalability. Clusters are groupings of multiple servers in which information is shared among systems. When a server in a cluster fails, one of the other servers in the cluster assumes the responsibility of the failed server, thereby ensuring server, application, and data availability.

community name (SNMP)
A name that represents an simple network management protocol (SNMP) community that the agent software recognizes as a valid source for SNMP requests. A product recognizes a management station as a valid recipient for trap information when the station's community names are configured.

community profile
Information that specifies which management objects are available to what management domain or simple network management protocol (SNMP) community name.

community (SNMP)
A relationship between an simple network management protocol (SNMP) agent and a set of SNMP managers that defines authentication, access control, and proxy characteristics.

concurrent firmware upgrade
Firmware is upgraded without disrupting switch operation.

configuration data
The collection of data that results from configuring product and system operating parameters. For example, configuring operating parameters, simple network management protocol (SNMP) agent, zoning configurations, and port configurations through the Product Manager application, results in a collection of configuration data. Configuration data includes: identification data, port configuration data, operating parameters, simple network management protocol (SNMP) configuration, and zoning configuration.

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

connectivity
The ability of devices to link together.

connectivity attribute
In S/390 mode, the characteristic that determines port address status for the Director or Switch. See also blocked connection; connectivity capability; connectivity control; dynamic connection; dynamic connectivity; unblocked connection.

connectivity capability
(1) The capability that allows attachment of a device to a system without requiring physical reconfiguration of either the device or the interconnections. (2) The Director or Switch capability that allows logical manipulation of link connections to provide physical device attachment (D). See also active port address matrix; connectivity attribute; connectivity control.

connectivity control
In S/390 mode, in a Director or Switch, the method used to change port address connectivity attributes and determine the communication capability of the link attached to the port (D). See also active port address matrix; connectivity attribute; connectivity capability.

control processor card
CTP card. Circuit card that contains the Director or Switch microprocessor. The CTP card also initializes hardware components of the system after power-on. The card may contain an RJ-45 twisted pair connector.

credit
See buffer-to-buffer credit (buffer-to-buffer credit).

CTP card
See control processor card.

customer support
Synonym for technical support.

data center
A collection of servers and data storage devices, usually in one location, administered by an information technology/information services (IT/IS) manager.

default
Pertaining to an attribute, value, or option that is assumed by a system when none is explicitly specified (D, I).

default zone
A zone that contains all attached devices that are not members of a separate active zone.

destination
A point or location, such as a processor, Director or Switch, or server, to which data is transmitted (D).

destination address
D_ID. An address identifier that indicates the targeted destination of a data frame.

device
(1) Mechanical, electrical, or electronic hardware with a specific purpose (D). See also managed product.

(2) See node.

device number
In a channel subsystem, four hexadecimal digits that uniquely identify an I/O device (D).

diagnostics
(1) The process of investigating the cause or nature of a problem in a product or system. (2) Procedures or tests used by computer users and service personnel to diagnose hardware or software problems (D).

dialog box
A pop-up window in the user interface with informational messages or fields to be modified or completed with desired options.

D_ID
See destination address.

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

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

domain
A Fibre Channel term describing the most significant byte in the node port (N_Port) identifier for the Fibre Channel device. It is not used in the Fibre Channel small computer system interface (FC-SCSI) hardware path ID. It is required to be the same for all SCSI targets logically connected to a Fibre Channel adapter.

domain ID
Domain identifier. A number that uniquely identifies a switch in a multiswitch fabric. A distinct domain ID is automatically allocated to each switch in the fabric by the principal switch. The preferred domain ID is the domain ID value that a switch requests from the principal switch. If the value has not been allocated to another switch in the fabric, it will be granted by the principal switch and will become the requesting switch's active domain ID. The active domain ID is the domain ID that has been assigned by the principal switch and that a switch is currently using.

domain name server
In TCP/IP, a server program that supplies name-to-address translation by mapping domain name to internet addresses. (D)

DRAM
See dynamic random access memory.

drop-down menu
A menu that displays when a heading in a navigation bar is clicked on with the mouse. The objects that display in the drop-down menus are organized by their headings in the navigation bar.

dump
The file that is created when the Director detects a software fault. It contains various data fields that, when extracted, assist in the debugging of software.

dynamic connection
A connection between two ports, established or removed by the Directors and that, when active, displays as one continuous link. See also connectivity attribute. See also blocked connection; connectivity capability; dynamic connectivity; unblocked connection.

dynamic connectivity
The capability that allows connections to be established and removed at any time.

dynamic random access memory
DRAM. Random access memory that resides in a cell comprised of a capacitor and transistor. DRAM data deteriorates (that is, is dynamic) unless the capacitor is periodically recharged by the controlling microprocessor. DRAM is slow, but relatively inexpensive (D). Contrast with static random access memory.

E_D_TOV
See error-detect time-out value (error-detect time-out value).

EIA
See Electronic Industries Association.

Electronic Industries Association
EIA. The governing body that publishes recommended standards for physical devices and associated interfaces. For example, RS-232 is the EIA standard that defines computer serial port connectivity (D). See also Telecommunications Industry Association.

electronic mail
E-mail. Any communications service that permits the electronic transmission and storage of messages and attached or enclosed files.

e-mail
See electronic mail.

Embedded Web Server interface
The interface provides a graphical user interface (GUI) similar to the Product Manager application, and supports Director or Switch configuration, statistics monitoring, and basic operations. With Director or Switch firmware installed, administrators or operators with a browser-capable personal computer (PC) and an Internet connection can monitor and manage the Director or Switch through an Embedded Web Server interface.

Embedded Web Server interface timeout
If the Embedded Web Server interface is running but no user activity occurs, (such as viewing different pages, refreshing, or reconfiguring information), the application times out after 30 minutes. The user must log in again. A login dialog box displays if the user attempts to access any pages after the timeout has occurred.

Embedded Web Server interface window
The window for the Embedded Web Server interface. The window is divided into two separate panels: the navigation panel on the left, and the main panel on the right.

enhanced availability feature
EAF. A backup field-replaceable unit (backup FRU) that is ordered and installed to provide redundancy and reduce disruption in case of failure.

enterprise
The entire storage system. The series of computers employed largely in high-volume and multi-user environments such as servers or networking applications; may include single-user workstations required in demanding design, engineering and audio/visual applications.

Enterprise Systems Architecture
ESA™. A computer architecture introduced by IBM in 1988 as ESA/370. The architecture added access registers to improve virtual memory management and increase storage from 2 gigabyte to 6 terabytes. The architecture was enhanced with the introduction of ESA/390 in 1990 (D).

Enterprise Systems Connection
ESCON™. An IBM architecture, technology, and set of products and services introduced in 1990 that provides a dynamically connected environment using fiber-optic cables as the data transmission medium (D).

Enterprise Systems Connection Director
ESCON™ Director. A device that provides connectivity capability and control for attaching any two links to each other through the ESON channel. Specifically, any of the hardware devices provided for interconnecting IBM-compatible mainframe equipment through the proprietary ESCON channel connection. IBM's model numbers for ESCON Directors include the 9031 and 9033.

E_Port
See expansion port.

erase
To remove electrically or magnetically stored data, leaving the space where the data was stored unoccupied (D).

error-detect time-out value
E_D_TOV. The time the switch waits for an expected response before declaring an error condition.

error log
See Event Log.

error message
Indication that an error has been detected (D). See also information message; warning message.

ESA™
See Enterprise Systems Architecture.

ESCON™
See Enterprise Systems Connection.

Ethernet
A widely implemented local area network (LAN) protocol that uses a bus or star topology and serves as the basis for the Institute of Electrical and Electronics Engineers (IEEE) 802.3 standard, which specifies the physical and software layers.

Ethernet hub
A device used to connect the HAFM server and the Directors it manages.

event code
A three-digit number that specifies the exact event that occurred. This code provides information on system failures, such as hardware failures, failure locations, or general information on normal system events.

Event Log
Record of significant events that have occurred on the Director or Switch (Director or Switch Event Log) or through the *HAFM Management Services* application (HAFM Event Log). There are two Event Logs: Director or Switch Event Log, and HAFM Event Log.

(1) Director or switch Event Log. Log displayed through the *Product Manager* application that provides a history of events for an individual Director or Switch, such as system events, degraded operation, FRU failures, FRU removals and replacements, port problems, Fibre Channel link incidents, and HAFM server-to-product communication problems. All detected software and hardware failures are recorded in the Event Log. The information is useful to maintenance personnel for fault isolation and repair verification.

exchange
A term that refers to one of the Fibre Channel protocol "building blocks," composed of one or more nonconcurrent sequences.

expansion port
E_Port. Physical interface on a Fibre Channel switch within a fabric, that attaches to an E_Port on another Fibre Channel switch through an interswitch link (ISL) to form a multiswitch fabric. See also fabric loop port; fabric port; generic port; hub port; node loop port; node port; segmented expansion port.

extended distance feature
XDF. A means to extend the propagation distance of a fiber-optic signal.

fabric
Entity that interconnects node ports (N_Ports) and is capable of routing (switching) Fibre Channel frames, using the destination ID information in the Fibre Channel frame header accompanying the frames. A switch is the smallest entity that can function as a complete switched fabric topology.

fabric element
Any active Director, Switch, or node in a switched fabric.

fabric loop port
FL_Port. A fabric port (F_Port) that contains arbitrated loop (AL) functions associated with the Fibre Channel arbitrated loop (FC-AL) topology. The access point of the fabric for physically connecting an arbitrated loop of node loop ports (NL_Ports). See also expansion port; fabric port; generic port; hub port; node loop port; node port; segmented expansion port.

Fabric Manager application
Fabric Manager is a High Availability Fabric Manager (HAFM) application used for controlling and managing fabrics. The Fabric Manager contains two views: the Topology view and the Zoning view. Menu options and displays in these views enable the user to manage and monitor the selected fabric, whether it is a single-switch or multiswitch fabric.

fabric mode
See interoperability mode.

fabric port
F_Port. Physical interface within the fabric that connects to a node port (N_Port) through a point-to-point full duplex connection. See also expansion port; fabric loop port; generic port; hub port; node loop port; node port; segmented expansion port.

fabric services
The services that implement the various Fibre Channel protocol services that are described in the standards. These services include the fabric controller (login server), name server, and management server.

fabric switches
A device which allows the communication between multiple devices using Fibre Channel protocols. A fabric switch enables the sharing bandwidth and end-nodes using basic multiplexing techniques.

failover
Automatic and nondisruptive transition of functions from an active field-replaceable unit (FRU) that has failed to a backup FRU.

FC
See Fibre Channel.

FCA
See Fibre Channel Association.

FC-AL
See Fibre Channel arbitrated loop.

FC adapter
Fibre Channel adapter. See host bus adapter.

FCC
Federal Communications Commission.

FCIA
See Fibre Channel Industry Association.

FC IP
See Fibre Channel IP address.

feature key
A unique key to enable additional product features. This key is entered into the Configure Feature Key dialog box in the *Product Manager* application to activate optional hardware and software features. Upon purchasing a new feature, HP will provide the feature key to the customer.

fiber
The fiber-optic cable made from thin strands of glass through which data in the form of light pulses is transmitted. It is used for high-speed transmissions over medium (200 m) to long (10 km) distances.

fiber optics
The branch of optical technology concerned with the transmission of radiant power through fibers of transparent materials such as glass, fused silica, or plastic (E). Telecommunication applications of fiber optics use optical fibers. A single fiber or a nonspatially aligned fiber bundle is used for each information channel. Such fibers are often called optical fibers to differentiate them from fibers that are used in noncommunication applications (D).

fibre
A generic Fibre Channel term used to cover all transmission media types specified in the Fibre Channel Physical Layer (FC-PH) standard such as optical fiber, copper twisted pair, and copper coaxial cable.

Fibre Channel
FC. Integrated set of standards recognized by American National Standards Institute (ANSI) which defines specific protocols for flexible information transfer. Logically, a point-to-point serial data channel, structured for high performance.

Fibre Channel adapter
FC adapter. See host bus adapter.

Fibre Channel address
A 3-byte node port (N_Port) identifier which is unique within the address domain of a fabric. Each port may choose its own identifier, or the identifier may be assigned automatically during fabric login.

Fibre Channel arbitrated loop
FC-AL. A high-speed (100 Mbps) connection which is a true loop technology where ports use arbitration to establish a point-to-point circuit. Data can be transferred in both directions simultaneously, achieving a nominal transfer rate between two devices of 200 Mbps.

Fibre Channel Association
FCA. The FCA is a non-profit corporation consisting of over 150 members throughout the world. Its mission is to nurture and help develop the broadest market for Fibre Channel products through market development, education, standards monitoring, and fostering interoperability among members' products.

Fibre Channel fabric element
FCFE. Any device linked to a fabric.

Fibre Channel Industry Association
FCIA. A corporation consisting of over 100 computer industry-related companies. Its goal is to provide marketing support, exhibits, and trade shows for its member companies. The FCIA complements activities of the various standards committees.

Fibre Channel IP address
FC IP. The default FC IP on a new switch is a temporary number divided by the switch's World Wide Name (WWN). The system administrator needs to enter a valid IP address.

Fibre Channel standard
American National Standards Institute (ANSI) standard that provides a common, efficient data transport system that supports multiple protocols. The architecture integrates both channel and network technologies, and provides active, intelligent interconnection among devices. All data transmission is isolated from the control protocol, allowing use of point-to-point, arbitrated loop, or switched fabric topologies to meet the needs of an application.

Fibre Connection
FICON. An IBM set of products and services introduced in 1999 that is based on the Fibre Channel Standard. FICON technology uses fiber-optic cables as the data transmission medium, and significantly improves I/O performance (including one Gbps bi-directional data transfer). FICON is designed to coexist with ESCON™ channels, and FICON-to-ESCON control unit connections are supported.

fibre port module
FPM. A 1 gigabit-per-second module that contains four generic ports (G_Ports).

FICON
See Fibre Connection.

FICON Management server
An optional feature that can be enabled on the Director or Switch through the *Product Manager* application. When enabled, host control and management of the Director or Switch is provided through an S/390 Parallel Enterprise or 2/Series server attached to a Director or Switch or Switch port.

field-replaceable unit
FRU. Assembly removed and replaced in its entirety when any one of its components fails (D). See active field-replaceable unit.

file server
A computer that stores data centrally for network users and manages access to that data.

firmware
Embedded program code that resides and runs on, for example, Directors, Switches, and hubs.

FLASH memory
Reusable nonvolatile memory that is organized as segments for writing, and as bytes or words for reading. FLASH memory is faster than read-only memory, but slower than random access memory (D).

FL_Port
See fabric loop port.

FPM
See fibre port module.

F_Port
See fabric port.

frame
A variable-length packet of data that is transmitted in frame relay technology.

FRU
See field-replaceable unit.

gateway address
(1) In transmission control protocol/Internet protocol (TCP/IP), a device that connects two systems that use the same or different protocols. (2) In TCP/IP, the address of a router to which a device sends frames destined for addresses not on the same physical network (for example, not on the same Ethernet) as the sender. The hexadecimal format for the gateway address is XXX.XXX.XXX.XXX.

generic port
G_Port. Physical interface on a Director or Switch that can function either as a fabric port (F_Port) or an expansion port (E_Port), depending on the port type to which it connects. See also expansion port; fabric loop port; fabric port; hub port; node loop port; node port; segmented expansion port.

generic port module card
GPM card. A port card that implements four generic ports (G_Ports) and provides the physical connection point for links to Fibre Channel devices.

GPM card
See generic port module card.

G_Port
See generic port.

graphical user interface
GUI. A visually oriented interface where the user interacts with representations of real-world objects displayed on the computer screen. Interactions with such objects produce actions that are intuitive to the user (D).

GUI
See graphical user interface.

HAFM application
High Availability Fabric Manager (1) Software application that is the system management framework providing the user interface for managing HP Fibre Channel connectivity products. (2) The software application that implements the management user interface for all managed hardware products. The *HAFM* application can run both locally on the HAFM server and remotely on a user workstation.

HAFM server
High Availability Fabric Manager server. A laptop shipped with the product for the purpose of running the *High Availability Fabric Manager* application, *HAFM Product Manager* application, *HAFM Product Services* application, and *HAFM Management Services* applications.

hardware
Physical equipment (director, switch, or personal computer) as opposed to computer programs or software.

HBA
See host bus adapter.

Hertz
Hz. A unit of frequency equal to one cycle per second.

heterogeneous fabric
A fabric containing open-fabric-compliant products from various vendors. Contrast with homogeneous fabric.

high availability
A performance feature characterized by hardware component redundancy and concurrent maintenance. High-availability systems maximize system uptime while providing superior reliability, availability, and serviceability.

High Availability Fabric Management
The management scheme for HP products. This includes the HAFM server, *HAFM Manager* application, *HAFM Management Services* application, and all *Product Manager* applications and their associated services.

homogeneous fabric
A fabric consisting of only one vendor's products. Contrast with heterogeneous fabric.

hop
(1) Data transfer from one node to another node. (2) Describes the number of switches that handle a data frame from its origination point through it's destination point.

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

host
The computer that other computers and peripherals connect to.

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

hot spare
See field-replaceable unit.

H_Port
See hub port.

HTTP
See hypertext transport protocol.

hub
(1) In Fibre Channel protocol, a device that connects nodes into a logical loop by using a physical star topology. (2) In Ethernet, a device used to connect the HAFM server and the Directors it manages.

hub port
H_Port. In arbitrated loop devices, a port that uses arbitrated loop protocols. The physical interface that attaches to a loop device, either an end device or another loop interconnect device (hub).

hyperlink
A predefined link for jumping from one location to another, within the same computer or network site or even to a location at a completely different physical location. Commonly used on the world wide web for navigation, reference, and depth where published text will not suffice.

hypertext transport protocol
HTTP. A simple protocol that allows world wide web pages to be transferred quickly between web browsers and servers.

ID
See identifier.

identifier
ID. (1) One or more characters used to identify or name a data element and possibly to indicate certain properties of that data element (D, T). (2) A sequence of bits or characters that identifies a program, device, or system to another program, device, or system. See also port name.

IEEE
See Institute of Electrical and Electronics Engineers.

IML
See initial machine load.

inband management
Management of the Director or Switch through Fibre Channel. An interface connection to a port card. Contrast with out-of-band management(out-of-band management).

industry standard architecture
ISA. Bus architecture designed for personal computers (PCs) that use an Intel 80386, 80486, or Pentium microprocessor. ISA buses are 32 bits wide and support multiprocessing.

Infiniband
The name applied to the merged specifications for Next Generation Input Output (NCGIO) from Intel and System IO from Compaq, HP, and IBM. Infiniband is a serial interconnect technology with a wire/fiber data speed of 2.5 GB. The basic Infiniband is a full-duplex dual wire/fiber.

information message
Message notifying a user that a function is performing normally or has completed normally. See also error message; warning message.

information services
IS. IS is the name of the department responsible for computers, networking, and data management. See also information technology.

information technology
IT. The broad subject concerned with all aspects of managing and processing information, especially within a large organization or company. Because computers are central to information management, computer departments within companies and universities are often called IT departments. See also information services.

initial machine load
IML. Hardware reset for all installed control processor (CTP) cards on the Director or Switch. This reset does not affect other hardware. It is initiated by pushing the IML button on a Director's or Switch's operating panel.

initial program load
IPL. The process of initializing the device and causing the operating system to start. An IPL may be initiated through a menu option or a hardware button.

initial program load configuration
IPL configuration. In S/390 mode, information stored in a Director or Switch's nonvolatile memory that contains default configurations. The Director or Switch loads the file for operation when powered on.

input/output
I/O. (1) Pertaining to a device whose parts can perform an input process and an output process at the same time (I). (2) Pertaining to a functional unit or channel involved in an input process, output process, or both, concurrently or not, and to the data involved in such a process. (3) Pertaining to input, output, or both (D). (4) An operation or device that allows input and output.

Institute of Electrical and Electronics Engineers
IEEE. An organization of engineers and technical professionals that promotes the development and application of electronic technology and allied sciences.

interface
(1) A shared boundary between two functional units, defined by functional, signal, or other characteristics. The concept includes the specification of the connection of two devices having different functions (T). (2) Hardware, software, or both, that link systems, programs, or devices (D).

interface controller
The chip or circuit that translates computer data and commands into a form suitable for use by the hard drive and controls the transfer of data between the buffer and the host.

Internet protocol
IP. Network layer for the transmission control protocol/Internet protocol (TCP/IP) protocol used on Ethernet networks. IP provides packet routing, fragmentation, and reassembly through the data link layer (D).

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

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

interoperability mode
Interop mode. An operating mode set through management software that allows products to operate in homogeneous or heterogeneous fabrics.

interop mode
See interoperability mode.

interswitch link
ISL. Physical expansion port (E_Port) connection between two Directors in a fabric.

interswitch link hop
ISL hop. See hop.

intranet
A private version of the Internet that provides a cost-effective way to publicize critical information and that provides an interactive communication path for heterogeneous systems. Internal to a specific organizational structure and secured from or disconnected from the global Internet.

I/O
See input/output.

IP
See Internet protocol.

IP address
See Internet protocol address.

IPL
See initial program load.

IPL configuration
See initial program load configuration.

IS
See information services.

ISL
See interswitch link.

ISL hop
Interswitch link hop. See hop.

isolated E_Port
Isolated expansion port. See segmented expansion port

isolated expansion port
Isolated E_Port. See segmented expansion port.

laser
Laser is an acronym for light amplification by stimulated emission of radiation. A device that produces a very powerful narrow beam of coherent light of a single wavelength by simulating the emissions of photons from atoms, molecules, or ions.

latency
Amount of time elapsed between receipt of a data transmission at a switch's incoming fabric port (F_Port) from the originating node port (N_Port) to retransmission of that data at the switch's outgoing F_Port to the destination N_Port. The amount of time it takes for data transmission to pass through a switching device.

LED
See light-emitting diode(light-emitting diode).

light-emitting diode
LED. A semiconductor chip that emits visible or infrared light when electricity passes through it. LEDs are used on Switch or Director field-replaceable units (FRUs) and the front bezel to provide visual indications of hardware status or malfunctions.

LIN
See link incident.

link
Physical connection between two devices on a switched fabric. A link consists of two conductors, one used for sending and the other for receiving, thereby providing a duplex communication path.

link incident
LIN. Interruption to link due to loss of light or other causes. See also link incident alerts.

link incident alerts
A user notification, such as a graphic symbol in the *Product Manager* application Hardware view that indicates that a link incident has occurred. See also link incident.

LIP
See loop initialization primitive.

load balancing
Ability to evenly distribute traffic over multiple interswitch links within a fabric. Load balancing on HP Directors and Switches takes place automatically.

local
Synonym for channel-attached.

local area network
LAN. A computer network in a localized geographical area (for example, a building or campus), whose communications technology provides a high-bandwidth medium to which many nodes are connected (D). See also storage area network; wide area network.

logical unit number
LUN. In Fibre Channel addressing, a logical unit number is a number assigned to a storage device which, in combination with the storage device's node port's World Wide Name represents a unique identifier for a logical device on a storage area network. Peripherals use LUNs to represent addresses. A small computer system interface (SCSI) device's address can have up to eight LUNs.

login server
Entity within the Fibre Channel fabric that receives and responds to login requests.

loop
A loop is a configuration of devices connected to the fabric via a fabric loop port (FL_Port) interface card.

loop address
In Fibre Channel protocol, a term indicating the unique ID of a node in Fibre Channel loop topology, sometimes referred to as a loop ID.

loopback plug
In a fiber optic environment, a type of duplex connector used to wrap the optical output signal of a device directly to the optical input. Contrast with protective plug. Synonymous with wrap plug.

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

loop initialization primitive
LIP. In an arbitrated loop device, a process by which devices connected to hub ports (H_Ports) on the arbitrated loop device notify other devices and the switch of the presence in the loop by sending LIP sequences and subsequent frames through the loop. This process allows linked arbitrated loop devices to perform fabric loop port (FL_Port) arbitration as they link through hub ports.

loop master
In an arbitrated loop device, a reference to the loop master World Wide Name (WWN) field in the Loop view, the loop master is the arbitrated loop device that is responsible for allocating arbitrated loop physical addresses (AL-PAs) on the loop. An arbitrated loop device becomes the loop master through arbitration when there are multiple arbitrated loop devices on the loop. The arbitrated loop device with the lowest WWN becomes the loop master.

loop port
L_Port. Synonym for hub port.

loop switches
Loop switches support node loop port (NL_Port) Fibre Channel protocols. Switches sold as loop support but upgradeable to fabric switches recounted as loop switches.

L_Port
Loop port. Synonym for hub port.

LUN
See logical unit number.

maintenance port
Connector on the Director or Switch where a PC running an American National Standard Code for Information Interchange (ASCII) terminal emulator can be attached or dial-up connection made for specialized maintenance support.

managed product
Hardware product that can be managed with the *HAFM Product Manager* application. HP Directors and Switches are managed products. See also device(device).

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

management session
A session that exists when a user logs on to the *HAFM* application. HAFM can support multiple concurrent management sessions. The user must specify the network address of the *HAFM* application's server at logon time.

matrix
See active port address matrix.

MIB
See management information base.

modem
Modem is an abbreviation for modulator/demodulator. A communication device that converts digital computer data to signals and signals to computer data. These signals can be received or transmitted by the modem via a phone line or other method of telecommunication.

multimedia
A simultaneous presentation of data in more than one form, such as by means of both visual and audio.

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

name server
(1) In TCP/IP, see domain name server. (2) In Fibre Channel protocol, a server that allows node ports (N_Ports) to register information about themselves. This information allows N_Ports to discover and learn about each other by sending queries to the name server.

name server zoning
Node port (N_Port) access management that allows N_Ports to communicate if and only if they belong to a common name server zone.

navigation panel
The left side of the Embedded Web Server interface window. Click words in this panel to display menu options.

network address
Name or address that identifies a device on a transmission control protocol/Internet protocol (TCP/IP) network. The network address can be either an IP address in dotted-decimal notation (composed of four three-digit octets in the format xxx.xxx.xxx.xxx) or a domain name (as administered on a customer network).

network-attached storage
NAS. Storage connected directly to the network, through a processor and its own operating system. Lacks the processor power to run centralized, shared applications.

network management
The broad subject of managing computer networks. There exists a wide variety of software and hardware products that help network system administrators manage a network. Network management covers a wide area, including security, performance, and reliability.

nickname
Alternate name assigned to a World Wide Name for a node, Director or Switch in the fabric.

NL_Port
See node loop port.

node
In Fibre Channel protocol, an end device (server or storage device) that is or can be connected to a switched fabric. See also device.

node loop port
NL_Port. A physical interface within an end device (node) that participates in a loop containing one or more fabric loop ports (FL_Ports) or other NL_Ports. See also expansion port; fabric loop port; fabric port; generic port; hub port; node port; segmented expansion port.

node port
N_Port. Physical interface within an end device that can connect to an fabric port (F_Port) on a switched fabric or directly to another N_Port (in point-to-point communications). See also expansion port; fabric loop port; fabric port; generic port; hub port; node loop port; segmented expansion port.

node port identifier
N_Port ID. In Fibre Channel protocol, a unique address identifier by which an N_Port is uniquely known. It consists of a domain (most significant byte), an area, and a port, each 1 byte long. The N_Port ID is used in the source identifier (S_ID) and destination identifier (D_ID) fields of a Fibre Channel frame.

nonvolatile random access memory
NV-RAM. RAM that retains its content when the device power is turned off.

N_Port
See node port.

N_Port ID
See node port identifier.

NV-RAM
See nonvolatile random access memory.

OEM
See original equipment manufacturer.

offline
Referring to data stored on a medium, such as tape or even paper, that is not available immediately to the user.

offline diagnostics
Diagnostics that only operate in stand alone mode. User operations cannot take place with offline diagnostics running.

offline sequence
OLS. (1) Sequence sent by the transmitting port to indicate that it is attempting to initialize a link and has detected a problem in doing so. (2) Sequence sent by the transmitting port to indicate that it is offline.

offline state
When the Switch or Director is in the offline state, all the installed ports are offline. The ports transmit an offline sequence (OLS) and they cannot accept a login got connection from an attached device. Contrast with online state.

OLS
See offline sequence.

online
Referring to data stored on the system so it is available immediately to the user.

online diagnostics
Diagnostics that can be run by the customer engineer while the operational software is running. These diagnostics do not impact user operations.

online state
When the Switch or Director is in the online state, all of the unblocked ports are allowed to log in to the fabric and begin communicating. Devices can connect to the Switch or Director if the port is not blocked and can communicate with another attached device if both devices are in the same zone, or if the default zone is enabled. Contrast with offline state.

Open Systems Architecture
OSI. A model that represents a network as a hierarchical structure of functional layers. Each layer provides a set of functions that can be accessed and used by the layer above. Layers are independent, in that implementation of a layer can be changed without affecting other layers (D).

open systems management server
OSMS. An optional feature that can be enabled on the Director or Switch through the *Product Manager* application. When enabled, host control and management of the Director or Switch are provided through an Open System Interconnection (OSI) device attached to a Director or Switch port.

open systems mode
The mode that is used for HP or open fabrics. See also operating mode; S/390 mode(S/390 mode).

operating mode
In Directors or Switches, in managed products, a selection between S/390 and open systems mode. See also open systems mode; S/390 mode.

operating system
OS. Software that controls execution of applications and provides services such as resource allocation, scheduling, I/O control, and data management. Most operating systems are predominantly software, but partial hardware implementations are possible (D, T).

Operating System/390
OS/390™. An integrated, open-enterprise server operating system developed by IBM that incorporates a leading-edge and open communications server, distributed data and file services, parallel Sysplex support, object-oriented programming, distributed computing environment, and open application interfaces (D).

original equipment manufacturer
OEM. A company that has a special relationship with computer producers. OEMs buy components and customize them for a particular application. They sell the customized computer under their own name. OEMs may not actually be the original manufacturers. They are usually the customizers and marketers.

See operating system.

OS/390™
See Operating System/390.

OSI
See Open Systems Architecture.

OSMS
See open systems management server.

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

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

panel
A logical component of the interface window. Typically, a heading and/or frame marks the panel as an individual entity of the window. Size and shape of the panel and its data depend upon the purpose of the panel and may or may not be modified.

persistent binding
A form of server-level access control that uses configuration information to bind a server to a specific Fibre Channel storage volume (or logical device), using a unit number. See also access control.

point-to-point
A Fibre Channel protocol topology that provides a single, direct connection between two communication ports. The Director or Switch supports only point-to-point topology. See also arbitrated loop.

port
Receptacle on a device to which a cable leading to another device can be attached. Ports provide Fibre Channel connections (D).

port address name
A user-defined symbolic name of 24 characters or less that identifies a particular port address.

port authorization
Feature of the password definition function that allows an administrator to extend operator-level passwords to specific port addresses for each Director or Switch definition managed by a personal computer (PC). Port authorization affects only operator-level actions for active and saved matrices (D).

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 port numbers and port card slot numbers inside a hardware cabinet.

port name
Name that the user assigns to a particular port through the *Product Manager* application. See also identifier. Synonymous with address name.

preferred domain ID
Configured value that a switch will request from the Principal Switch. If the preferred value is already in use, the Principal Switch will assign a different value.

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

private device
A loop device that cannot transmit a fabric login command (FLOGI) command to a Switch or Director, nor communicate with fabric-attached devices. Contrast with public device.

private loop
A private loop is not connected to a switched fabric, and the switch's embedded expansion port (E_Port) and fabric loop port (FL_Port) are inactive. All devices attached to the loop can only communicate with each other. Contrast with public loop.

Product Manager application
Application that implements the management user interface for a Director or Switch. There are two *Product Manager* applications: Director or Switch Product Manager, and HAFM Product Manager. (1) In the *HAFM Management Services* application, the software component that provides a graphical user interface for managing and monitoring HAFM products. When a product instance is opened from the *HAFM* application Product view or Fabric Manager Topology view, the corresponding *HAFM Product Manager* application is invoked.

product name
User-configurable identifier assigned to a managed product. Typically, this name is stored on the product itself. A Director or Switch product name can also be accessed by a simple network management protocol (SNMP) manager as the system name.

prohibited port connection
In a Director or Switch, in S/390 operating mode, an attribute that removes dynamic connectivity capability.

proprietary
Privately owned and controlled. In the computer industry, proprietary is the opposite of open. A proprietary design or technique is one that is owned by a company. It also implies that the company has not divulged specifications that would allow other companies to duplicate the product. Increasingly, proprietary architectures are seen as a disadvantage. Consumers prefer open and standardized architectures, which allow them to mix and match products from different manufacturers.

protective plug
In a fiber-optic environment, a type of duplex connector (or cover) that provides physical protection (D). Contrast with loopback plug.

protocol
(1) Set of semantic and syntactic rules that determines the behavior of functional units in achieving communication. (2) In systems network architecture, the meanings of and sequencing rules for requests and responses for managing the network, transferring data, and synchronizing network component states. (3) A specification for the format and relative timing of data exchanged between communicating devices (D, I).

public device
A loop device that can transmit a fabric login command (FLOGI) to a switch, receive acknowledgement from the switch's login server, register with the switch's name server, and communicate with fabric-attached devices. Public devices communicate with fabric-attached devices through the switch's bridge port (B_Port) connection to a Director or Switch. Contrast with private device.

public loop
A public loop is connected to a switched fabric (through the switch bridge port (B_Port)), and the switch has an active embedded fabric loop port (FL_Port) that is user transparent. All devices attached to the loop can communicate with each other, and public devices attached to the loop can communicate with fabric-attached devices. Contrast with private loop.

pull-down menu
See drop-down menu.

RAID
See redundant array of independent disks.

RAM
See random access memory.

random access memory
RAM. A group of computer memory locations that is numerically identified to allow high-speed access by the controlling microprocessor. A memory location is randomly accessed by referring to its numerical identifier (D). Contrast with redundancy. See also dynamic random access memory; nonvolatile random access memory; static random access memory.

R_A_TOV
See resource allocation time-out value.

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

redundant array of independent disks
RAID. Grouping of hard drives in a single system to provide greater performance and data integrity. RAID systems have features that ensure data stored on the drives are safe and quickly retrievable.

remote notification
A process by which a system is able to inform remote users and workstations of certain classes of events that occur on the system. E-mail notification and the configuration of simple network management protocol (SNMP) trap recipients are two examples of remote notification programs that can be implemented on director-class switches.

remote user workstation
Workstation, such as a personal computer (PC), using *HAFM* application and *Product Manager* application software that can access the HAFM server over a local area network (LAN) connection.

rerouting delay
An option that ensures that frames are delivered in order through the fabric to their destination.

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

ring topology
A logically circular, unidirectional transmission path without defined ends, in which control is distributed or centralized (D). See also token ring.

RS-232
The Electronic Industry Association (EIA)-recommended specification for asynchronous serial interfaces between computers and communications equipment. It specifies both the number of pins and type of connection, but does not specify the electrical signals (D).

S/390 mode
The mode that is most useful when attaching to IBM S/390 Enterprise servers. See also open systems mode; operating mode.

SAN
See storage area network; system area network.

SBAR
See serial crossbar assembly.

scalable
Refers to how well a system can adapt to increased demands. For example, a scalable network system could start with just a few nodes but easily expands to thousands of nodes. Scalability is important because it allows the user to invest in a system with confidence that a business will not outgrow it. Refers to anything whose size can be changed.

SCSI
See small computer system interface.

segment
A fabric segments when one or more switches cannot join the fabric because of various reasons. The switch or switches remain as separate fabrics.

segmented E_Port
See segmented expansion port.

segmented expansion port
Segmented E_Port. E_Port that has ceased to function as an E_Port within a multiswitch fabric due to an incompatibility between the fabrics that it joins. See also fabric loop port; fabric port; generic port; hub port; node loop port; node port.

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

serial port
A full-duplex channel that sends and receives data at the same time. It consists of three wires: two that move data one bit at a time in opposite directions, and a third wire that is a common signal ground wire.

server
A computer that provides shared resources, such as files and printers, to the network. Used primarily to store data, providing access to shared resources. Usually contains a network operating system.

shared mode
If a Director or Switch is in shared mode, all devices on the loop share the 100MB bandwidth available on the loop. In shared mode, only one end device can communicate with another device through the fabric loop port (FL_Port) on the Director or Switch.

simple mail transfer protocol
SMTP. A transmission control protocol/Internet protocol (TCP/IP) protocol that allows the user to create, send, and receive text messages. SMTP protocols specify how messages are passed across a link from one system to another. They do not specify how the mail application accepts, presents, or stores the mail.

simple network management protocol
SNMP. A transmission control protocol/Internet protocol (TCP/IP)-derived protocol governing network management and monitoring of network devices.

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

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

simple network management protocol management station
SNMP management station. An SNMP workstation personal computer (PC) used to oversee the SNMP network.

simple network management protocol version 1
SNMP v1. The original standard for SNMP is now referred to as SNMP v1.

simple network management protocol version 2
SNMP v2. The second version of the SNMP standard. This version expands the functionality of SNMP and broadens its ability to include OSI-based, as well as TCP/IP-based, networks as specified in RFC 1441 through 1452.

small computer system interface
SCSI. An interface standard that enables computers to communicate with peripherals connected to them. Commonly used in enterprise computing and in Apple Macintosh systems. Usually pronounced as "scuzzy." The equivalent interface in most personal computers is enhanced integrated drive electronics (EIDE).

A narrow SCSI adapter supports up to eight devices, including itself. SCSI address 7 has the highest priority followed by 6, 5, 4, 3, 2, 1, 0, with 0 being the lowest priority.

SNMP
See simple network management protocol.

SNMP community
See simple network management protocol community.

SNMP community name
See simple network management protocol community name.

SNMP management station
See simple network management protocol management station.

SNMP v1
See simple network management protocol version 1.

SNMP v2
See simple network management protocol version 2.

SRAM
See static random access memory.

SSP
See system services processor.

state
The state of the Switch or Director. Possible values include online, offline, testing, and faulty. See also offline state; online state

static random access memory
SRAM. SRAM is microprocessor-cache random access memory. It is built internal to the microprocessor or on external chips. SRAM is fast, but relatively expensive (D). Contrast with dynamic random access memory.

storage area network
SAN. A high-performance data communications environment that interconnects computing and storage resources so that the resources can be effectively shared and consolidated. See also local area network; wide area network.

stored addresses
In S/390 mode, a method for configuring addresses.

subnet
A portion of a network that shares a common address component. On transmission control protocol/Internet protocol (TCP/IP) networks, subnets are defined as all devices whose IP addresses have the same prefix. Dividing a network into subnets is useful for both security and performance reasons. IP networks are divided using a subnet mask.

subnet mask
A mask used by a computer to determine whether another computer with which it needs to communicate is located on a local or remote network. The network mask depends upon the class of networks to which the computer is connecting. The mask indicates which digits to look at in a longer network address and allows the router to avoid handling the entire address. Subnet masking allows routers to move the packets more quickly. Typically, a subnet may represent all the machines at one geographic location, in one building, or on the same local area network.

switch
A device that connects, filters and forwards packets between local area network (LAN) segments or storage area network (SAN) nodes or devices.

switched mode
If the arbitrated loop device is in switched mode, each pair of communicating ports on the arbitrated loop device can share the 100MB bandwidth. In switched mode, up to three pairs of loop devices can communicate with each other simultaneously. Or, a public device on the loop can communicate with another device on the fabric while up to two pairs of loop devices can communicate simultaneously.

switchover
Changing a backup field-replaceable unit (FRU) to the active state, and the active FRU to the backup state.

switch priority
Value configured into each switch in a fabric that determines its relative likelihood of becoming the fabric's principal switch. Lower values indicate higher likelihood of becoming the principal switch. A value of 1 indicates the highest priority; 225 is the lowest priority. A value of 225 indicates that the switch is not capable of acting as the principal switch. The value 0 is illegal.

system name
See product name.

system services processor
SSP. In a Director or Switch, the central controlling processor. Controls the RS-232 maintenance port and the Ethernet port of a Fibre Channel Director or Switch.

TCP
See transmission control protocol.

TCP/IP
See transmission control protocol/Internet protocol.

technical support
Single point of contact for a customer when assistance is needed in managing or troubleshooting a product. Technical support provides assistance twenty-four hours a day, seven days a week, including holidays. The technical support number is (800) 752-4572 or (720) 566-3910. Synonymous with customer support.

Telecommunications Industry Association
TIA. A member organization of the Electronic Industries Association (EIA), TIA is the trade group representing the communications and information technology industries. See also Electronic Industries Association.

telnet
The Internet standard protocol for remote terminal connection over a network connection.

terabyte
TB. One thousand (1,000) gigabytes; one terabyte of text on paper would consume 42,500 trees. At 12 characters per inch, 1 TB of data in a straight line would encircle the earth 56 times and stretch some 1.4 million miles equalling nearly three round trips from the earth to the moon.

TIA
See Telecommunications Industry Association.

token
A sequence of bits passed from one device to another on a token ring network that signifies permission to transmit over the network. The token consists of a starting delimiter, access control field, and end delimiter. If a device has data to transmit, it appends the data to the token (D).

token ring
A local area network (LAN) configuration where devices attach to a network cable in a closed path or ring. A token (unique sequence of bits) circulates on the ring to allow devices to access the LAN for data transmission (D). See also ring topology.

token ring controller adapter card
TKRG. The circuit card that provides a port to connect a Director or Switch to a 4/16 Mbps token ring local area network (LAN) (D).

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

transceiver modules
Transceiver modules come in longwave, extra longwave, or shortwave laser versions, providing a single fiber connection.

transfer rate
The speed with which data can be transmitted from one device to another. Data rates are often measures in megabits (Mbps) or megabytes (MBps) per second, or gigabits (Gbps) or gigabytes per second (GBps).

transmission control protocol
TCP. The transport layer for the transmission control protocol/Internet protocol (TCP/IP) protocol widely used on Ethernet networks and any network that conforms to U.S. Department of Defense standards for network protocol. TCP provides reliable communication and control through full-duplex connections (D).

transmission control protocol/Internet protocol
TCP/IP. A layered set of protocols (network and transport) that allows sharing of applications among devices on a high-speed local area network (LAN) communication environment (D). See also transmission control protocol; Internet protocol.

trap
Unsolicited notification of an event originating from a simple network management protocol (SNMP) managed device and directed to an SNMP network management station.

trap host
Simple network management protocol (SNMP) management workstation that is configured to receive traps.

trap recipient
In simple network management protocol (SNMP), a network management station that receives messages through SNMP for specific events that occur on the arbitrated loop device.

UDP
See user datagram protocol.

UL
See Underwriters Laboratories.

unblocked connection
In a Director or Switch, the absence of the blocked attribute for a specific port. Contrast with blocked connection. See also connectivity attribute; dynamic connection; dynamic connectivity.

unblocked port
Devices communicating with an unblocked port can login to the Director or Switch and communicate with devices attached to any other unblocked port (assuming that this is supported by the current zoning configuration).

Underwriters Laboratories
UL. A laboratory organization accredited by the Occupational Safety and Health Administration and authorized to certify products for use in the home and workplace (D).

uniform resource locator
URL. A URL is the address of a document or other resource on the Internet.

uninterruptable power supply
UPS. A buffer between public utility power or another power source, and a system that requires precise, uninterrupted power (D).

universal port module
UPM. A flexible 1 gigabit-per-second or 2 gigabit-per-second module that contains four generic ports (G_Ports).

UNIX
A popular multi-user, multitasking operating system originally designed to be a small, flexible system used exclusively by programmers. UNIX was one of the first operating systems to be written in a high-level programming language, namely C. This meant that it could be installed on virtually any computer for which a C compiler existed. Due to its portability, flexibility, and power, UNIX has become the leading operating system for workstations. Historically, it has been less popular in the personal computer market, but the emergence of a new version called Linux is revitalizing UNIX across all platforms.

UPM
See universal port module.

UPS
See uninterruptable power supply.

URL
See uniform resource locator.

user datagram protocol
UDP. A connectionless protocol that runs on top of Internet protocol (IP) networks. User datagram protocol/Internet protocol (UDP/IP) offers very few error recovery services, instead providing a direct way to send and receive datagrams over an IP network. UDP/IP is primarily used for broadcasting messages over an entire network. Contrast with transmission control protocol/Internet protocol(transmission control protocol/Internet protocol).

vital product data
VPD. System-level data stored by field-replaceable units (FRUs) in the electrically erasable programmable read-only memory. This data includes serial numbers and identifies the manufacturer.

VPD
See vital product data.

warning message
A message that indicates a possible error has been detected. See also error message; information message.

wide area network
WAN. A network capable of transmission over large geographic areas that uses transmission lines provided by a common-carrier. See also local area network; storage area network.

window
The main window for the *HAFM* application or *Product Manager* applications. Each application has a unique window that is divided into separate panels for the title, navigation control, alerts, and the main or Product view. The user performs all management and monitoring functions for these Fibre Channel products through the application window.

Windows
A graphical user interface and windowing system introduced by Microsoft Corporation in 1985. Windows runs on top of the MS-DOS operating system (D).

workstation
A terminal or microcomputer usually connected to a network or mainframe at which a user can perform applications.

World Wide Name
WWN. Eight-byte string that uniquely identifies a Fibre Channel entity (that is, a port, a node, a switch, a fabric), even on global networks.

wrap plug
Synonym for loopback plug.

wrap test
A test that checks attachment or control unit circuitry, without checking the mechanism itself, by returning the output of the mechanism as input. A wrap test can transmit a specific character pattern through a system and compare the pattern received with the pattern transmitted (D).

write authorization
Permission for an simple network management protocol (SNMP) management station with the proper community name to modify writable management information base (MIB) variables.

WWN
See World Wide Name.

XDF
See extended distance feature.

zip drive
A high capacity floppy disk and disk drive developed by the Iomega Corporation. Zip disks are slightly larger than conventional floppy disks. The storage capacity for zip disks is between 100 and 250 MB of data. The zip drive and disk is used for backing up the HAFM server, and is located on the communications tray behind the HAFM server.

zone
Set of devices that can access one another. All connected devices may be configured into one or more zones. Devices in the same zone can see each other. Those devices that occupy different zones cannot. See also active zone set; zone set; zoning.

zone member
Specification of a device to be included in a zone. A zone member can be identified by the port number of the Director or Switch to which it is attached or by its port World Wide Name (WWN). In multiswitch fabrics, identification of end-devices or nodes by WWN is preferable.

zone set
A collection of zones that may be activated as a unit. See also active zone set; zone.

zoning
Grouping of several devices by function or by location. All devices connected to a connectivity product, such as the Director or Switch, may be configured into one or more zones. See also access control; zone.

Index

D

E

F

G

H

O

P

R

S

T

U

V

W

Z