Maintenance Menu Tasks

This chapter describes the Maintenance menu tasks of Element Manager and contains these sections:

Note The Maintenance menu provides opportunities to monitor your Server Switch and configure fundamental behavior.

Viewing Basic System Information

Basic system information includes the name of your device, the location of your device, and support resources.

To view basic system information, perform the following steps:

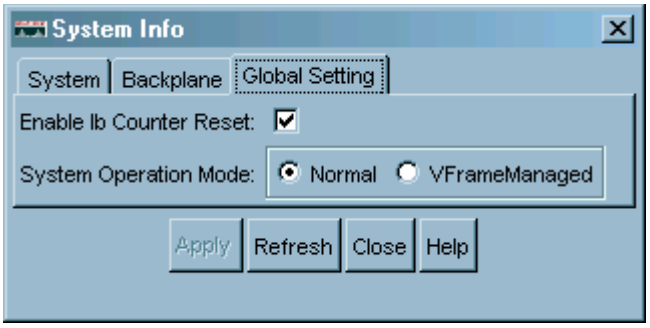
Step 1 Click the **Maintenance** menu and choose **System Info**. The System Info window opens. Table 5-1 lists and describes the fields in the window.

Table 5-1 System Info Window Fields

Element	Description
Description field	Description of the chassis and the image that runs on the chassis.
System Uptime field	Amount of time that the chassis has run since the last boot.
Last Change Made At field	Date and time that a user last changed the running configuration.
Last Config Saved At field	Date and time that a user last saved the running configuration as the startup configuration.
System Name field	Configurable name for your Server Switch.
Location field	Configurable location of your Server Switch.
Support Contact field	Configurable support information for your Server Switch.
Rack Locator UID field (select chassis)	Unique identifier (UID) for the Rack Locator test.
SystemSyncState field	Displays SFS-7008 system synchronization state information.

Step 2 Click the **Global Setting** tab to display the Global Settings shown in Figure 5-1.

Figure 5-1 Global Settings



Step 3 Table 5-2 lists and describes the fields in the Global Settings window.

Table 5-2 Global Settings Window Fields

Element	Description
Enable Ib Counter Reset:	When checked, resets the Enable Ib counter.
SystemOperMode field	Provides the Normal radio button for non-VFrame systems and the VFrameManaged radio button for systems in a VFrame environment. For more information, refer to VFrame documentation.

Configuring Basic System Information

Basic system information includes the name of your device, the location of your device, and support resources.

Naming Your InfiniBand Switch

To assign a hostname to your device, perform the following steps:

Step 1 Click the **Maintenance** menu and choose **System Info**. The System Info window opens.

Step 2 In the System Name field, type the name that you want to assign to the device, and then click the **Apply** button.

Defining Device Location

To add a physical device location description to your switch, perform the following steps:

Step 1 Click the **Maintenance** menu and choose **System Info**. The System Info window opens.

Step 2 In the Location field, type the name location of your device, and then click the **Apply** button.

Defining Technical Support Resource

The technical support e-mail address that you define appears in the System frame when you refresh or restart Element Manager. To define a technical support resource, perform the following steps:

Step 1 Click the **Maintenance** menu and choose **System Info**. The System Info window opens.

Step 2 In the Support Contact field, type the e-mail address of your technical support provider, and then click the **Apply** button.

Configuring SystemOperMode

Configure SystemOperMode status to alter the behavior of the Server Switch to respond appropriately to a VFrame environment or a non-VFrame environment. To configure SystemOperMode, perform the following steps:

Step 1 Click the **Maintenance** menu and choose **System Info**. The System Info window opens.

Step 2 In the SystemOperMode field, click one of the following radio buttons:

- Click **Normal** to configure the Server Switch for a non-VFrame environment.

– Click **VFrameManaged** to configure the Server Switch for a VFrame-managed environment.

Step 3 Click the **Apply** button.

Configuring Date and Time Properties

An internal clock runs on your device, but we recommend that you configure your device to access a network time protocol (NTP) server to synchronize your device with your network.

Configuring Date and Time

To configure the date and time of the internal clock on your device, perform the following steps:

Step 1 Click the **Maintenance** menu and choose **Time**. The Date and Time Properties window opens.

Step 2 In the Date field, enter the date in the *MM*/*DD*/*YY* format.

Step 3 In the Time field, enter the time in *HH*:*MM*:*SS* format, and then click the **Apply** button.

Step 4 Click the **Apply** button in the Date and Time partition.

Assigning NTP Servers

To configure your device to use an NTP server to synchronize your Server Switch with the network, perform the following steps:

Step 1 Click the **Maintenance** menu and choose **Time**. The Date and Time Properties window opens.

Step 2 In the NTP Server 1 field, enter the IP address of the NTP server that you want your Server Switch to use.

Step 3 (Optional) In the NTP Server 2 field, enter the IP address of the NTP server that you want your switch to use in the event that your switch cannot access the primary NTP server.

Step 4 (Optional) In the NTP Server 3 field, enter the IP address of the NTP server that you want your switch to use in the event that your switch cannot access the primary or secondary NTP servers.

Step 5 Click the **Apply** button in the NTP Servers partition.

Note When your device cannot access a NTP server, it defaults to the onboard clock.

Configuring Basic Services

You can configure basic services to facilitate remote access to your device.

Assigning a DNS Server

To assign a DNS server to your device, perform the following steps:

Step 1 Click the **Maintenance** menu and choose **Services**. The Services window opens.

Step 2 Click the **DNS** tab.

Step 3 In the Server 1 field, enter the IP address of the primary DNS server that you want to use.

Step 4 (Optional) In the Server 2 field, enter the IP address of the DNS server that you want to use if your device cannot access the primary DNS server.

Step 5 In the Domain field, enter the domain to which you want your switch to belong, and then click the **Apply** button.

Enabling or Disabling the FTP Access

To enable or disable FTP transfers to and from your device, perform the following steps:

Step 1 Click the **Maintenance** menu and choose **Services**. The Services window opens.

Step 2 Click the **FTP** tab.

Step 3 Check (to enable) or uncheck (to disable) the **Enable FTP Server** checkbox, and then click the **Apply** button.

Enabling or Disabling the Telnet Access

To enable or disable Telnet access to your device, perform the following steps:

Step 1 Click the **Maintenance** menu and choose **Services**. The Services window opens.

Step 2 Click the **Telnet** tab.

Step 3 Check (to enable) or uncheck (to disable) the **Enable Telnet Server** checkbox, and then click the **Apply** button.

Assigning a SYSLOG Server

Note This task assumes that you have already configured the host and connected it to the IB fabric.

To assign a syslog server to store logs from your device, perform the following steps:

Step 1 Click the **Maintenance** menu and choose **Services**. The Services window opens.

Step 2 Click the **Syslog** tab.

Step 3 In the Remote Syslog Server field, enter the IP address of the remote server to accept messages from your device, and then click the **Apply** button.

Assigning an Authentication Method

To assign an authentication method to your device, perform the following steps:

Step 1 Click the **Maintenance** menu and choose **Services**. The Services window opens.

Step 2 Click the **Radius** tab.

Step 3 In the Authentication Method field, click a radio button to choose a method, and then click the **Apply** button. Table 5-3 lists and describes the radio buttons that you can choose.

Table 5-3 CLI Authentication Methods

Button	Description
local	Authenticates user logins with the local CLI user database only.
localThenRadius	Authenticates user logins with the local CLI user database. Upon failure, authenticates with the RADIUS server.
radiusThenLocal	Authenticates user logins with the RADIUS server. Upon failure, authenticates with the local CLI user database.

Viewing RADIUS Servers

To view the RADIUS servers that you have configured your device to use to authenticate CLI and Element Manager logins, perform the following steps:

Step 1 Click the **Maintenance** menu and choose **Services**. The Services window opens.

Step 2 Click the **Radius Servers** tab. Table 5-4 lists and describes the fields in the Radius Servers table.

Table 5-4 Radius Server Properties Window Elements

Element	Description
Address field	Displays the IP address of the RADIUS server.
UDP Port field	UDP authentication port of the RADIUS server. Edit this value and click the **Apply** button to configure the UDP port of the RADIUS server. The numbers to the right of the field indicate the range of integer values that this field supports.
Encryption Key field	Authentication key that the client and RADIUS server use. Enter a value and click the **Apply** button to configure the encryption key of the RADIUS server. The numbers to the right of the field indicate the range of integer values that this field supports.
Timeout field	Amount of time, in seconds, in which the server must authenticate a login before the login fails. Edit this value and click the **Apply** button to configure the timeout value of the RADIUS server. The numbers to the right of the field indicate the range of integer values that this field supports.
Max Retries field	Number of sequential logins that a user may perform before the server denies access to the username altogether. Edit this value and click the **Apply** button to configure the maximum number of retries that the RADIUS server permits. The numbers to the right of the field indicate the range of integer values that this field supports.
Access Requests field	Number of authentication requests that the server has received from your device since your device booted.
Access Accepts field	Number of logins to your device that the server authenticated since your device booted.
Access Rejects field	Number of logins to your device that the server denied since your device booted.
Server Timeout field	Number of authentications that timed out on the server since your device booted.

Adding RADIUS Servers

To configure a new RADIUS server on your device, perform the following steps:

Step 1 Click the **Maintenance** menu and choose **Services**. The Services window opens.

Step 2 Click the **Radius Servers** tab.

Step 3 Click the **Insert** button. The Insert Radius Server window opens.

Note Click the **Close** button at any time to abort this process with no changes to your device. Configurations apply only after you click the **Apply** button.

Step 4 In the Address field, enter the IP address of the server.

Step 5 (Optional) Edit the UDP Port field. The numbers to the right of the field indicate the range of integer values that this field supports.

Step 6 (Optional) Enter an encryption key in the Encryption Key field.

Step 7 (Optional) Edit the Timeout field. The numbers to the right of the field indicate the range of integer values that this field supports.

Step 8 (Optional) Edit the Max Retries field. The numbers to the right of the field indicate the range of integer values that this field supports.

Step 9 Click the **Insert** button.

Editing a RADIUS Server Configuration

To remove a RADIUS server from your configuration, perform the following steps:

Step 1 Click the **Maintenance** menu and choose **Services**. The Services window opens.

Step 2 Click the **Radius Servers** tab.

Step 3 Identify the row of the RADIUS server that you want to reconfigure, and then double-click the cell that you want to edit.

Note You can only edit cells that have a white background.

Step 4 Edit the content of the cell.

Step 5 Click the **Apply** button.

Step 6 Delete RADIUS Servers.

To remove a RADIUS server from your configuration, perform the following steps:

Step 1 Click the **Maintenance** menu and choose **Services**. The Services window opens.

Step 2 Click the **Radius Servers** tab.

Step 3 Click the row entry of the RADIUS server that you want to delete.

Step 4 Click the **Delete** button.

Enabling HTTP Services

To configure RADIUS services, perform the following steps:

Step 1 Click the **Maintenance** menu and choose **Services**. The Services window opens.

Step 2 Click the **HTTP** tab.

Step 3 Check the **Enable HTTP Server** checkbox.

Step 4 (Optional) Assign a port in the HTTP Port field.

Step 5 (Optional) Check the **Enable HTTP Polling** checkbox.

Step 6 (Optional) Check the **Enable HTTPS Server** checkbox.

Step 7 (Optional) Assign a port in the HTTPS Port field.

Step 8 Select a security method from the Secure Cert Common Name field.

Step 9 Click the **Apply** button.

Customizing the Boot Configuration

To customize the boot configuration do the following:

- View the image that the switch will boot during the next reboot.
- Delete the startup configuration.
- Overwrite the startup configuration with another configuration file in your file system.

Configuring Reboot Image

To choose the image that the Server Switch loads when it reboots, perform the following steps:

Step 1 Click the **Maintenance** menu and choose **Boot Config**. The Boot Configuration window opens.

Step 2 From the Image Source For Next Reboot pulldown menu, choose the image that you want the Server Switch to boot when it reboots.

Step 3 Click the **Apply** button in the Software Images partition.

Deleting or Overwriting the Startup Configuration

Step 1 Click the **Maintenance** menu and choose **Boot Config**. The Boot Configuration window opens.

Step 2 (Optional) Click the Overwrite startup configuration with radio button, and then choose a configuration from the pulldown menu to replace the current startup configuration with another configuration file.

Note To overwrite your startup configuration with your running configuration, refer to the "Backing Up the Running Configuration File" section on page 5-10.

Step 3 (Optional) Click the **Delete startup configuration** radio button to configure your Server Switch to use the factory default startup configuration.

Step 4 Click the **Apply** button in the Startup Configuration partition.

Backing Up the Running Configuration File

To save your running configuration file, perform the following steps:

Step 1 Click the **Maintenance** menu and choose **Backup Config**. The Backup Configuration window opens.

Step 2 Enter a file name in the Save Configuration As field. Element Manager will save your running configuration in the configuration directory with the name that you specify.

Note Enter **startup-config** in this field if you want to save the running configuration as the startup configuration. This process overwrites the existing startup configuration file.

Step 3 Click the **Save** button.

Viewing Files in the File System

To view files, such as image files, log files, and configuration files, that reside on your device, perform the following steps:

Step 1 Click the **Maintenance** menu and choose **File Management**. The File Management window opens. Table 5-5 lists and describes the fields in the Current Files on System table in this window.

Table 5-5 Current Files on System Table Field Descriptions

Field	Description
Slot ID	Slot of the controller card on which the file resides.
File Name	Name of the file.
File Type	Type of file. The following types may appear: config log image

Table 5-5 Current Files on System Table Field Descriptions (continued)

Field	Description
Size	Size of the file, in bytes.
Date	Most recent date and time that your device or a user updated the file.

Step 2 (Optional) Click the **Refresh** button to poll your switch and update your display to reflect the most current inventory of your file system.

Deleting Files in the File System

To delete files from your file system, perform the following steps:

Step 1 Click the **Maintenance** menu and choose **File Management**. The File Management window opens.

Step 2 Click the line in the **Current Files on System** table that lists the file that you want to delete, and then click the **Delete** button. A Delete File window opens.

Step 3 Click the **Yes** button.

Understanding Configuration Files

A configuration file is a text file that stores a list of CLI commands.

Startup-Config

The main configuration file is called startup-config. This file stores all of the CLI commands necessary to completely configure a box from a factory default state. This configuration file can be copied, backed up, and modified.

Running-Config

Whenever configuration changes are made via the GUI or CLI, a CLI command is temporarily saved in a virtual configuration file called running-config. If the administrator wishes to save these changes permanently, this file is copied into the startup-config file.

Any number of configuration files can be stored. For convenience and rapid configuration, files can also maintain a partial list of CLI commands. These files can also be copied into running-config for immediate use or startup-config for persistent use across reboots.

Understanding Log Files

Log files are text files that record activity, including configuration changes. Depending on their size, log files are rotated and compressed. Log files can also be exported from the system by using the **copy** command.

File Management and Storage

The management of log files is performed automatically, but you can configure log files. Log files are stored separately from other file types, but all files share the 128 MB of flash memory. Log files are stored in syslog files.

The system checks the size of the active log file hourly, and when it exceeds 1 MB, the active log file, ts_log, is closed, compressed, and renamed ts_log.1.gz. Other ts_log.x.gz files are incremented by 1. These files can be downloaded via the Log Viewer GUI, which can create filters for troubleshooting and auditing purposes.

Message Types

The following levels of logging are captured:

- CONF—configuration changes; no user action is required.
- INFO—general information; no user action is required.
- WARN— abnormal condition; user intervention may be required.
- ERROR— abnormal condition; user intervention is required.
- FATAL—abnormal condition; user must reboot.

Installing Software Images

To proceed to the instructions, refer to the "Installing a Software Image" section on page 5-15. The sections that follow provide context and details about installing images.

The Image data that is used to configure the software is being continuously updated and enhanced. Use the latest system image data to ensure the most efficient usage of your system.

Refer to the user's support portal at support.cisco.com for the latest upgrades.

System Image

A system image is an unpacked and installed image file. An image file is the source from which to install a system image and it has an .img extension.

When an image file is installed, the image file is expanded into a system image. The system image is what the user will refer to in order to specify what the system should use to boot up each card in the system.

Image File

Image files are stored in flash memory as a single complete file with an ".img" extension. Each image file contains all the operating software (application software and firmware/microcode) needed by the various cards that can be installed into the system.

The system cannot use an image file directly to boot up the system. The image file must first be installed. The installation process automatically unbundles the image file and distributes the software components to each card in the system. Users do not have to be aware of individual software components. The user executes one CLI command to install an image file. Refer to the install command in the *CLI Reference Guide*.

The Server Switch operating system stores up to three images on a disk: the uninstalled image, the current system (or installed) image, and the recovery image.

The system only has enough flash memory to store:

- one system image file (active)
- one image file (inactive/uninstalled)
- one recovery image

Occasionally, you will have to manually delete an image file from the InfiniBand system to make room for a new version. Refer to the "Deleting Files in the File System" section on page 5-11.

Inactive Image

An inactive image is an image that has been downloaded, but has not been installed. It is not the active, or system image.

The operating system can only store one inactive image. Delete inactive images through the CLI (refer to the "Deleting Files in the File System" section on page 5-11), or by clicking the delete button in the Element Manager.

Active Image

An active image is the current system image. An installed, or active image has gone through the entire upgrade process. The system image usually has a slash (/) in its name. Do not modify or delete the installed system image.

Recovery Image

The Recovery Image is a default image that comes installed on the system. The Recovery Image can be used to quickly restore operation to the system if an image upgrade should fail.

Version Numbers

The operating system and installed system image running on the InfiniBand system determine the supported software features.

Two types of system-images are provided:

- An image for the HCA card
- An image for the Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 7008, or Cisco IB Server Switch Module.

Before configuring the InfiniBand system, check the version of the installed system image used to boot the chassis. Use this information to ensure that you upgrade to the correct software.

Copying/Downloading the Image

Upgrading the Server Switch operating system requires several steps, which are described in the following sections. One step is to copy the image before installing it.

Table 5-6 lists several options for copying the image into the system.

Table 5-6 Copying/Downloading Image Options

Through the CLI	Through the GUI
FTP	Remote FTP Server
TFTP	Local File
SCP	Remote Secure Server

Card Status Requirements

Only cards with an oper-status of “up” are updated. If a card is down when you run install, or a card is added after running install, perform the following steps:

Step 1 Bring up the card

Step 2 Run the installation again.

Step 3 Specify the same image file. If the image is already installed on a card, that card is skipped.

Step 4 Be sure to specify the boot-config again so that all cards know to boot from the same system image.

Upgrade Procedure Overview

The system upgrade process is summarized in the following steps:

Step 1 Set up the hardware connection for the upgrade.

Step 2 Verify the installed system image version number.

Step 3 Download an image file from a network-accessible FTP server, or download an image file remotely from a TFTP server.

Step 4 Install the new system image.

Step 5 Configure the CLI and Element Manager to use the appropriate configuration file the next time they reboot.

Step 6 Reboot the system.

Installing a Software Image

To install an image file, perform the following steps:

Step 1 Click the **Maintenance** menu and choose **File Management**. The File Management window opens.

Note If you have not already imported an image file to your file system, refer to the "Importing Configuration Files and Image Files" section on page 5-15.

Step 2 Click the line in the **Current Files on System** table that lists the file that you want to install, and then click the **Install** button. A verification window opens.

Note Before you install an image, verify that you have brought up all of the cards on the chassis that you want to run the new image. Cards that run a different image from the chassis cannot pass traffic.

Note Alert other users that you plan to install a new image to your Server Switch.

Step 3 Click the **Yes** button to install the image.

Importing Configuration Files and Image Files

You can import files to your Server Switch from your local host or a remote FTP server.

Importing from a Remote Server

To import files to your Server Switch from remote devices, perform the following steps:

Step 1 Click the **Maintenance** menu and choose **File Management**. The File Management window opens.

Step 2 Click the **Import** button. The Import File window opens.

Step 3 From the File Type pulldown menu, choose the type of file that you want to import (image or configuration).

Step 4 Click the **Remote FTP Server** radio button or **Remote SCP Server** radio button.

Step 5 Enter the DNS name or IP address of the FTP server that holds the file that you want to import in the Server Name or IP Address field.

Step 6 Enter the user ID that logs you in to the FTP server in the User Name field.

Step 7 Enter the password that logs you in to the FTP server in the Password field.

Step 8 Enter the directory path and name of the file on the FTP server in the File Path and Name field.

Step 9 Enter the name that the file will take on your Server Switch in the File Name on System field.

Step 10 Click the **Copy** button.

Importing from Your Local Host

To import files to your Server Switch from your local host, perform the following steps:

Step 1 Click the **Maintenance** menu and choose **File Management**. The File Management window opens.

Step 2 Click the **Import** button. The Import File window opens.

Step 3 Select, from the **File Type** pulldown menu, the type of file that you want to import (image or configuration).

Step 4 Click the **Local File** radio button.

Step 5 Click the **Choose** button and navigate to the file that you want to import.

Step 6 Click the file that you want to import, and then click the **OK** button.

Step 7 Enter the name that the file will take on your Server Switch in the File Name on System field.

Step 8 Click the **Copy** button.

Exporting Configuration Files and Log Files

You can export files from your Server Switch to your local host or a remote FTP server.

Exporting to a Remote Server

To export files from your Server Switch to a remote device, perform the following steps:

Step 1 Click the **Maintenance** menu and choose **File Management**. The File Management window opens.

Step 2 Click the file that you want to export. The **Export** button becomes active.

Step 3 Click the **Export** button. The Export File window opens.

Step 4 Click the **Remote FTP Server** radio button or **Remote SCP Server** radio button.

Step 5 In the Server Name or IP Address field, enter the DNS name or IP address of the FTP server that will receive the file that you want to export.

Step 6 In the User Name field, enter the user ID that logs you in to the FTP server.

Step 7 In the Password field, enter the password that logs you in to the FTP server.

Step 8 In the File Path and Name field, enter the path on your remote host where you want to copy the exported file, and the name that you want to assign for the file.

```
/root/files/old-config.cfg
```

Step 9 Click the **Copy** button.

Exporting to Your Local Host

To export files from your Server Switch to your local host, perform the following steps:

Step 1 Click the **Maintenance** menu and choose **File Management**. The File Management window opens.

Step 2 Click the file that you want to export. The **Export** button becomes active.

Step 3 Click the **Export** button. The Export File window opens.

Step 4 Click the **Local File** radio button.

Step 5 Click the **Choose** button.

Step 6 Navigate to the directory where you want to copy the file, and then click the **OK** button.

Step 7 Click the **Copy** button.

Saving a Configuration File

To back up your running configuration to the standby controller on your chassis, perform the following steps:

Step 1 Click the **Maintenance** menu and choose **Save Config**.

Note If you make configuration changes to the master image and then save the configuration, verify that the master and backup have synchronized, and then save the configuration on the backup as well. For more information, see the "Configuring Database Synchronization" section on page 8-25.

Rebooting the Server Switch with Element Manager

To reboot your Server Switch with Element Manager, perform the following steps:

Step 1 Click the **Maintenance** menu and choose **Reboot**.

Step 2 Click the **OK** button.

Running General Diagnostics

With Element Manager, you can run the following diagnostics:

- chassis
- card
- port

Running Chassis Diagnostics

To run chassis diagnostics, perform the following steps:

Step 1 Click the **Maintenance** menu, and then choose **Diagnostics > General**.

Step 2 Click the **Chassis** tab.

Step 3 In the Module Type field, click the radio button of the type of the element that you want to diagnose.

Step 4 Enter the index number of the element that you want to diagnose in the Module Number field.

Step 5 In the Test field, click the radio button of the type of test that you want to run.

Step 6 Enter the number of times that you want the test to run in the Iterations field.

Step 7 In the Action field, click the start radio button to begin a test or the stop radio button to end a test.

Step 8 In the Option field, click the error condition that you want to apply.

Step 9 Click the **Apply** button to execute the configuration and start or stop the test.

Configuring Card Diagnostics

To run card diagnostics, perform the following steps:

Step 1 Click the **Maintenance** menu, and then choose **Diagnostics > General**.

Step 2 Click the **Card** tab.

Step 3 Click the **Insert** button. The Diagnostic, Insert Card window opens.

Step 4 Click the **Card** pulldown menu and choose the card that you want to test.

Step 5 In the Test field, click the type of test that you want to execute.

Step 6 In the Iterations field, click the number of test iterations that you want to run.

Step 7 Choose an action from the Action field:

- Click the **start** radio button if you want the test to run when you click the Insert button
- Click the **stop** radio button if you want the test to appear in the table but not execute. To run the test later, see the "Running Configured Diagnostic Tests" section on page 5-20.

Step 8 Click the **Insert** button.

Deleting a Card Test Entry

To delete a card test entry, perform the following steps:

Step 1 Click the **Maintenance** menu, and then choose **Diagnostics > General**.

Step 2 Click the **Card** tab.

Step 3 Click the row of the entry that you want to delete, and then click the **Delete** button.

Configuring Port Diagnostics

To run port diagnostics, perform the following steps:

Step 1 Click the **Maintenance** menu, and then choose **Diagnostics > General**.

Step 2 Click the **Port** tab.

Step 3 Click the **Insert** button. The Diagnostic, Insert Port window opens.

Step 4 Enter a port in the Port field, or click the "**...**" button, choose ports, and click the **OK** button.

Step 5 In the Test field, click the radio button of the test that you want to execute.

Step 6 (Optional) Check the **Data Validation** checkbox to validate data.

Step 7 Enter the size, in bits, of the data packet that you want to send in the Data Size field.

Step 8 Enter the data pattern that you want to iterate in the test in the Data Pattern field.

Step 9 Enter the number of iterations that you want to execute in the Iterations field.

Step 10 Enter a source LID in the Source ID field.

Step 11 Enter a destination LID in the Target ID field.

Step 12 Select an action from the **Action** field:

- Click the **start** radio button if you want the test to execute when you click the Insert button.
- Click the **stop** radio button if you want the test to appear in the table but not execute. To execute the test later, see "Running Configured Diagnostic Tests" section on page 5-20.

Step 13 Click the **Insert** button.

Deleting a Port Test Entry

To delete a card test entry, perform the following steps:

Step 1 Click the **Maintenance** menu, and then choose **Diagnostics > General**.

Step 2 Click the **Port** tab.

Step 3 Click the row of the entry that you want to delete, and then click the **Delete** button.

Running Configured Diagnostic Tests

To run a diagnostic test that you have already added to the Diagnostics window, perform the following steps:

Step 1 Click the **Maintenance** menu, and then choose **Diagnostics > General**.

Step 2 Click the appropriate tab for the test that you want to run.

Step 3 Identify the entry of the test that you want to run.

Step 4 Click the cell in the **Action** column of that entry and choose **start** from the pulldown menu.

Note The cell must display **stop** for this process to work. If the cell displays **start**, choose **stop** from the pulldown menu and click the **Apply** button, and then perform this step.

Step 5 Click the **Apply** button, and then repeatedly click the **Refresh** button to track the progress of the test.

Viewing POST Diagnostics

You can view POST diagnostics for the following elements:

- Cards
- Power Supplies
- Fans

Viewing Card POST Diagnostics

To view card POST diagnostics, perform the following steps:

Step 1 Click the **Maintenance** menu, and then choose **Diagnostics > POST**.

Step 2 Click the **Card** tab. Table 5-7 lists and describes the fields that appear.

Table 5-7 Card POST Field Descriptions

Field	Description
Slot ID	Slot number.
POST Status	Indicates the result of POST (Power-on-self-test): unknown passed failed
PostErrorCodes	Show error(s) detected during POST.

Viewing Power Supply POST Diagnostics

To view power supply POST diagnostics, perform the following steps:

Step 1 Click the **Maintenance** menu, and then choose **Diagnostics > POST**.

Step 2 Click the **Power Supply** tab. Table 5-8 lists and describes the fields that appear.

Table 5-8 Card POST Field Descriptions

Field	Description
PS ID	Power supply number.
POST Status	Indicates the result of POST: unknown passed failed
PostErrorCodes	Show error(s) detected during POST.

Viewing Fan POST Diagnostics

To view fan POST diagnostics, perform the following steps:

Step 1 Click the **Maintenance** menu, and then choose **Diagnostics > POST**.

Step 2 Click the **Fan** tab. Table 5-9 lists and describes the fields that appear.

Table 5-9 Card POST Field Descriptions

Field	Description
Fan ID	Fan number.
POST Status	Indicates the result of POST): • unknown • passed • failed
PostErrorCodes	Show error(s) detected during POST.

Viewing FRU Diagnostics

You can view FRU diagnostics for the following elements:

- cards
- power supplies
- fans

Viewing Card FRU Diagnostics

To view card FRU diagnostics, perform the following steps:

Step 1 Click the **Maintenance** menu, and then choose **Diagnostics** > **POST**.

Step 2 Click the **Card** tab. Table 5-10 lists and describes the fields that appear.

Table 5-10 Card POST Field Descriptions

Field	Description
Slot ID	Slot number.
FruError	Shows the last hardware error (if any) detected on this FRU. The information returned in this variable is read from the device's VPD.

Viewing Power Supply FRU Diagnostics

To view power supply FRU diagnostics, perform the following steps:

Step 1 Click the **Maintenance** menu, and then choose **Diagnostics** > **POST**.

Step 2 Click the **Power Supply** tab. Table 5-11 lists and describes the fields that appear.

Table 5-11 Card POST Field Descriptions

Field	Description
PS ID	Power supply number.
FruError	Shows the last hardware error (if any) detected on this FRU. The information returned in this variable is read from the device's VPD.

Viewing Fan FRU Diagnostics

To view fan FRU diagnostics, perform the following steps:

Step 1 Click the **Maintenance** menu, and then choose **Diagnostics** > **POST**.

Step 2 Click the **Fan** tab. Table 5-12 lists and describes the fields that appear.

Table 5-12 Card POST Field Descriptions

Field	Description
Fan ID	Fan number.
FruError	Shows the last hardware error (if any) detected on this FRU. The information returned in this variable is read from the device's VPD.