lenovo

Flex System FC3171 8 Gb SAN Switch QuickTools User's Guide

lenovo

Flex System FC3171 8 Gb SAN Switch QuickTools User's Guide

Note: Before using this information and the product it supports, read the general information in “Notices” on page B-113.

First Edition, April 2015

Contents

Chapter 1. Lenovo Flex System FC3171 8 Gb SAN Switch

The Lenovo® Flex System™ FC3171 8 Gb SAN Switch is a full-fabric switch that can be converted to a pass-thru module when configured in transparent mode. This product installs in an Lenovo Flex System chassis.

This *User's Guide* contains information and instructions for managing the Lenovo Flex System FC3171 8 Gb SAN Switch using QuickTools. This information includes a description of the QuickTools menus and displays, fabric management tasks, switch management tasks, and port management tasks.

Related documents

This *User's Guide* contains instructions for managing the switch using QuickTools. Follow the instructions in this *User's Guide* after you read the *Lenovo Important Notices* document that comes with the switch.

The following related Lenovo documentation contains important, useful information to help you with the setup, installation, configuration, operation, and troubleshooting processes for these devices. This documentation is preloaded on the Lenovo Flex System Manager management node and is also available at http://publib.boulder.ibm.com/infocenter/flexsys/information/index.jsp:

- Lenovo Flex System network device *User's Guides*

  Each type of network adapter has a customized *User's Guide* that contains detailed information about the expansion card, which is compatible with the 8 Gb switches. These switches contain connectors for the compute nodes in which the network adapter is installed.

- *Lenovo Flex System Enterprise Chassis Installation and Service Guide*

  Each type of Lenovo Flex System chassis has a customized *Installation and Service Guide*.

- Lenovo Flex System Compute Node *Installation and Service Guides*

  Each type of compute node has a customized *Installation and Service Guide*.

- Lenovo *Notices for Network Devices* CD

  This CD ships with networking products (adapters, switches, and pass-thru modules). It contains license documentation and the following documents:

- *IBM Flex System FC3171 8 Gb SAN Switch and Pass-thru Installation and User's Guide*

  This document contains instructions for setting up, installing, removing, configuring, and troubleshooting the switch.

- *Lenovo Flex System FC3171 8 Gb SAN Switch Command Line Interface User's Guide*

  This document explains how to manage the SAN switch using the CLI.

- *IBM Flex System FC3171 8 Gb SAN Switch and Pass-thru CIM Agent Reference Guide*

  This document describes how the Common Interface Model (CIM) Agent functions as an implementation of the Storage Management Initiative (SMI)-Specification 1.1

- *IBM Flex System FC3171 8 Gb SAN Switch and Pass-thru Event Message Guide*

  This document lists the event messages for the Lenovo Flex System FC3171 8 Gb SAN Switch

- *IBM Flex System FC3171 8 Gb SAN Switch and Pass-thru Simple Network Management Protocol Reference Guide*

  This document describes the support for Simple Network Management Protocol (SNMP) and how to use SNMP to manage and monitor the Lenovo Flex System FC3171 8 Gb SAN Switch.

The updated Lenovo Flex System documentation is available on the Lenovo Flex System switch and from the IBM Flex System Information Center at http://publib.boulder.ibm.com/infocenter/flexsys/information/index.jsp.

Notices and statements in this document

The caution and danger statements in this document are also in the multilingual *Safety Information* document, which is on the *Documentation* CD. Each statement is numbered for reference to the corresponding statement in the *Safety Information* document.

The following notices and statements are used in this document:

- **Note:** These notices provide important tips, guidance, or advice.
- **Important:** These notices provide information or advice that might help you avoid inconvenient or problem situations.
- **Attention:** These notices indicate possible damage to programs, devices, or data. An attention notice is placed just before the instruction or situation in which damage might occur.
- **Caution:** These statements indicate situations that can be potentially hazardous to you. A caution statement is placed just before the description of a potentially hazardous procedure step or situation.
- **Danger:** These statements indicate situations that can be potentially lethal or hazardous to you. A danger statement is placed just before the description of a potentially lethal or hazardous procedure step or situation.

JDOM License

This product includes software developed by the JDOM Project (http://www.jdom.org/). Copyright (C) 2000-2002 Brett McLaughlin & Jason Hunter. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the disclaimer that follows these conditions in the documentation and/or other materials provided with the distribution.
3. The name "JDOM" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact license@jdom.org.
4. Products derived from this software may not be called "JDOM", nor may "JDOM" appear in their name, without prior written permission from the JDOM Project Management (pm@jdom.org).

In addition, we request (but do not require) that you include in the end-user documentation provided with the redistribution and/or in the software itself an acknowledgment equivalent to the following: "This product includes software developed by the JDOM Project (http://www.jdom.org/)."

Alternatively, the acknowledgment may be graphical using the logos available at http://www.jdom.org/images/logos.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE JDOM AUTHORS OR THE PROJECT CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the JDOM Project and was originally created by Brett McLaughlin brett@jdom.org and Jason Hunter jhunter@jdom.org. For more information on the JDOM Project, please see http://www.jdom.org/.

Chapter 2. Using QuickTools

This chapter describes how to use QuickTools and its menus. The following topics are covered:

- Getting started
- QuickTools user interface
- Setting QuickTools preferences
- Using online help
- Viewing software version
- Exiting QuickTools

Getting started

This section describes the workstation requirements, encryption mode, and opening QuickTools.

Workstation requirements

The following sections describe the workstation hardware and software requirements for running QuickTools. The software requirements are listed for the default switch configuration and for strong encryption.

Workstation hardware

The workstation hardware requirements for running QuickTools are listed in Table 1.

Table 1. Workstation hardware requirements

Requirement	Description
Memory	2 GB or more
Processor	2 GHz or faster
Interfaces	RJ-45 Ethernet port

Workstation software

Workstation software requirements for the default switch configuration are listed in Table 2.

Table 2. Workstation software requirements (default)

Requirement	Description
Operating systems	Windows® 7, Windows Server 2008 R2, Windows XP SP2 Mac OS® X 10.7.3 Solaris™ 10 and 10 x86 Red Hat® Enterprise Linux® 5.5+, 6 SUSE™ Linux Enterprise Server 10, 11
Java	Java® 2 Runtime Environment 8
Internet browsers	Microsoft® Internet Explorer® 9.0 and later Firefox® 3.6 and later Safari® 5.1.3 and later

The switch supports strong encryption and extended key/certificate lengths according the *National Institute of Standards and Technology (NIST) Special Publication SP800-131A*. The EncryptionMode service (Legacy or Strict) determines which encryption algorithms, Diffie-Hellman groups, and key lengths can be applied to IP security associations, Internet Key Exchange (IKE) peers, IKE policies, Public Key Infrastructure (PKI) keys, and certificates.

- Legacy mode, which is the default, uses encryption algorithms with a strength of 80 bits or greater, and keys/certificates with a length of 1,024 or greater.
- Strict mode uses encryption algorithms with a strength of 112 bits or greater, and keys/certificates with a length of 2,048 or greater.

The workstation software requirements listed in Table 3 apply when EncryptionMode=Strict.

Table 3. Workstation software requirements (strong security)

Requirement	Description
Transport Layer Security (TLS)	TLS 1.2. See "Configuring the Browser and Java for Strong Encryption" on page 2-7 for information about enabling TLS 1.2.
Operating systems	Windows 7, Windows Server 2008 R2, Windows XP SP2
Internet browsers	Microsoft Internet Explorer 9.0 and later Firefox 25 and later

Configuring the Browser and Java for Strong Encryption

TLS 1.2 must be enabled in your browser and in Java to support strong encryption (Encryption Mode = Strict). For information about Encryption Mode, see "Encryption Mode" on page 4-62.

To use QuickTools in Strict mode:

1. Enable TLS 1.2 in your browser.
   - For Internet Explorer:
   a. Select **Tools > Internet Options**.
   b. In the Internet Options dialog box, choose the **Advanced** tab.
   c. Scroll to the Security settings, and click the **Use TLS 1.2** check box.
   d. Click **OK**.
   - For Chrome:
   a. In the Chrome pull-down menu, select **Settings**.
   b. At the bottom of the Settings page, select **Show advanced settings...**.
   c. Under Network, click **Change proxy settings...**.
   d. In the Internet Properties dialog box, choose the **Advanced** tab.
   e. Scroll to the Security settings, and click the **Use TLS 1.2** check box.
   f. Click **OK**.
   - For Firefox:
   a. Type `about:config` in address bar, and then press Enter.
   b. Type `tls` in Search bar, and then press Enter.
   c. In the list of TLS preferences, find **security.enable_tls**. This value should be True. If necessary, double-click the entry to change the value.
   d. In the list of TLS preferences, find **security.tls.version.min**. The values for this preference are 0 (SSL 3.0), 1 (TLS 1.0), 2 (TLS 1.1), and 3 (TLS 1.2). Double click the **security.tls.version.min** preference, type `3` in the dialog box, and then click **OK.**
2. Enable TLS 1.2 in Java.

a. Click the **Start** button, and select **Control Panel**.

b. On the Control Panel home page, select **Programs**.

c. On the Programs page, select **Java**.

d. In the Java Control Panel, choose the **Advanced** tab.

e. In the Settings list, expand the **Security** setting.

f. In the Security list, expand the **General** setting.

g. Click the **Use TLS 1.2** check box

h. Click **OK**.

3. Finally, log in to the switch through SSH, and use the Set Setup Services command to set the EncryptionMode service to Strict. For more information about the EncryptionMode service, see the description of the Set Setup Services command and the EncryptionMode parameter in the *Lenovo Flex System FC3171 8 Gb SAN Switch Command Line Interface User's Guide* or the *IBM Flex System FC3171 8 Gb Pass-thru Command Line Interface User's Guide*.

Opening QuickTools

After the switch is operational, open QuickTools by entering the switch IP address in an Internet browser (use “https://”, not “http”). If your workstation does not have the Java 2 Run Time Environment 8 program, you will be prompted to download it.

Notes:

After upgrading to firmware version 9.1.5, when using Internet Explorer 9, you may encounter a general exception application error. To remedy this problem, clear the temporary Internet files:

1. Select **Tools**, **Internet Options**, **Delete. . .** (Browsing history).
2. Select only the **Temporary Internet Files**, and then click **Delete**.
3. Close and reopen Windows Internet Explorer.

The Add a New Fabric dialog shown in Figure 1 prompts you for your username and password. Click the **Add Fabric** button to open the fabric.

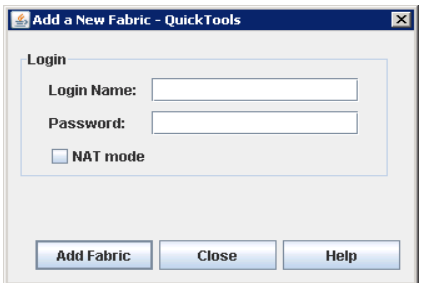

Figure 1. Add a New Fabric dialog

The opening window is displayed, as shown in Figure 3. For security reasons, you will be prompted to change your user account password that was initially set up by the administrator, as shown in Figure 2. You will be prompted to change the password each time you attempt to open the fabric until you change the default password. Click the **OK** button, and change the user account password. For more information, see ”Managing user accounts” on page 4-50.

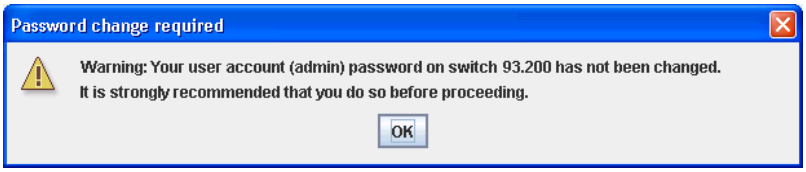

Figure 2. Password Change Required dialog

QuickTools user interface

QuickTools uses the faceplate display to manage the switches in a fabric. The interface, as shown in Figure 3, consists of a menu bar, fabric tree, graphic window, data windows (some with buttons), and data window tabs.

The fabric name is displayed for reference in the fabric tree above the switch names. Click a switch name or icon to display a different switch faceplate in the graphic window. Information displayed in the data windows corresponds to the data window tab selected.

The graphics window shows the switch faceplate, the Lenovo Flex System chassis interface, and the general switch status. The switch faceplate shows switch LEDs, switch external ports (0, 15–19) and port LEDs. The Lenovo Flex System chassis interface shows switch port connections (1–14) and chassis mezzanine cards (1, 2). Information is available for elements in the interface, such as ports and LEDs, when you select a port and mouse over the object.

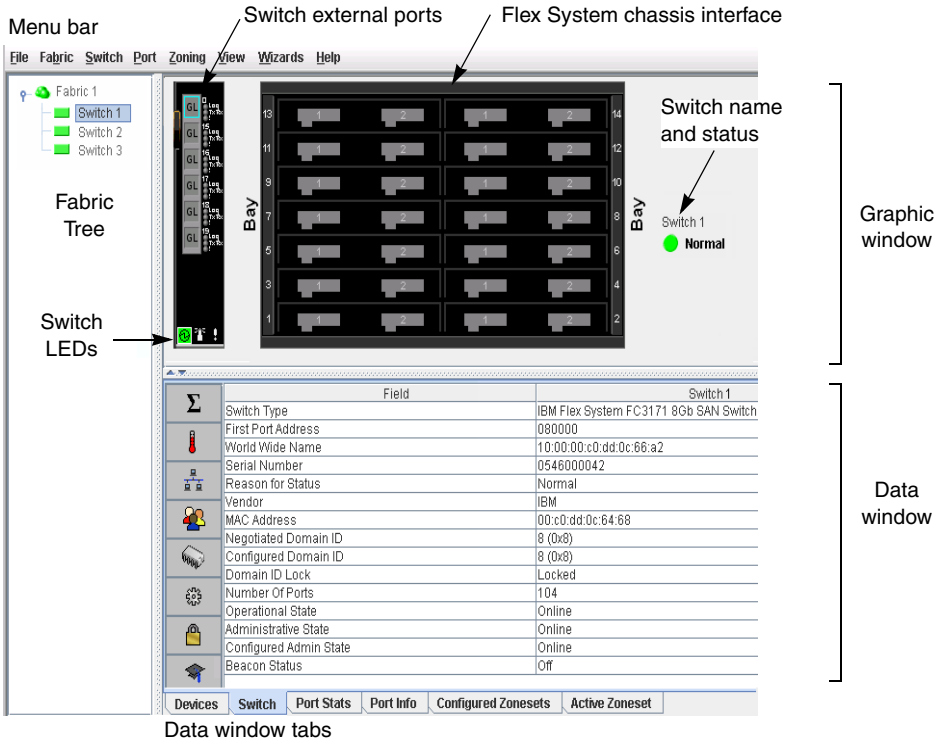

Figure 3. QuickTools interface

Fabric tree

QuickTools allows you to manage the switches in one fabric. The fabric tree, shown in Figure 3, provides access to each switch faceplate display in the fabric. Click a switch name or icon to display that switch faceplate in the graphic window. The window width of the fabric tree can be adjusted by clicking and dragging the movable window border.

The fabric tree entry has a small icon next to it that uses color to indicate operational status.

- A green icon indicates normal operation.
- A yellow icon indicates that a switch is operational, but may require attention to maintain maximum performance.
- A red icon indicates a potential failure or non-operational state as when the switch is offline.
- A blue icon indicates that a switch is unknown, unreachable, or unmanageable.

If the status of the fabric is not normal, the fabric icon in the fabric tree will indicate the reason for the abnormal status. The same message is provided when you rest the mouse on the fabric icon in the fabric tree.

Graphic window

The graphic window shows the switch faceplate display and the Lenovo Flex System chassis interface as show in Figure 3. The window height can be adjusted by clicking and dragging the window border that it shares with the data window.

The switch faceplate shows the six switch external ports and port status. For more information about port status, see “Port states” on page 5-100. The Lenovo Flex System chassis interface shows the 14 internal port connections to the switch and the corresponding chassis mezzanine cards (1 and 2). The Lenovo Flex System chassis has four switch bays numbered 1, 2, 3, and 4. Switches installed in bays 1 and 2 connect to the chassis through mezzanine card 1, and switches installed in bays 3 and 4 connect to the chassis through mezzanine card 2. The mezzanine card states are described in Table 4.

Table 4. Mezzanine card states

Mezzanine icon	Status
	The corresponding switch internal port is connected and logged in through the mezzanine card.
	The corresponding switch internal port is connected, but not logged in through the mezzanine card.
	The corresponding switch internal port is not connected. This indicates that the switch is not installed in bay that is associated with this mezzanine card.

Data windows and tabs

The data window, shown in Figure 3, presents a table of data and statistics associated with the selected tab for the switch displayed in the graphic window. Use the scroll bar to browse through the data. The window length can be adjusted by clicking and dragging the border that it shares with the graphic window. Adjust the column width by moving the pointer over the column heading border shared by two columns until a right/left arrow graphic is displayed. Click and drag the arrow to the desired width. The data windows and tabs are described below.

- Devices. The Devices tab displays information about devices (hosts and storage targets) connected to the switch. Refer to "Devices data window" on page 3-21 for more information.
- Switch. The Switch tab displays current network and switch configuration data for the selected switches. See "Using the Switch data window" on page 4-44 for more information.
- Port Statistics. The Port Statistics tab displays performance data for the selected ports. See "Using the Port Statistics data window" on page 5-96 for more information.
- Port Information. The Port Information tab displays information for the selected ports. See "Using the Port Statistics data window" on page 5-96 for more information.
- Configured Zonesets. The Configured Zonesets tab displays all zone sets, zones, and zone membership in the zoning database.
- Active Zoneset. The Active Zoneset tab displays the active zone set for the fabric including zones and their member ports. Refer to "Active Zone Set data window" on page 3-26 for more information about this data window. Refer to "Zoning" on page 3-25 for information about zone sets and zones.

Menu bar

QuickTools menu bar options are listed in Table 5.

Table 5. Menu bar options

Menu	Options
File	Preferences
Fabric (SAN Switch only)	Nicknames Rediscover Fabric Show Event Browser

Table 5. Menu bar options (Continued)

Menu	Options
Switch	Archive Restore User Accounts Set Date/Time Switch Properties Advanced Switch Properties (SAN Switch only) Services Call Home (Setup, Profile Manager, Message Queue, Test Profile, Changer Over) Network Properties SNMP (SNMP Properties, SNMP v3 Manager) Switch Diagnostics (Online Switch Diagnostics, Offline Switch Diagnostics (disrupts traffic)) Toggle Beacon Load Firmware Reset Switch Restore Factory Defaults Features Auth Servers Download Support File
Port	Port Properties Advanced Port Properties Reset Port Port Diagnostics
Zoning	Edit Zoning Resolve Zoning Edit Zoning Config Activate Zone Set Deactivate Zone Set Restore Default Zoning
View	Refresh View Port Types View Port States View Port Speeds View Port Media
Wizards	Configuration Wizard
Help	Help Topics About

Popup menus

Popup menus are displayed when you right-click the switch faceplate image in the graphic window. Popup menu options give you quick access to the common tasks and dialogs, such as:

- Refreshing a Switch
- Selecting all ports
- Properties dialogs (Port, Switch, Network, and SNMP)
- Services dialog
- Port diagnostics dialogs
- Only valid when module is the entry switch:
  - Network Properties
  - SNMP
  - Auth Servers

Shortcut keys

Shortcut key combinations provide an alternative method of accessing menu options in the web applet. For example, to open the Preferences dialog, press Alt+F, and then press R. The shortcut key combinations are not case-sensitive. Shortcut keys are not supported on the Mac OS platform.

Selecting switches

Switches are selectable in the fabric tree. Click a switch icon or name to display its faceplate display in the graphic window. For detailed switch information, see “Managing switches” on page 4-43.

Selecting ports

Ports are selectable and serve as access points for other displays and menus. You select ports to display information about them in the data window or to modify them. Context-sensitive popup menus are displayed when you right-click the faceplate image or on a port icon. See Chapter 5. Managing ports for detailed port information.

Selected ports in the faceplate display are outlined in cyan color. You can select ports the following ways.

- To select a port, click the port.
- To select all ports, right-click the faceplate image and select **Select All Ports** from the popup menu.
- To select a range of consecutive ports, click a port, press the **Shift** key and click another port. The web applet selects both end ports and all ports in between the end ports.

  Notes:

  When using the **Shift** key to select a range of ports, the first port you click in the range is the *anchor* selection. Subsequent ranges are based on this anchor selection. For example, after clicking port 4 and port 9 respectively, port 4 becomes the anchor selection. The next range includes all ports between port 4 and the next port you select.

- To select several non-consecutive ports, press the **Control** key while clicking each port.
- To un-select ports in a group of selected ports, press the **Control** key while clicking each port.
- To cancel a selection, press the **Control** key and select it again.

Setting QuickTools preferences

The preferences settings allow you to perform the following tasks:

- Change the location of the working directory in which to save files.
- Change the location of the browser used to view the online help. The Browser Location field is not supported/displayed for Mac OS X.
- Select a Display Dialog When Making Non-secure Connections option. If enabled, the Non-secure Connections Check dialog is displayed when you attempt to open a non-secure fabric. You then have the option of opening a non-secure fabric. If disabled, you cannot open a fabric with a non-secure connection.
- Enable (default) or disable the Event Browser. See "Event Browser" on page 3-18. If the Event Browser is enabled using the Preferences dialog as shown in Figure 4, the next time QuickTools is started, all events will be displayed. If the Event Browser is disabled when QuickTools is started and later enabled, only those events from the time the Event Browser was enabled and forward will be displayed.

- Choose the default port view when opening the faceplate display. You can set the faceplate to reflect the current port type (default), port speed, port operational state, or port transceiver media. Regardless of the default port view you choose, you can change the port view in the faceplate display by opening the View menu and selecting a different port view option. See the corresponding subsection for more information:
  - — "Port types" on page 5-102
  - — "Port operational states" on page 5-101
  - — "Port speeds" on page 5-103
  - — "Port transceiver media status" on page 5-103

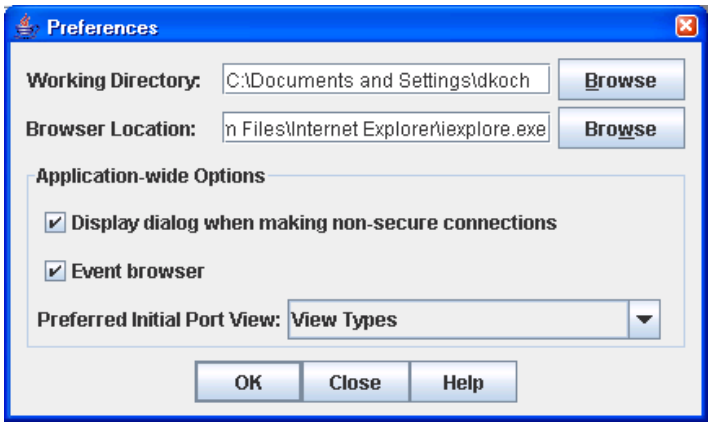

Figure 4. Preferences dialog

To set preferences for your QuickTools sessions, do the following:

1. Open the File menu, and select **Preferences** to open the Preferences dialog (Figure 4).
2. Enter, or browse, for paths to the working directory and browser.
3. In the Application-wide Options area, choose the preferences you want.
4. Click the **OK** button to save the changes.

Using online help

The browser-based online help system can be accessed from QuickTools several ways. Online help is also context-sensitive, that is, the online help opens to the topic that describes the dialog you have open.

To open the first topic in the help system, choose one of the following:

- Open the Help menu and select **Help Topics**.
- With no dialog displayed, press the **F1** function key.

To open the help system to the topic that describes the dialog you have open, choose one of the following:

- Click the **Help** button in the dialog.
- Press the **F1** function key.

Viewing software version

To view the QuickTools software version information, open the Help menu and select **About**.

Exiting QuickTools

To exit a QuickTools session, close the browser.

Chapter 3. Managing fabrics

This chapter describes the following fabric topics:

- Fabric services
- Rediscovering a fabric
- Event Browser
- Device information and nicknames
- Zoning

Fabric services

Fabric services include Simple Network Management Protocol (SNMP) and in-band management. SNMP is the protocol governing network management and monitoring of network devices. SNMP security consists of a read community string and a write community string, which are the passwords that control read and write access to the switch. The read community string ("public") and write community string ("private") are set at the factory to these well-known defaults and should be changed if SNMP is enabled. If SNMP is enabled (default) and the read and write community strings have not been changed from their defaults, you risk unwanted access to the switch.

In-band management is the ability to manage switches across inter-switch links using QuickTools, SNMP, management server, or the application programming interface. The switch comes from the factory with in-band management enabled. If you disable in-band management on a particular switch, you can no longer communicate with that switch by means other than a direct Ethernet or serial connection.

To enable in-band management, do the following:

1. Open the Switch menu and select **Switch Properties** to open the Switch Properties dialog.
2. Click the **In-band Management Enable** option.
3. Click the **OK** button to save the change to the database.

Rediscovering a fabric

After making changes to or deleting switches from a fabric view, it may be helpful to view the actual fabric configuration again. The rediscover fabric option clears out the current fabric information being displayed, and rediscovers all switch information. To rediscover a fabric, open the Fabric menu, and select **Rediscover Fabric**. The rediscover function is more comprehensive than the refresh function.

Event Browser

The Event Browser displays a list of events generated by the switches in the fabric and QuickTools. Events that are generated by QuickTools are not saved on the switch, but can be saved to a file during the QuickTools session.

Entries in the Event Browser, shown in Figure 5, are formatted by severity, time stamp, source, type, and description. The maximum number of entries allowed in the Event Browser is 10,000. The maximum number of entries allowed on a switch is 1200. Once the maximum is reached, the event list wraps and the oldest events are discarded and replaced with the new events. Event entries from the switch use the switch time stamp, while event entries generated by the web applet have a workstation time stamp. You can filter, sort, and export the contents of the Event Browser to a file. The Event Browser begins recording when enabled and QuickTools is running.

If the Event Browser is enabled using the Preferences dialog, the next time QuickTools is started, all events from the switch log will be displayed. If the Event Browser is disabled when QuickTools is started and later enabled, only those events from the time the Event Browser was enabled and forward will be displayed.

To display the Event Browser, open the Fabric menu and select **Show Event Browser**, or click the **Events** button on the tool bar. If the **Show Event Browser** selection or the **Events** button is grayed-out, you must first enable the **Events Browser** preference. See "Setting QuickTools preferences" on page 2-14.

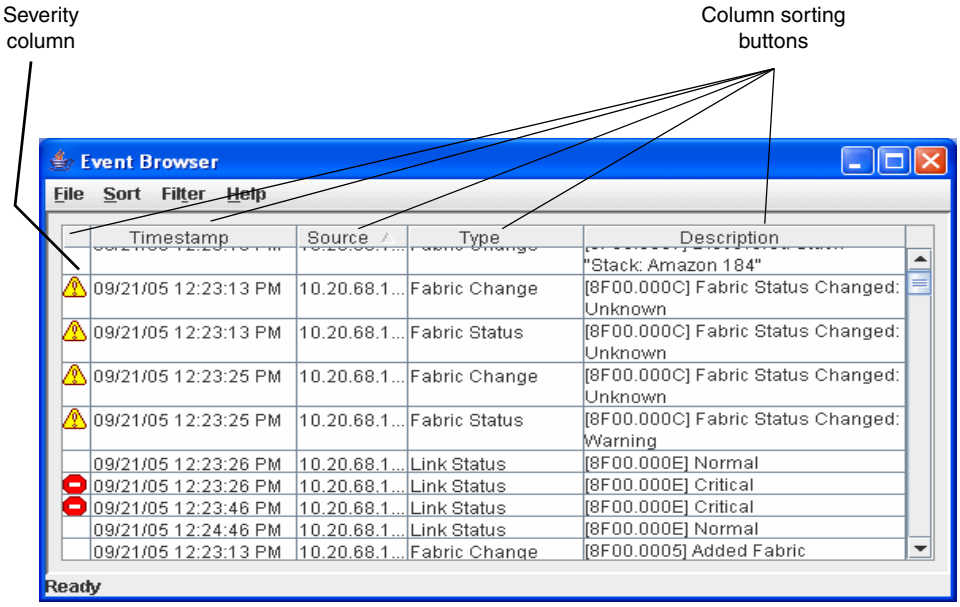

Figure 5. Event browser

Severity is indicated in the severity column using icons as described in Table 6.

Table 6. Severity levels

Severity Icon	Description
	Alarm—an alarm is a *serviceable event*. This alarm means that attention by the user or field service is required. Alarms are posted asynchronously to the screen and cannot be turned off. If the alarm denotes that a system error has occurred, the customer and/or field representative will generally be directed to provide a "show support" capture of the switch.
	Critical event—an event that indicates a potential failure. Critical log messages are events that warrant notice by the user. By default, these log messages will be posted to the screen. Critical log messages do not have alarm status as they require no immediate attention from a user or service representative.
	Warning event—an event that indicates errors or other conditions that may require attention to maintain maximum performance. Warning messages will not be posted to the screen unless the log is configured to do so. Warning messages are not disruptive and, therefore, do not meet the criteria of Critical. The user need not be informed asynchronously.
No icon	Informative—an unclassified event that provides supporting information.

Notes:

- Events (Alarms, Critical, Warning, and Informative) generated by the web applet are not saved on the switch. They are permanently discarded when you close a QuickTools session, but you can save these events to a file on the workstation before you close QuickTools and read it later with a text editor or browser.
- Events generated by the switch are stored on the switch, and will be retrieved when the web applet is restarted. Some alarms are configurable.

Filtering the Event Browser

Filtering the Event Browser enables you to display only those events that are of interest based on the event severity, timestamp, source, type, and description. To filter the Event Browser, open the Filter menu and select **Filter Entries**. This command opens the Filter Events dialog shown in Figure 6. The Event Browser displays those events that meet all of the criteria in the Filter Events dialog. If the filtering criteria is cleared or changed, then all the events that were previously hidden that satisfy the new criteria will be shown.

You can filter the event browser in the following ways:

- **Severity**—select one or more of the corresponding options to display alarm events, critical events, warning events, or informative events.
- **Date/Time**—select one or both of the From: and To: options. Enter the bounding timestamps (MM/DD/YY HH:MM AA) to display only those events that fall within those times. ("AA" indicates AM or PM.) The current year (YY) can be entered as either two or four digits. For example, 12/12/11 will be interpreted December 12, 2011.
- **Text**—select one or more of the corresponding options and enter a text string (case sensitive) for event source, type, and description. The Event Browser displays only those events that satisfy all of the search specifications for the Source, Type, and Description text.

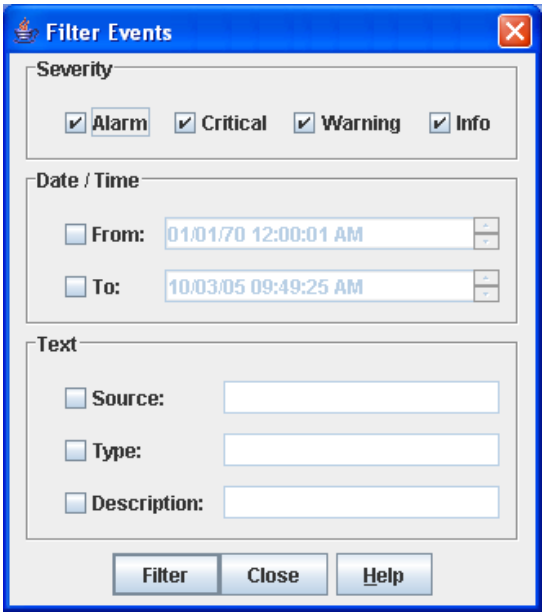

Figure 6. Filter Events dialog

Sorting the Event Browser

Sorting the Event Browser enables you to display the events in alphanumeric order based on the event severity, timestamp, source, type, or description. Initially, the Event Browser is sorted in ascending order by timestamp. To sort the Event Browser, click the **Severity**, **Timestamp**, **Source**, **Type**, or **Description** column buttons. You can also open the Sort menu and select **By Severity**, **By Timestamp**, **By Source**, **By Type**, or **By Description**. Successive sort operations of the same type alternate between ascending and descending order.

Saving the Event Browser to a file

You can save the displayed Event Browser entries to a file. Filtering affects the save operation, because only displayed events are saved. To save the Event Browser to a file, do the following:

1. Filter and sort the Event Browser to obtain the desired display.
2. Open the File menu and select **Save As**.
3. Select a folder and enter a file name in which to save the event log, and then click the **Save** button. The file can be saved in XML, CSV, or text format. XML files can be opened with an internet browser or text editor. CSV files can be opened with most spreadsheet applications.

Device information and nicknames

Devices are hosts and storage targets connected to the switch. A nickname is a user-definable, meaningful name that can be used in place of the World Wide Name. This sub-section describes how to view and manage device information and nicknames.

- Devices data window
- Displaying detailed device information
- Managing device port nicknames

Devices data window

The Devices data window, shown in Figure 7, displays information about devices connected to the switch. To display the Devices data window, click the **Devices** tab below the data window.

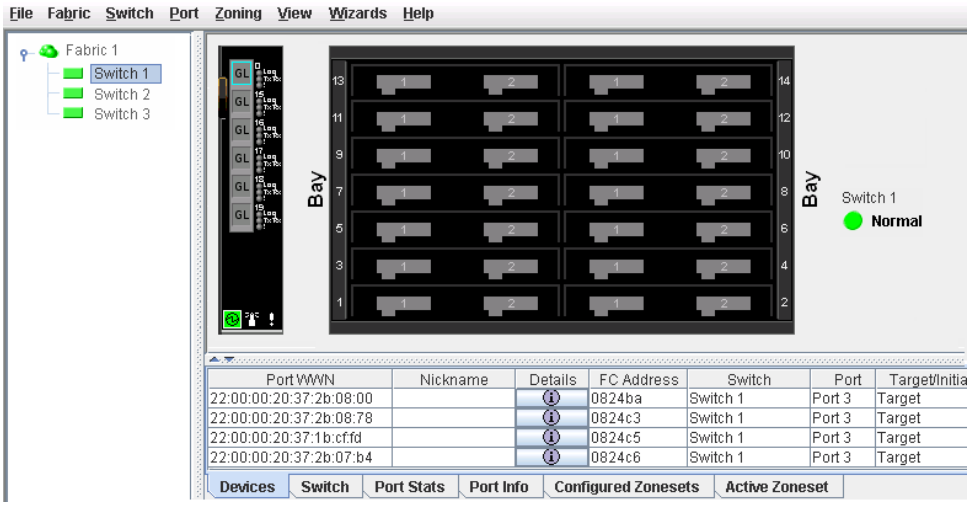

Figure 7. Devices data window

Table 7 describes the entries in the Devices data window.

Table 7. Devices Data Window entries

Entry	Description
Port WWN	Port world wide name
Nickname	Device port nickname. To create a new nickname or edit an existing nickname, double-click the cell and enter a nickname in the Edit Nickname dialog. Refer to "Managing device port nicknames" on page 3-23 for more information.
Details	Click the **(i)** to display additional information about the device. Refer to "Displaying detailed device information" on page 3-23.
FC Address	Fibre Channel address
Switch	Switch name
Port	Switch port number
Target/Initiator	Device type: target or initiator
Vendor	Host Bus Adapter/Device Vendor
Active Zones	The active zone to which the device belongs
Row #	Row number reference for each listing in the Devices data window table

Displaying detailed device information

In addition to the information that is available in the Devices data window, you can click the **(i)** in the Details column to open the Detailed Devices Display dialog, shown in Figure 8, to display more information.

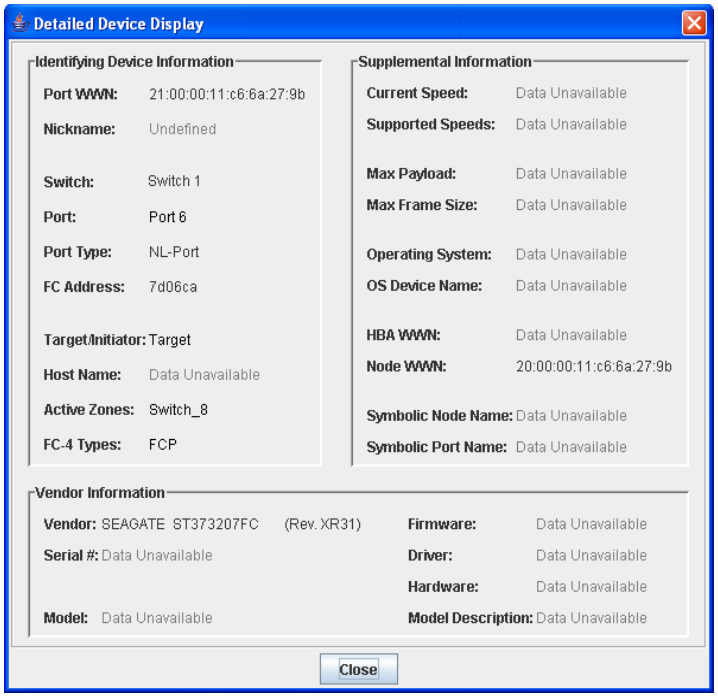

Figure 8. Detailed Devices Display dialog

Managing device port nicknames

You can assign a nickname to a device port World Wide Name. A nickname is a user-definable, meaningful name that can be used in place of the World Wide Name. Assigning a nickname makes it easier to recognize device ports when zoning your fabric or when viewing the Devices data window. In addition to creating, editing, and deleting nicknames, you can also export the nicknames to a file, which can then be imported into the Nicknames.xml file on other workstations.

Nicknames are saved to an XML file stored on the switch. If different nickname files exist on other switches in the fabric, you will be prompted to resolve differences before the Nicknames dialog will be displayed. A series of dialogs is presented to resolve differences between the nicknames stored on that switch with nicknames stored on other switches. The most recent nickname takes precedence during nickname resolution. Changes made in the Nickname dialog are propagated to all switches in the fabric after you click the **Apply** button.

Creating a nickname

To create a device port nickname, do the following:

1. Open the Fabric menu and select **Nicknames** to open the Nicknames dialog. The device entries are listed in table format.
2. Choose one of the following methods to enter a nickname. A nickname must start with a letter and can have up to 64 characters. Valid characters include alphanumeric characters [aA–zZ][0–9] and special symbols [$ _ - ^].
   - Double-click a cell in the **Nicknames** column, and enter a new nickname in the text field. Click the **Save** button to save the changes and exit the Nicknames dialog.
   - Click a device in the table. Open the Edit menu and select **Create Nickname** to open the Add Nickname dialog. In the Add Nickname dialog, enter a nickname and WWN and click the **OK** button.

Editing a nickname

A nickname must start with a letter and can have up to 64 characters. Valid characters include alphanumeric characters [aA–zZ][0–9] and special symbols [$ _ - ^].

Open the Fabric menu and select **Nicknames** to open the Nicknames dialog. The device entries are listed in table format. Choose one of the following methods to edit a nickname:

- Double-click a cell in the **Nicknames** column, and edit the nickname in the text field. In the Nicknames dialog, click the **Apply** button to save the changes.
- Click a device entry in the table. Open the Edit menu and select **Edit Nickname** to open the Edit Nicknames dialog. Edit the nickname in the text field. Click the **OK** button to save the changes. In the Nicknames dialog, click the **Apply** button to save the changes.

Deleting a nickname

To delete a device port nickname, do the following:

1. Open the Fabric menu and select **Nicknames** to open the Nicknames dialog.
2. Choose one of the following:
   - Click a device in the table. Open the Edit menu and select **Delete Nickname**.
   - Double-click a cell in the **Nicknames** column, and delete the nickname text.
3. Click the **Apply** button to save the changes.

Exporting nicknames to a file

You can save nicknames to a file. This capability is useful for distributing nicknames to other management workstations. To save nicknames to an XML file, do the following:

1. Open the Fabric menu and select **Nicknames** to open the Nicknames dialog.
2. Open the File menu in the Nicknames dialog, and select **Export**.
3. Enter a name for the XML nickname file in the Save dialog and click **Save**.

Importing a nicknames file

Importing a nicknames file copies its contents into and replaces the contents of the Nicknames.xml file which is used by QuickTools. To import a nickname file, do the following:

1. Open the Fabric menu and select **Nicknames** to open the Nicknames dialog.
2. Open the File menu in the Nicknames dialog, and select **Import**.
3. Select an XML nickname file in the Open dialog and click **Open**. When prompted to overwrite existing nicknames, click **Yes**.

Zoning

Zoning a fabric enables you to divide the ports and devices of the fabric into zones for more efficient and secure communication among functionally grouped nodes. This section addresses the following topics:

- Active Zone Set data window
- Configured Zonesets data window
- Zoning concepts
- Managing the zoning database
- Managing zone sets
- Managing zones
- Managing aliases
- Merging fabrics and zoning

Active Zone Set data window

The Active Zoneset data window, shown in Figure 9, displays the zone membership for the active zone set that resides on the fabric management switch. The active zone set is the same on all switches in the fabric. To open the Active Zoneset data window, click the **Active Zoneset** tab below the data window.

The Active Zoneset data window uses display conventions for expanding and contracting entries that are similar to the fabric tree. An entry handle located to the left of an entry in the tree indicates that the entry can be expanded. Click this handle or double-click the following entries:

- A zone set entry expands to show its member zones.
- A zone entry expands to show its member ports/devices.
- Ports/devices that are zoned by WWN or FC address, but no longer part of the fabric, are grayed-out.

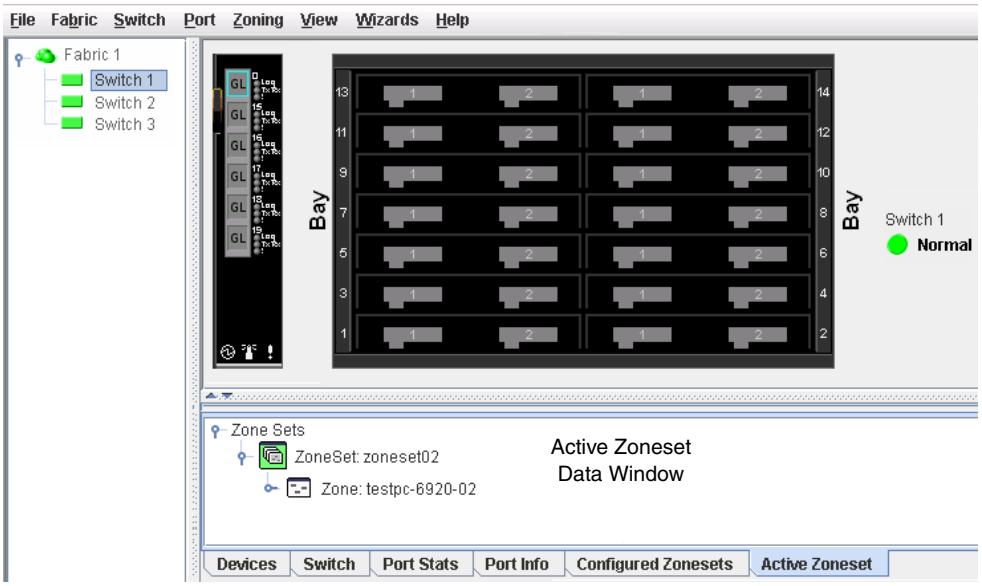

Figure 9. Active Zone Set Data window

Configured Zonesets data window

The Configured Zonesets data window, shown in Figure 10, displays all zone sets, zones, aliases, and zone membership in the zoning database. To open the Configured Zonesets data window, click the **Configured Zonesets** tab below the data window.

The Configured Zonesets data window uses display conventions for expanding and contracting entries that are similar to the fabric tree. An entry handle located to the left of an entry in the tree indicates that the entry can be expanded. Click this handle or double-click the following entries to expand or collapse them:

- A zone set entry expands to show its member zones.
- A zone entry expands to show its members by device port World Wide Name, or device port Fibre Channel address.
- The alias entry expands to show its entries.

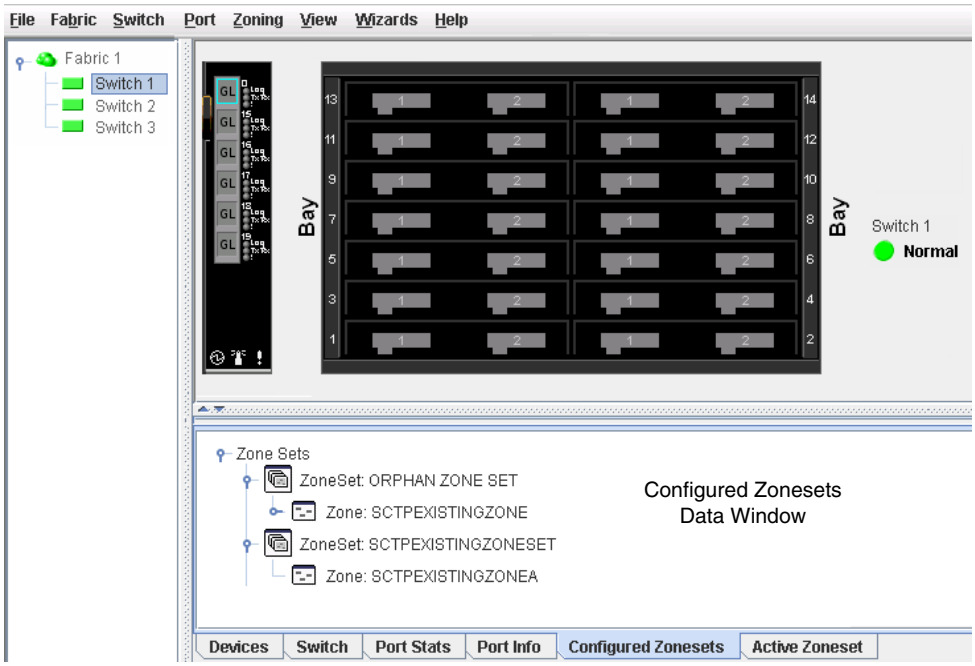

Figure 10. Configured Zonesets Data window

Zoning concepts

The following zoning concepts provide some context for the zoning tasks described in this section:

- Zones
- Aliases
- Zone sets
- Zoning database
- Configuring the zoning database

Zones

Zoning divides the fabric for purposes of controlling discovery and inbound traffic. A zone is a named group of ports or devices. Members of the same zone can communicate with each other and transmit outside the zone, but cannot receive inbound traffic from outside the zone. A port/device can be a member of up to eight zones whose combined membership does not exceed 64.

Zoning is hardware enforced on a switch port if the sum of the logged-in devices plus the devices zoned with devices on that port is 64 or less. If a port exceeds this sum, that port behaves as a soft zone member. The port continues to behave as a soft zone member until the sum of logged-in and zoned devices falls back to 64, and the port is reset.

A zone can be a component of more than one zone set. Several zone sets can be defined for a fabric, but only one zone set can be active at one time. The active zone set determines the current fabric zoning.

Membership in a zone can be defined by switch domain ID and port number, device Fibre Channel identifier address (FCID), or device World Wide Name (WWN).

- WWN entries define zone membership by the World Wide Name of the attached device. With this membership method, you can move WWN member devices to different switch ports in different zones without having to edit the member entry as you would with a domain ID/port number member. Furthermore, unlike FCID members, WWN zone members are not affected by changes in the fabric that could change the Fibre Channel address of an attached device.
- FCID entries define zone membership by the Fibre Channel address of the attached device. With this membership method you can replace a device on the same port without having to edit the member entry as you would with a WWN member.
- Domain ID/Port number entries define zone membership by switch domain ID and port number. All devices attached to the specified port become members of the zone. The specified port must be an F_Port or an FL_Port.

Aliases

To make it easier to add a group of ports or devices to one or more zones, you can create an alias. An alias is a named set of ports or devices that are grouped together for convenience. Unlike zones, aliases impose no communication restrictions between its members. You can add an alias to one or more zones. However, you cannot add a zone to an alias, nor can an alias be a member of another alias.

Zone sets

A zone set is a named group of zones. A zone can be a member of more than one zone set. Each switch in the fabric maintains its own zoning database containing one or more zone sets. This zoning database resides in non-volatile or permanent memory and is therefore retained after a reset. Refer to “Configured Zonesets data window” on page 3-27 for information about displaying the zoning database.

Notes:

Zones that are currently not in a zone set are considered to be part of the “orphan zone set.” The orphan zone set is not an actual zone set, but rather a way of displaying the zones that are not currently in a zone set.

To apply zoning to a fabric, choose a zone set and activate it. When you activate a zone set, the switch distributes that zone set and its zones, excluding aliases, to every switch in the fabric. This zone set is known as the active zone set. Refer to “Active Zone Set Data window” on page 3-26 for information about displaying the active zone set.

Zoning database

Each switch has its own zoning database. The zoning database is made up of all aliases, zones, and zone sets that have been created on the switch or received from other switches. The switch maintains two copies of the inactive zoning database: one copy is maintained in temporary memory for editing purposes; the second copy is maintained in permanent memory. Zoning database edits are made on an individual switch basis and are not propagated to other switches in the fabric when saved.

The Merge Auto Save parameter determines whether changes to the active zone set that a switch receives from another switch in the fabric will be saved to permanent memory on that switch. For information about zoning configuration, see ”Configuring the zoning database” on page 3-33.

Viewing zoning limits and properties

To view zoning limits and properties on a switch, do the following:

1. Open the Zoning menu and select **Edit Zoning** to open the Edit Zoning dialog.
2. Choose one of the following:
   - In the zone sets tree (left windowpane), right-click the top zonesets entry, a zone set, a zone, or a zone member. In the popup menu, select **Properties**.
   - In the zone set tree (left windowpane), select the top Zone Sets entry, a zone set, a zone, or a zone member. Open the Edit menu and select **Properties**.
3. View the zoning limits and properties information in the Properties dialog.
4. Click the **OK** button to close the Properties dialog.

The zoning limits are:

- **MaxZoneSets is 256**. This limit is the maximum number of zone sets that can be configured on the switch.
- **MaxZones is 2000**. This limit is the maximum number of zones that can be configured on the switch, including orphan zones.
- **MaxAliases is 2500**. This limit is the maximum number of aliases that can be configured on the switch.

- **MaxTotalMembers is 10,000**. This limit is the maximum number of zone and alias members (10,000) that can be stored in the switch's zoning database. Each instance of a zone member or alias member counts toward this maximum.
- **MaxZonesInZoneSets is 2000**. This limit is the maximum number of zone linkages to zonesets that can be configured on the switch. Every time a zone is added to a zoneset this constitutes a linkage.
- **MaxMembersPerZone is 2000**. This limit is the maximum number of zone members that can be added to any zone on the switch. Aliases are considered zone members when added to a zone.
- **MaxMembersPerAlias is 2000**. This limit is the maximum number of zone members that can be added to any alias on the switch.

Managing the zoning database

Managing the zoning database consists of the following:

- Editing the zoning database
- Configuring the zoning database
- Saving the zoning database to a file
- Restoring the zoning database from a file
- Restoring the default zoning database
- Removing all zoning definitions

Editing the zoning database

Use the Edit Zoning dialog, shown in Figure 11, to edit the zoning database for a particular switch. To open the Edit Zoning dialog, open the Zoning menu and select **Edit Zoning**. Changes can be made only to inactive zone sets, which are stored in flash (non-volatile) memory and retained after resetting a switch.

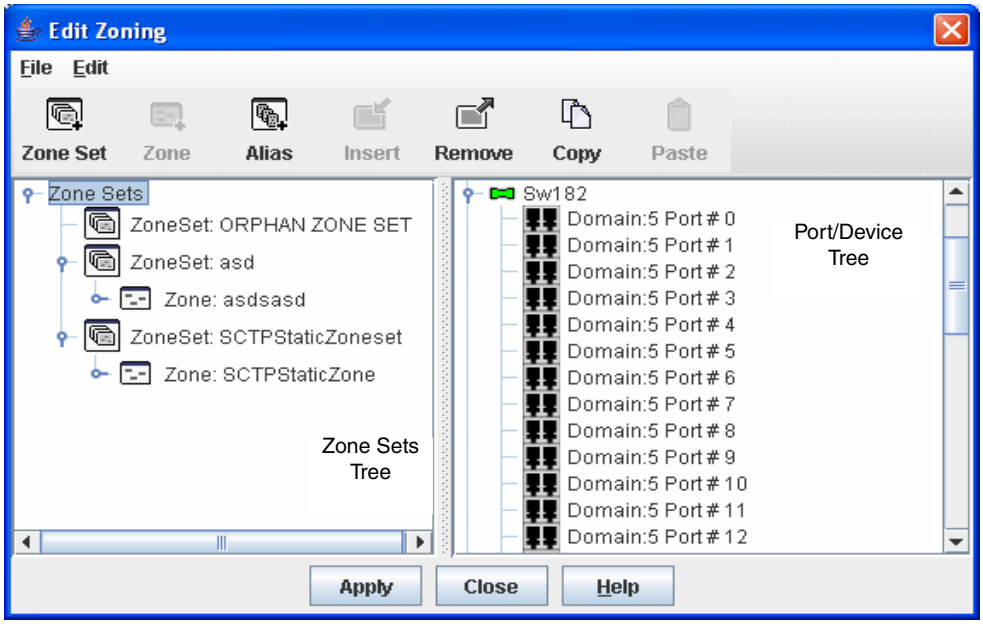

Figure 11. Edit Zoning dialog

To apply zoning to a fabric, choose a zone set and activate it. When you activate a zone set, the switch distributes that zone set and its zones, excluding aliases, to every switch in the fabric. This zone set is known as the active zone set.

You cannot edit an active zone set on a switch. You must configure an inactive zone set to your needs and then activate that updated zone set to apply the changes to the fabric. When you activate a zone set, the switch distributes that zone set to the temporary zoning database on every switch in the fabric. However, in addition to the merged active zone set, each switch maintains its own original zone set in its zoning database. Only one zone set can be active at one time.

Notes:

If the Merge Auto Save parameter is enabled on the Zoning Configuration dialog, then every time the active zone set changes, the switch will copy it into an inactive zone set stored on the switch. You can edit this copy of the active zone set stored on the switch, and activate the updated copy to conveniently apply the changes to the active zone set. The edited copy then becomes the active zone set.

The Edit Zoning dialog has a Zone Sets tree on the left and a Port/Device (or members) tree on the right. Both trees use display conventions similar to the fabric tree for expanding and contracting zone sets, zones, and ports. An expanded port shows the port Fibre Channel address; an expanded address shows the port World Wide Name. You can select zone sets, zones, and ports in the following ways:

- Click a zone, zone set, or port icon.
- Right-click to select a zone set or zone, and open the corresponding popup menu.
- Press the **Shift** key while clicking several consecutive icons.
- Press the **Control** key while clicking several non-consecutive icons.

Using tool bar buttons, popup menus, or a drag-and-drop method, you can create and manage zone sets and zones in the zoning database. Table 8 describes the zoning tool bar operations.

Use the Edit Zoning dialog to define zoning changes, and click the **Apply** button to open the Error Check dialog. Click the **Error Check** button to have QuickTools check for zoning conflicts, such as empty zones, aliases, or zone sets, and zones with non-domain ID/port number membership. Click the **Save Zoning** button to implement the changes. Click the **Close** button to close the Error Check dialog. On the Edit Zoning dialog, click the **Close** button to close the Edit Zoning dialog.

Table 8. Edit Zoning dialog tool bar buttons and icons

Button/Icon	Description
	Create Zone Set button. This button creates a new zone set.
	Create Zone button. This button creates a new zone.
	Create Alias button. This button creates another name for a set of objects.

Table 8. Edit Zoning dialog tool bar buttons and icons (Continued)

Button/Icon	Description
	Add Member button. This button adds selected port/device to a zone.
	Remove Member button. This button deletes the selected zone from a zone set, or deletes the selected port/device from a zone.
	Copy button. This button copies selected zoning items to clipboard.
	Paste button. This button pastes clipboard items to selected zoning item where applicable.
	Switch port icon. Not logged in
	Switch port icon. Logged in
	NL_Port (loop) device icon. Logged in to fabric
	NL_Port (loop) device icon. Not logged in to fabric
	N_Port device icon. Logged in to fabric
	N_Port device icon. Not logged in to fabric

Configuring the zoning database

Use the Zoning Config dialog, shown in Figure 12, to change the Merge Auto Save, Default Zone, and Discard Inactive configuration parameters. Open the Zoning menu and select **Edit Zoning Config** to open the Zoning Config dialog. After making changes, click the **OK** button to put the new values into effect.

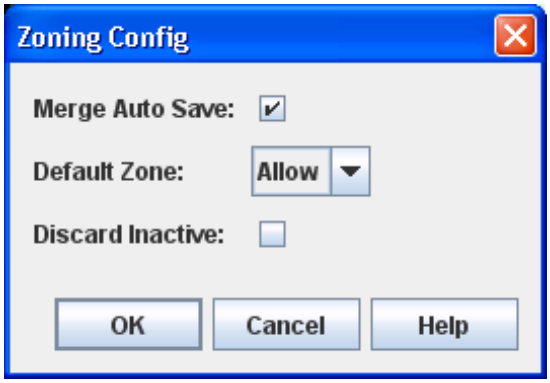

Figure 12. Zoning Config dialog

Merge auto save The Merge Auto Save parameter determines whether changes to the active zone set that a switch receives from other switches in the fabric will be saved to the zoning database on that switch. Changes are saved when an updated zone set is activated. Zoning changes are always saved to temporary memory. However, if Merge Auto Save is enabled, the switch firmware saves changes to the active zone set in temporary memory and to the zoning database. If Merge Auto Save is disabled, changes to the active zone set are stored only in temporary memory, which is cleared when the switch is reset.

Notes:

Disabling the Merge Auto Save parameter can be useful to prevent the propagation of zoning information when experimenting with different zoning schemes. However, leaving the Merge Auto Save parameter disabled can disrupt device configurations should a switch have to be reset. For this reason, the Merge Auto Save parameter should be enabled in a production environment.

Default zone The Default Zone parameter enables (True) or disables (False) communication among ports/devices that are not defined in the active zone set or when there is no active zone set. This parameter must have the same value throughout the fabric.

Discard inactive The Discard Inactive parameter automatically removes inactive zones and zone sets when a zone set is activated or deactivated from a remote switch.

Saving the zoning database to a file

You can save the zoning database to an XML file. You can later reload this zoning database on the same switch or another switch. To save a zoning database to a file, do the following:

1. Open the Zoning menu, and select **Edit Zoning**.
2. In the Edit Zoning dialog, open the File menu and select **Save As**.
3. In the Save dialog, enter a file name for the database file.
4. Click the **Save** button to save the zoning file.

Restoring the zoning database from a file

CAUTION:
Restoring the zoning database from a file will replace the current zoning database on the switch.

Do the following to restore the zoning database from a file to a switch:

1. Open the Zoning menu and select **Edit Zoning** to open the Edit Zoning window.
2. Open the File menu and select **Open File**. A popup window will prompt you to select an XML zoning database file.
3. Select a file and click **Open**.

Restoring the default zoning database

Restoring the default zoning clears the switch of all zoning definitions.

CAUTION:
This command will deactivate the active zone set.

To restore the default zoning for a switch:

1. Open the Zoning menu and select **Restore Default Zoning**.
2. Click the **OK** button to confirm that you want to restore default zoning and save changes to the zoning database.

Removing all zoning definitions

To clear all zone and zone set definitions from the zoning database, choose one of the following:

- Open the Edit menu and select **Clear Zoning**. In the Removes All dialog, click the **Yes** button to confirm that you want to delete all zones and zone sets.
- Right-click the Zone Sets heading at the top of the Zone Sets tree, and select **Clear Zoning** from the popup menu. Click the **Yes** button to confirm that you want to delete all zone sets and zones.

Managing zone sets

Zoning a fabric involves creating a zone set, creating zones as zone set members, and then adding devices as zone members. The zoning database supports multiple zone sets to serve the different security and access needs of your storage area network, but only one zone set can be active at one time. Managing zone sets consists of the following tasks:

- Creating a zone set
- Activating and deactivating a zone set
- Copying a zone to a zone set
- Removing a zone set

Notes:

Changes that you make to the zoning database are limited to the managed switch and do not propagate to the rest of the fabric. To distribute changes to configured zone sets fabric wide, you must edit the zoning databases on the individual switches.

Creating a zone set

To create a zone set, do the following:

1. Open the Zoning menu, and select **Edit Zoning** to open the Edit Zoning dialog.
2. Open the Edit menu, and select **Create Zone Set** to open the Create Zone Set dialog.
3. Enter a name for the zone set, and click the **OK** button. The new zone set name is displayed in the Zone Sets dialog. A zone set name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, -, ^, and $.
4. To create new zones in a zone set, choose one of the following:
   - Right-click a zone set and select **Create A Zone** from the popup menu. In the Create a Zone dialog, enter a name for the new zone, and click the **OK** button. The new zone name is displayed in the Zone Sets dialog.
   - Copy an existing zone by dragging a zone into the new zone set. Refer to "Copying a zone to a zone set" on page 3-37.
5. Click the **Apply** button to save changes to the zoning database.

Activating and deactivating a zone set

You must activate a zone set to apply its zoning definitions to the fabric. Only one zone set can be active at one time. When you activate a zone set, the switch distributes that zone set to the temporary zoning database on every switch in the fabric.

The purpose of the deactivate function is to suspend all fabric zoning, which results in free communication fabric wide or no communication. It is not necessary to deactivate the active zone set before activating a new one.

- To activate a zone set, open the Zoning menu and select **Activate Zone Set** to open the Activate Zone Set dialog. Select a zone set from the Select Zone Set drop-down list, and click the **Activate** button.
- To deactivate the active zone set, open the Zoning menu, select **Deactivate Zone Set**. Acknowledge the warning about traffic disruption, and click the **Yes** button to confirm that you want to deactivate the active zone set.

Renaming a zone set

To rename a zone set, do the following:

1. In the Zone Sets tree of the Edit Zoning dialog, click the zone set to be renamed.
2. Open the Edit menu and select **Rename**.
3. In the Rename Zone Set dialog, enter a new name for the zone set.
4. Click the **OK** button.

Removing a zone set

Removing a zone set from the database affects the member zones in the following ways:

- Member zones that are members of other zone sets are not affected.
- Zones that are currently not in a zone set are considered to be part of the "orphan zone set." The orphan zone set is not an actual zone set, but rather a way of displaying the zones that are not currently in a zone set.

To remove a zone set, do the following:

1. Open the Zoning menu and select **Edit Zoning** to open the Edit Zoning dialog.
2. In the Zone Sets tree, select the zone set to be removed.
3. Open the Edit menu, and select **Remove** to remove the zone set.
4. Click the **Apply** button to save changes to the zoning database.

Alternatively, you may use shortcut menus to remove a zone set from the database.

Managing zones

Managing zones involves the following:

- Creating a zone in a zone set
- Adding zone members
- Renaming a zone
- Removing a zone member
- Removing a zone from a zone set
- Removing a zone from all zone sets

Notes:

Changes that you make to the zoning database are limited to the managed switch and do not propagate to the rest of the fabric. To distribute changes to configured zone sets fabric wide, you must edit the zoning databases on the individual switches.

Creating a zone in a zone set

To create a zone in a zone set, do the following:

1. Open the Zoning menu, and select **Edit Zoning** to open the Edit Zoning dialog.
2. Select a zone set.
3. Open the Edit menu and select **Create a Zone**.
4. In the Create a Zone dialog, enter a name for the new zone, and click the **OK** button. The new zone name is displayed in the Zone Sets dialog. A zone name must begin with a letter and be no longer than 64 characters. Valid characters are 0–9, A–Z, a-z, _, ^, $,and -.

   Notes:

   If you enter the name of a zone that already exists in the database, QuickTools prompts you to add that zone and its membership to the zone set.

5. To add switch ports or attached devices to the zone, choose one of the following:
   - In the zone set tree, select the zone set. In the graphic window, select the port to add to the zone. Open the Edit menu and select **Add Members**.
   - Select a port by port number, Fibre Channel address, or World Wide Name in the Port/Device tree, and drag it into the zone.
   - Select a port by port number, Fibre Channel address, or World Wide Name in the Port/Device tree. Right-click the zone and select **Add Zone Members** from the popup menu.
6. Click the **Apply** button to save changes to the zoning database.

Copying a zone to a zone set

To copy an existing zone and its membership from one zone set to another, do the following:

1. In the faceplate display, open the Zoning menu and select **Edit Zoning** to open the Edit Zoning dialog.
2. In the zone set tree, select the zone to copy, and drag it to the chosen zone set.
3. Click the **OK** button to display the Error Check dialog.
4. Click the **Error Check** button to have the application check for zoning conflicts, such as empty zones, aliases, or zone sets.
5. Click the **Save Zoning** button to implement the changes.
6. Click the **Close** button to close the Error Check dialog.

Adding zone members

You can zone a port/device by switch domain ID and port number, device port Fibre Channel address, or the device port WWN. Adding a port/device to a zone affects every zone set in which that zone is a member. To add ports/devices to a zone, do the following:

1. Open the Zoning menu, and select **Edit Zoning** to open the Edit Zoning dialog.
2. Choose one of the following methods to add the port/device:
   - Select a port/device in the Port/Device tree, and drag it into the zone. To select multiple ports/devices, press the **Control** key while selecting.
   - Select a port/device in the Port/Device tree. To select multiple ports/devices, press the **Control** key while selecting. Select a zone set in the left pane. Open the Edit menu and select **Add Members**.
   - Select a port/device in the Port/Device tree. To select multiple ports/devices, press the **Control** key while selecting. Select a zone set in the left pane. Click the **Insert** button.

   If the port/device you want to add is not in the Port/Device tree, you can add it by doing the following:

   a. Right-click the selected zone.

   b. Open the Edit menu and select **Create Members**.

   c. Select the **WWN**, **Domain/Port**, or **First Port Address** option.

   d. Enter the hexadecimal value for the port/device according to the option selected: 16 digits for a WWN member, 4 digits for a Domain/Port member (DDPP), or a 6-digit Fibre Channel Address for a First Port Address member (DDPPAA) where D=domain ID, P=port number, and A=ALPA.
3. Click the **OK** button to display the Error Check dialog.
4. Click the **Error Check** button to have the application check for zoning conflicts, such as empty zones, aliases, or zone sets.
5. Click the **Save Zoning** button to implement the changes.
6. Click the **Close** button to close the Error Check dialog.
7. On the Edit Zoning dialog, click the **Close** button to close the Edit Zoning dialog.

Notes:

Domain ID conflicts can result in automatic reassignment of switch domain IDs. These reassignments are not reflected in zones that use domain ID/port number pair to define their membership. Be sure to reconfigure zones that are affected by a domain ID change.

Renaming a zone

To rename a zone, do the following:

1. In the Zone Sets tree of the Edit Zoning dialog, click the zone to be renamed.
2. Open the Edit menu and select **Rename**.
3. In the Rename Zone dialog, enter a new name for the zone.
4. Click the **OK** button.

Removing a zone member

Removing a zone member will affect every zone and zone set in which that zone is a member. To remove a member from a zone:

1. In the Edit Zoning dialog, select the zone member to be removed.
2. Open the Edit menu and select **Remove**.
3. Click the **Yes** button in the Remove dialog to save the change.
4. Click the **Apply** button in the Edit Zoning dialog to save the change.
5. Click the **Close** button to close the Edit Zoning dialog.

Removing a zone from a zone set

To remove a zone from a zone set, do the following:

1. In the Edit Zoning dialog, select the zone to be removed. The selected zone will be removed only from that zone set.
2. Open the Edit menu and select **Remove**.
3. Click the **Yes** button in the Remove dialog to save the change.
4. Click the **Apply** button in the Edit Zoning dialog to save the change.
5. Click the **Close** button to close the Edit Zoning dialog.

Removing a zone from all zone sets

To remove a zone from all zone sets, do the following:

1. In the Edit Zoning dialog, select the zone to be removed.
2. Open the Edit menu and select **Delete Zone**.
3. Click the **Yes** button in the Remove dialog to save the change.
4. Click the **Apply** button in the Edit Zoning dialog to save the change.
5. Click the **Close** button to close the Edit Zoning dialog.

Managing aliases

An alias is a collection of objects that can be zoned together. An alias is not a zone, and cannot have a zone or another alias as a member.

Notes:

Changes that you make to the zoning database are limited to the managed switch and do not propagate to the rest of the fabric. To distribute changes to configured zone sets fabric wide, you must edit the zoning databases on the individual switches.

You will not see aliases in the active zone set.

Creating an alias

To create an alias, do the following:

1. Open the Zoning menu, and select **Edit Zoning** to open the Edit Zoning dialog.
2. Open the Edit menu, and select **Create Alias** to open the Create Alias dialog.
3. Enter a name for the alias, and click the **OK** button. The alias name is displayed in the Zone Sets dialog. An alias name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, $, ^, and -.
4. Click the **Apply** button to save the alias name to the zoning database.

Adding a member to an alias

You can add a port/device to an alias by domain ID and port number, device port Fibre Channel address, or the device port WWN. To add ports/devices to an alias, do the following:

1. Open the Zoning menu, and select **Edit Zoning** to open the Edit Zoning dialog.
2. Choose one of the following methods to add the port/device:
   - Select a port/device in the Port/Device tree, and drag it into the alias. To select multiple ports/devices, press the **Control** key while selecting.
   - Select a port/device in the Port/Device tree. Click an alias to select it, or to select multiple ports/devices, press the **Control** key while selecting. Select an alias. Open the Edit menu and select **Add Members**.
   - Select a port/device in the Port/Device tree. To select multiple ports/devices, press the **Control** key while selecting. Select an alias. Click the **Insert** button.

   If the port/device you want to add is not in the Port/Device tree, you can add it by doing the following:

   a. Right-click the selected alias.

   b. Open the Edit menu and select **Create Members**.

   c. Select the **WWN**, **Domain/Port**, or **First Port Address** option.

   d. Enter the hexadecimal value for the port/device according to the option selected: 16 digits for a WWN member, 4 digits for a Domain/Port member (DDPP), or a 6-digit Fibre Channel Address for a First Port Address member (DDPPAA) where D=domain ID, P=port number, and A=ALPA.
3. Click the **OK** button to add the member and save the change.

Removing an alias from all zones

To remove an alias from all zones, do the following:

1. In the Zone Sets tree in the Edit Zoning dialog, select the alias to be removed.
2. Open the Edit menu, and select **Delete Alias**.
3. Click the **Yes** button in the Remove dialog to save the change.
4. Click the **Apply** button in the Edit Zoning dialog to save the change.
5. Click the **Close** button to close the Edit Zoning dialog.

Merging fabrics and zoning

If you join two fabrics with an inter-switch link, the active zone sets from the two fabrics attempt to merge automatically. The fabrics may consist of a single switch or many switches already connected together. The switches in the two fabrics attempt to create a new active zone set containing the union of each fabric's active zone set. The propagation of zoning information only affects the active zone set, not the configured zone sets, unless Merge Auto Save is turned on.

Zone merge failure

If a zone merge is unsuccessful, the inter-switch links between the fabrics will isolate due to a zone merge failure, which will generate an alarm. The reason for the E_Port isolation can also be determined by viewing the port information. Refer to Table 25 for more information.

A zone merge will fail if the two active zone sets have member zones with identical names that differ in membership or type. For example, consider Fabric A and Fabric B each with a zone named “ZN1” in its active zone set. Fabric A "ZN1" contains a member specified by Domain ID 1 and Port 1; Fabric B “ZN1” contains a member specified by Domain ID 1 and Port 2. In this case, the merge will fail because the two zones have the same name, but different membership.

A zone merge may also fail if the merged zones/members exceeds the max zoning limits. Refer to ”Viewing zoning limits and properties” on page 3-29 for more information on zoning limits.

Zone merge failure recovery

When a zone merge failure occurs, the conflict that caused the failure must be resolved. You can correct a failure due to a zone conflict by deactivating one of the active zone sets or by editing the conflicting zones so that their membership is the same. You can deactivate the active zone set on one fabric if the active zone set on the other fabric accurately defines your zoning needs. If not, you must edit the zone memberships, and reactivate the zone sets. After correcting the zone membership, reset the isolated ports to allow the fabrics to join.

Notes:

If you deactivate the active zone set in one fabric and the Merge Auto Save parameter is enabled, the active zone set from the second fabric will propagate to the first fabric and replace all zones with matching names in the configured zone sets.

For information about adding and removing zone members, see ”Managing zones” on page 3-36. For information about resetting a port, see ”Resetting a port” on page 5-105.

Chapter 4. Managing switches

This chapter describes the following topics:

- Using the Switch data window
- Managing user accounts
- Paging a switch
- Setting the date/time and enabling NTP Client
- Resetting a switch
- Configuring a switch
- Configuring the network
- Configuring SNMP
- Archiving a switch
- Restoring a switch
- Restoring the factory default configuration
- Downloading a support file
- Installing feature license keys
- Installing firmware
- Configuring server authentication
- Using Call Home

Using the Switch data window

The Switch data window, shown in Figure 13, displays the current network and switch information for the selected switch. To open the Switch data window, click the **Switch** tab below the data window.

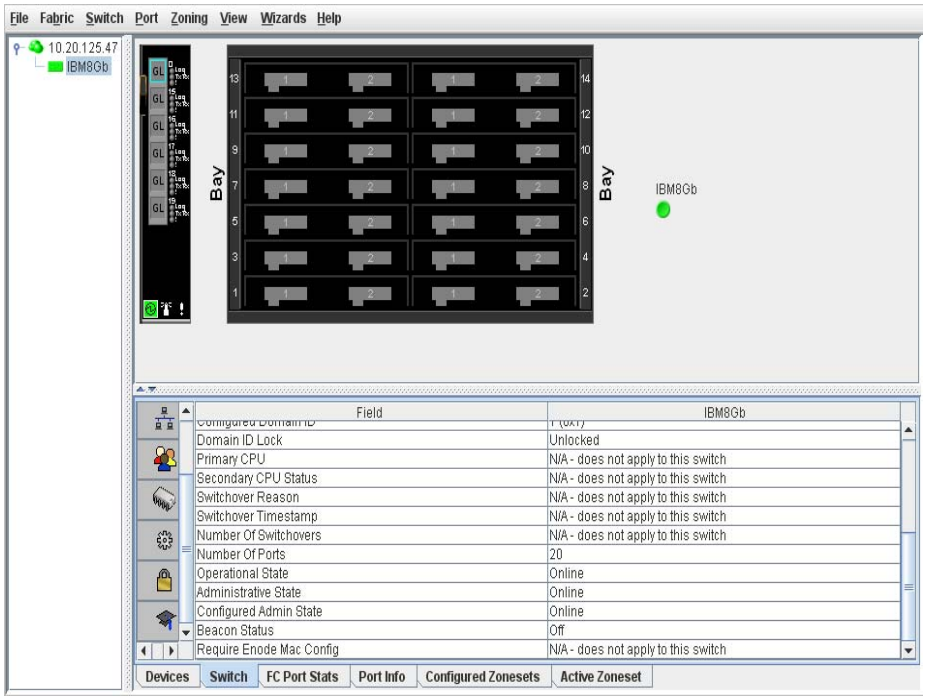

Figure 13. Switch data window

Information in the Switch data window is grouped and accessed by the Summary, Status, Network, User Login, Firmware, Services, Zones/Security, and Advanced buttons. Click a button to display the grouped information in the data window on the right. Figure 14 describes the Switch data window buttons.

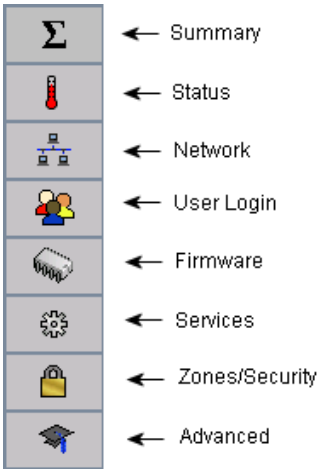

Figure 14. Switch data window buttons

The Switch data window entries are listed in Table 9.

Table 9. Switch data window entries

Entry	Description
Summary Group	
Switch Type	Switch model
First Port Address	Switch Fibre Channel address
World Wide Name	Switch world wide name
Serial Number	Number assigned to each chassis
Reason for Status	The reason for the operational state.
Vendor	Switch manufacturer
MAC Address	Media Access Control address
Switch UUID	The switch's universally unique ID
CPLD Revision	Complex Programmable Logic Device revision
Negotiated Domain ID	The domain ID currently being used by the fabric
Configured Domain ID	The domain ID defined by network administrator
Domain ID Lock	Domain ID lock status. Prevents (True) or permits (False) dynamic domain ID reassignment
Number of Ports	Number of ports activated on the switch
Operational State	Switch operational state: Online, Offline, Diagnostic, Down
Administrative State	Current switch administrative state
Configured Admin State	Switch administrative state that is stored in the switch configuration
Beacon Status	Beacon status. Switch LEDs are blinking (On) or not (off).
Status Group	
Operational State	Switch operational state: Online, Offline, Diagnostic, Down
Administrative State	Current switch administrative state
Configured Admin State	Switch administrative state that is stored in the switch configuration
Beacon Status	Beacon status. Switch LEDs are blinking (On) or not (off).
Reason for Status	The reason for the operational state
Temperature	Internal switch temperature in degrees Celsius
Fan 1 Status	NA—does not apply to this switch
Fan 2 Status	NA—does not apply to this switch
Fan 3 Status	NA—does not apply to this switch
Power Supply 1 Status	NA—does not apply to this switch

Table 9. Switch data window entries (Continued)

Entry	Description
Power Supply 2 Status	NA—does not apply to this switch
Temperature Failure Port Shutdown	Non-configurable (always enabled for this switch). All ports are shut down when the switch temperature exceeds the failure temperature.
Board Temperature	Current internal temperature in degrees Celsius
Board Warning Temperature	Non-configurable temperature threshold (65° Celsius) above which a warning condition alarm is generated
Board Failure Temperature	Non-configurable temperature threshold (70° Celsius) above which a failure condition alarm is generated
POST Status	Status from the most recent Power On Self Test
POST Fault Code	Fault code from the most recent Power On Self Test
Test Status	The current diagnostic test status for the switch
Test Fault Code	The code value for the last recorded diagnostic test status recorded on the switch
Network Group	
IPv4 Enabled	Internet Protocol version 4 enabled status
IPv4 Address	Internet Protocol version 4 IP address for the External management port
IPv4 Subnet Mask	Mask that determines the IP address subnet
IPv4 Gateway	Gateway address
IPv6 Enabled	Internet Protocol version 6 enabled status
IPv6 Address	Mask that determines the IP address subnet for the External management port
IPv6 Gateway	Gateway address
Eth1 IPv4 Address	Mask that determines the Eth1 IPv4 address for the Internal management port
Eth1 IPv4 Subnet Mask	Mask that determines the IPv4 address subnet for Eth1
Eth1 IPv4 Gateway	Gateway address
Eth1 IPv6 Address	Mask that determines theIPv6 IP address for Eth1 for the External management port
Eth1 IPv6 Gateway	Gateway address
CPU0 MAC Address	NA—does not apply to this switch
CPU1 MAC Address	NA—does not apply to this switch
SNMP Enabled	SNMP enabled or disabled
SNMP v3 Security Enabled	SNMP v3 security enabled or disabled

Table 9. Switch data window entries (Continued)

Entry	Description
Broadcast Support	Broadcast support status. Broadcast support is enabled (default) or disabled.
NTP Client Enabled	Enabled or disabled. Allows for switches to synchronize their time to a centralized server
NTP Server Address	The IP address of the centralized NTP server. Ethernet connection to NTP server is required.
Use Front Port	N/A—does not apply to this switch
DNS Enabled	DNS enabled status
Configured Local Hostname	Hostname for the switch. If a fully qualified domain name is given, the domain suffix is used as the first suffix in the DNS search list for DNS lookups performed by the switch.
IPv6 Assigned Address (1–20)	The set of IPv6 addresses assigned by DHCPv6, NDP, or the switch administrator
Assigned Hostname	Name assigned to host
User Login Group	
User Name	Account name
Login Level	Authority level
Super User	Super user privileges enabled/disabled
UserAuthentication Enabled	Enforcement of account names and authority (always True)
Firmware Group	
Firmware Version	Active firmware version
Inactive Firmware Version	N/A—does not apply to this switch
Pending Firmware Version	Firmware version that will be activated at the next reset
PROM/Boot Version	PROM firmware version
Services Group	
NTP Client Enabled	Enabled or disabled. Allows for switches to synchronize their time to a centralized server
NTP Server Address	The IP address of the centralized NTP server. Ethernet connection to NTP server is required.
FDMI Enable	Fabric Device Management Interface status. If enabled, device information can be obtained, managed, and saved through the fabric using Name Service Management Server functions. QuickTools will report all FDMI information reported by the entry switch, if FDMI is enabled on the entry switch.
FDMI HBA Entry Limit	Maximum number of adapters that can be registered with a switch

Table 9. Switch data window entries (Continued)

Entry	Description
Embedded GUI Enabled	QuickTools web applet status. Enables or disables the web applet on the switch
Inactivity Timeout	Number of minutes the switch waits before terminating an idle command line interface session. Zero (0) disables the time out threshold.
GUI Mgmt Enabled	Web applet status. If disabled, the switch cannot be managed using the web applet.
Telnet Enabled	Telnet client status
SSH Enabled	Secure Shell status. If enabled, an encrypted data path is provided for command line interface sessions.
SSL Enabled	Secure Sockets Layer status. If enabled, encryption for switch management web applet and CIM sessions is provided.
CIM Enabled	Common Information Model status. The Common Information Model (CIM) agent is based on the SNIA Storage Management Initiative Specification (SMI-S), which is the standard for SAN management in a heterogeneous environment.
SLP Enabled	Service location protocol status
FTP Enabled	FTP status
Management Server Enabled	Management server status
SNMP Enabled	SNMP enabled or disabled
Call Home Enabled	If enabled and configured, switches can send alerts and events to pagers and Email. Users can configure the type of events and where the alerts are sent.
Zones/Security Group	
Interop Mode	Non-configurable. Zoning merge status. When a zone set is activated on an FC-SW-2 compliant switch, only the active zone set is propagated to all switches in the fabric. When a zone set is activated on a non-FC-SW-2 compliant switch, the active zone set and all inactive zone sets (the entire zoning database) are stored in permanent memory.
Legacy Address Format	Non-configurable. Legacy port addressing status. Enabled only for interoperability with non-FC-SW-2 compliant switches
Merge Auto Save	Zoning auto save status. Saves zoning updates in temporary memory and the zoning database (True) or only in temporary memory (False)
Zoning Default Visibility	N/A—does not apply to this switch
Default Zone	Disables communication between ports and devices not defined in the active zone set, or when there is no active zone set

Table 9. Switch data window entries (Continued)

Entry	Description
Discard Inactive	Automatically removes the previously active zone set when a zone set is activated on a switch
Implicit Hard Zoning	Introduces hardware enforcement of zoning regardless of type. All zones and all supported zone member types will have hardware enforcement.
Security Auto Save	If enabled, the security configuration is saved to non-volatile memory on the switch. If disabled, the security file is saved only to temporary memory. The Auto Save feature is used when Fabric Binding is enabled. When Auto Save is disabled, any updates from remote switches will not be saved locally
Security Fabric Binding Enable	If enabled, it is required that the expected domain ID of a switch be verified before being allowed to attach to the fabric.
Advanced Group	
R_A_TOV	Resource allocation timeout value
E_D_TOV	Error detect timeout value
Number of Donor Groups	Total number of donor port groups. A donor group is a set of ports on a switch that can donate buffer credits to each other.
Inactivity Timeout	Number of minutes the switch waits before terminating an idle command line interface session. Zero (0) disables the time out threshold.
Interop Mode	Non-configurable. Zoning merge status. When a zone set is activated on an FC-SW-2 compliant switch, only the active zone set is propagated to all switches in the fabric. When a zone set is activated on a non-FC-SW-2 compliant switch, the active zone set and all inactive zone sets (the entire zoning database) are stored in permanent memory.
Legacy Address Format	Non-configurable. Legacy port addressing status. Enabled only for interoperability with non-FC-SW-2 compliant switches
In-band Enabled	In-band management status. Permits (True) or prevents (False) a switch from being managed over an inter-switch link (ISL)
Principal Switch	If there is a domain ID conflict in the fabric, the switch with the highest principal priority, or the principal switch, will reassign any domain ID conflicts and establish the fabric.

Managing user accounts

Only the Admin account can manage user accounts with the User Account Administration dialogs. However, any user can modify their own password. To open the User Account Administration dialogs, open the Switch menu and select **User Accounts**. A user account consists of the following:

- Account name or login
- Password
- Authority level
- Expiration date

Switches come from the factory with the user accounts listed in Table 10:

Table 10. Factory user accounts

Account Name	Password	Admin Authority	Expiration
USERID	PASSW0RD	true	never expires
images	images	false	never expires

The USERID account is the only user that can manage all user accounts with the User Account Administration dialogs. The USERID account can create, remove, or modify user accounts, and change account passwords. The USERID account cannot be removed.

Users with Admin authority can view and modify the switch and its configuration using QuickTools. Users without Admin authority are limited to viewing switch status and configuration.

The Images account exchanges files with the switch using sFTP. The Images account cannot be removed.

Notes:

If the same user account exists on a switch and its RADIUS server, that user can login with either password, but the authority and account expiration will always come from the switch database.

Creating user accounts

To create a user account on a switch, open the Switch menu and select **User Accounts** to open the User Account Administration dialog shown in Figure 15. A switch can have a maximum of 15 user accounts.

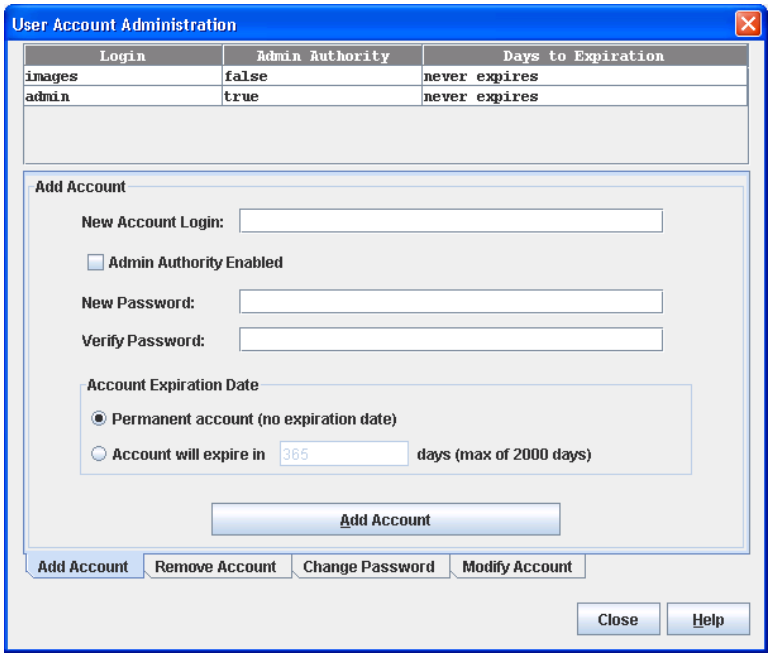

Figure 15. User Account Administration dialog – add account

1. To open the User Account Administration dialogs, open the Switch menu and select **User Accounts**.
2. Click the **Add Account** tab to open the Add Account tab page.
3. Enter an account name in the New Account Login field. Account names are limited to 15 characters.
4. If the account is to have the ability to modify switch configurations, select the **Admin Authority Enabled** option.
5. Enter a password in the New Password field and enter it again in the Verify Password field. A password must have a minimum of 8 characters and no more than 20.
6. If this account is to be permanent with no expiration date, select the **Permanent Account** option. Otherwise, click the **Account Will Expire** button and enter the number days in which the account will expire.
7. Click the **Add Account** button to add the newly defined account.

Removing a user account

To remove a user account on a switch, open the Switch menu and select **User Accounts**. Click the **Remove Account** tab in the User Account Administration dialog to present the dialog shown in Figure 16. Select the account (login) name from the list of accounts at the top of the dialog and click the **Remove Account** button.

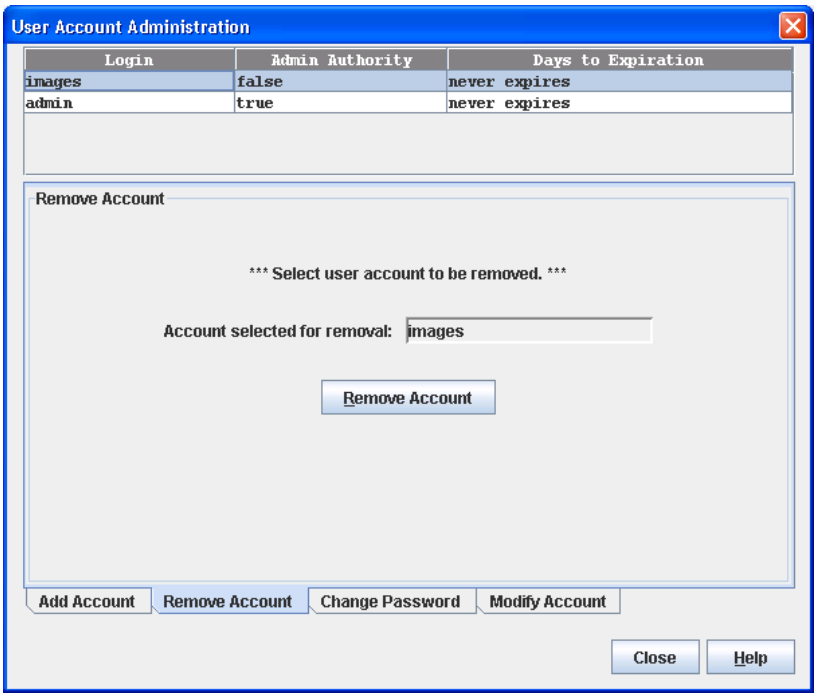

Figure 16. User Account Administration dialog—remove account

Changing a user account password

To change the password for an account on a switch, open the Switch menu and select **User Accounts**. Click the **Change Password** tab in the User Account Administration dialog to present the display shown in Figure 17. Select the account (login) name from the list of accounts at the top of the dialog, and then enter the old password, the new password, and verify the new password in the corresponding fields. Click the **Change Password** button. Any user can change their password for their account, but only the Admin account name can change the password for another user's account. If the administrator does not know the user's original password, the administrator must remove the account and add the account.

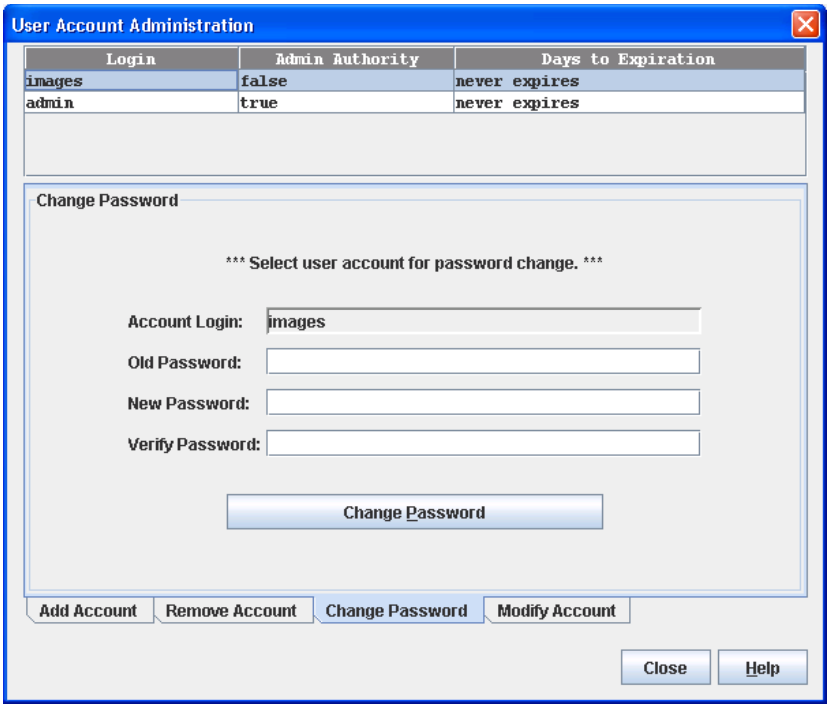

Figure 17. User Account Administration dialog—change password

Modifying a user account

To modify a user account on a switch, open the Switch menu and select **User Accounts**. Click the **Modify Account** tab in the User Account Administration dialog to present the display shown in Figure 18. Select the account (login) name from the list of accounts at the top of the dialog. Select the Admin Authority Enabled option to grant admin authority to the account name. Select an Account Expiration Date option. If the account is not to be permanent, enter the number of days until the account expires. Click the **Modify Account** button to save the changes. Click the **Close** button to close the User Account Administration dialog.

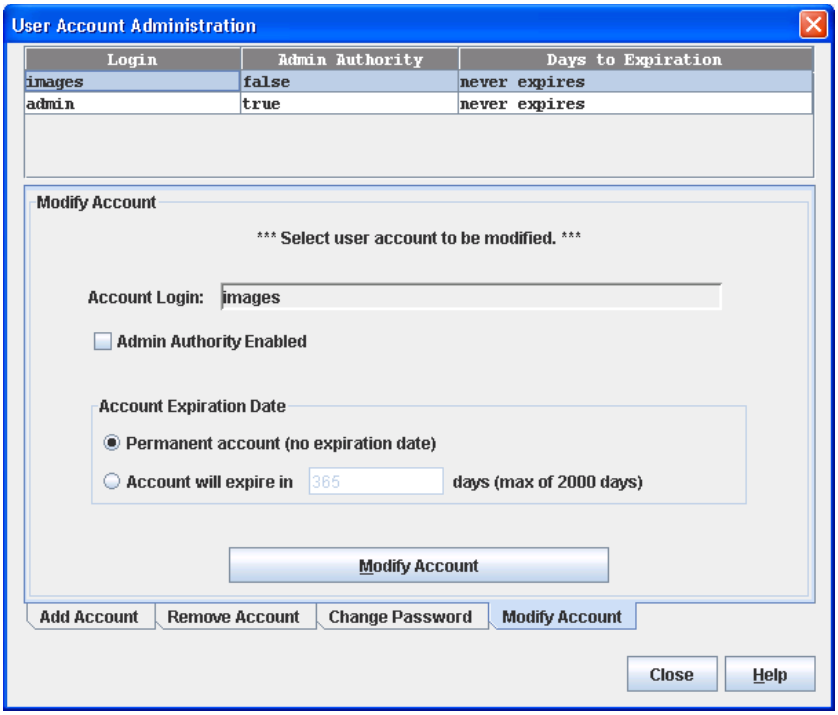

Figure 18. User Account Administration dialog—modify account

Paging a switch

Use the toggle beacon feature to cause all Logged-In LEDs to flash, making the switch easier to visually recognize. To page a switch, open the Switch menu in the faceplate display and select **Toggle Beacon**. To cancel the beacon, reselect **Toggle Beacon**.

Setting the date/time and enabling NTP Client

The Date/Time dialog allows you to manually set the date, time, and time zone on a switch, or to enable Network Time Protocol (NTP) Client to synchronize the date and time on the switch with an NTP server. Enabling the NTP client requires an Ethernet connection to an NTP server, but ensures the consistency of date and time stamps in alarms and log entries. When the date/time is set or displayed in the firmware, it is always in Universal Time. However, when displayed in the Date/Time dialog, the value is always in local time. If the NTP Client Enabled option is selected (default is un-selected), the Date and Time areas becomes inactive, thus preventing you from manually setting the date and time on the switch. The NTP Server Discovery and NTP Server IP Address fields become active, and allow you to select a discovery method (Static, DHCP, DHCPv6) and to specify an IP address.

Notes:

The difference between switch and workstation times must not exceed 24 hours, or the switch management application cannot connect using SSL.

To manually set the date and time on a switch, do the following:

1. Open the Switch menu, and select **Set Date/Time**.
2. In the NTP area of the Date/Time dialog, clear (un-select) the **NTP Client Enabled** option. The fields in the Date and Time areas become active.
3. Enter the day, year, hour, and minutes.
4. Select a month and time zone from the drop-down lists.
5. Click the **OK** button. The new date and time take effect immediately.

To synchronize the date and time on the switch with an NTP server, do the following:

1. Open the Switch menu, and select **Set Date/Time**.
2. In the NTP area of the Date/Time dialog, select the **NTP Client Enabled** option. The fields in the Date and Time areas become in-active.
3. Select a time zone from the **Select Time Zone** drop-down list.
4. Select an **NTP Server Discovery** option from the drop-down list.
5. Enter an NTP Server IP Address.
6. Click the **OK** button.

Resetting a switch

Resetting a switch reboots the switch using configuration parameters in memory. Depending on the reset type, a switch reset may include a Power On Self Test or it may disrupt traffic. Table 11 describes the types of switch resets.

During a hot reset operation, fabric services will be unavailable for a short period (30–75 seconds). Verify all administrative changes to the fabric (if any) are complete before performing a non-disruptive code load and activation (NDCLA). When upgrading firmware across a fabric using non-disruptive activation, upgrade one switch at a time and allow 75 seconds between switches.

CAUTION:
Changes to the fabric may disrupt the NDCLA process.

Common administrative operations that change the fabric include:

- Zoning modifications
- Adding, moving or removing devices attached to the switch fabric. This operation includes powering up or powering down attached devices.
- Adding, moving, or removing ISLs or other connections

After an NDCLA operation is complete, management connections must be re-initiated:

- QuickTools sessions will re-connect automatically.
- Telnet sessions must be restarted manually.

Applicable code versions:

- Future switch firmware releases will upgrade non-disruptively unless specifically indicated in the associated release notes.
- A nondisruptive upgrade to previous switch firmware releases is not supported.

Table 11. Switch reset types

Type	Description
Hot reset	Resets a switch without a Power On Self Test. This reset activates the pending firmware, but does not disrupt switch traffic. If errors are detected on a port during a hot reset, the port is reset automatically.
Reset	Resets a switch without a Power On Self Test. This reset activates the pending firmware and disrupts traffic.
Hard reset	Resets a switch with a Power On Self Test. This reset activates the pending firmware and disrupts traffic.

To reset a switch using QuickTools, do the following:

1. Select the switch to be reset in the fabric tree.
2. Open the Switch menu and select the **Reset Switch**:
   - Select **Hot Reset** to perform a hot reset.
   - Select **Reset** to perform a standard reset.
   - Select **Hard Reset** to perform a hard reset.

Configuring a switch

The switch configuration is divided into three areas: chassis, network, and SNMP. Chassis configuration specifies switch-wide Fibre Channel settings. Network configuration specifies IP settings, remote logging, and the NTP client. SNMP configuration specifies SNMP settings and traps.

Setting switch properties

To open the Switch Properties dialog (Figure 19), choose one of the following:

- Open the faceplate display for the switch you are configuring. Open the Switch menu and select **Switch Properties**.
- Right-click a switch graphic in the faceplate display, and select **Switch Properties** from the popup menu.

Use the Switch Properties dialog to change the following switch configuration parameters:

- Domain ID and domain ID lock
- Syslog
- Symbolic name
- Switch administrative states
- Broadcast support
- In-band management
- Fabric Device Management Interface

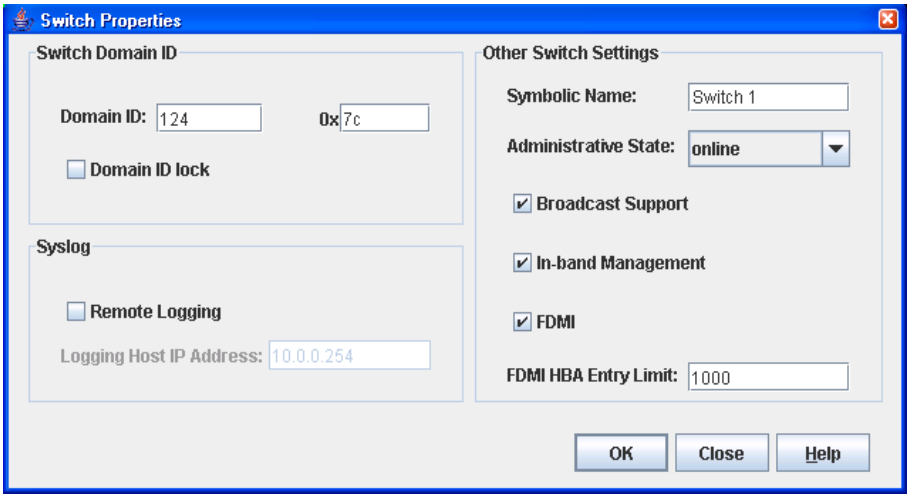

Figure 19. Switch Properties dialog

Domain ID and domain ID lock

The domain ID is a unique Fibre Channel identifier for the switch. The Fibre Channel address consists of the domain ID, port ID, and the Arbitrated Loop Physical Address (ALPA). The maximum number of switches within a fabric is 239 with each switch having a unique domain ID.

The Lenovo Flex System FC3171 8 Gb SAN Switch comes from the factory with the domain ID unlocked. This state means that if there is a domain ID conflict in the fabric, the switch with the highest principal priority, or the principal switch, will reassign any domain ID conflicts and establish the fabric. If you lock the domain ID on a switch and a domain ID conflict occurs, one of the switches will isolate as a separate fabric and the Logged-In LEDs on both switches will flash to show the affected ports. Refer to the *IBM Flex System FC3171 8 Gb SAN Switch Command Line Interface User's Guide* for information about the Set Config Switch command and the DomainIDLock and PrincipalPriority parameters.

If you connect a new switch to an existing fabric with its domain ID unlocked, and a domain conflict occurs, the new switch will isolate as a separate fabric. However, you can remedy this by resetting the new switch or taking it offline then back online. The principal switch will reassign the domain ID and the switch will join the fabric.

Notes:

Domain ID reassignment is not reflected in zoning that is defined by domain ID and port number pair. You must reconfigure zones that are affected by domain ID reassignment.

Syslog

The Syslog (Remote Logging) feature enables saving log information to a remote host that supports the syslog protocol. When enabled, the log entries are sent to the syslog host at the IP address that you specify in the Logging Host IP Address field. Log entries are saved in the internal switch log whether this feature is enabled or disabled.

To save log information to a remote host, you must edit the syslog.conf file (located on the remote host) and then restart the syslog daemon. Consult your operating system documentation for information on how to configure Remote Logging. The syslog.conf file on the remote host must contain an entry that specifies the name of the log file in which to save error messages. Add the following line to the syslog.conf file. A <tab> separates the selector field (local0.info) and action field that contains the log file path name (/var/adm/messages/messages.name).

```
local0.info <tab> /var/adm/messages.name
```

Symbolic name

The symbolic name is a user-defined name of up to 32 characters that identifies the switch. The symbolic name is used in the displays and data windows to help identify switches. The illegal characters are the pound sign (#), semi-colon (;), and comma (,).

Switch administrative states

The switch administrative state determines the operational state of the switch. The switch administrative state exists in two forms: the configured administrative state and the current administrative state.

- Configured administrative state—the state that is saved in the switch configuration and is preserved across switch resets. QuickTools always makes changes to the configured administrative state. The configured administrative state is displayed in the Switch Properties dialog.
- Current administrative state—the state that is applied to the switch for temporary purposes and is not retained across switch resets. The current administrative state is set using the Set Switch command.

Table 12 describes the switch administrative state values.

Table 12. Switch administrative states

Parameter	Description
Online	The switch is available.
Offline	The switch is unavailable.
Diagnostics	The switch is in diagnostics mode, is unavailable, and tests can be run on all ports.

Broadcast support

Broadcast is supported on the switch and allows for TCP/IP support. Broadcast is implemented using the proposed standard specified in *Multi-Switch Broadcast for FC-SW-3, T11 Presentation Number T11/02-031v0*. Fabric Shortest Path First (FSPF) is used to set up a fabric spanning tree used in transmission of broadcast frames. Broadcast frames are retransmitted on all ISLs indicated in the spanning tree and all online N_Ports and NL_Ports. Broadcast zoning is supported with zones. The default setting is enabled.

In-band management

In-band management is the ability to manage the switches across inter-switch links using QuickTools, SNMP, management server, or the application programming interface (API). The switch comes from the factory with in-band management enabled. If you disable in-band management on a particular the switch, you can no longer communicate with that the switch by means other than a direct Ethernet or serial connection.

Fabric Device Management Interface

Fabric device management interface (FDMI) provides a means to gather and display device information from the fabric, and allows FDMI capable devices to register certain information with the fabric, if FDMI is enabled. QuickTools will report all FDMI information reported by the entry switch, if FDMI is enabled on the entry switch. To view FDMI data, FDMI must be enabled on the entry switch and on all other the switches in the fabric that are to report FDMI data.

FDMI is comprised of the fabric-to-device interface and the application-to-fabric interface. The fabric-to-device interface enables a device's management information to be registered. The application-to-fabric interface provides the framework by which an application obtains device information from the fabric. Use the **FDMI HBA Entry Limit** field on the Switch Properties dialog to configure the maximum number of HBAs that can be registered with a switch. If the number of adapters exceeds the maximum number, the FDMI information for those HBAs cannot be registered.

Use the **FDMI Enabled** option on the Switch Properties dialog to enable or disable FDMI. If FDMI is enabled on an adapter, the adapter forwards information about itself to the switch when the adapter logs into the switch. If FDMI is enabled on a switch, the switch stores the adapter information in its FDMI database. Disabling FDMI on a switch clears the FDMI database. If you disable FDMI on a switch and then re-enable it, you must reset the ports to cause the adapters to log in again, and thus forward adapter information to the switch.

To view detailed FDMI information for a device, click the **Devices** tab, and click the **Information (i)** button in the Details column of the Devices data window. The Detailed Devices Display dialog displays the specific information for that device. Refer to "Devices data window" on page 3-21 for more information.

Advanced switch properties

The Advanced Switch Properties dialog enables you to set the timeout values and change to transparent mode. The Advanced Switch Properties dialog is available only for the entry switch. The switch will be taken offline temporarily and then restored to its original state after the changes are complete.

To open the Advanced Switch Properties dialog (Figure 20), open the Switch menu and select **Advanced Switch Properties**. After making changes, click the **OK** button to put the new values into effect.

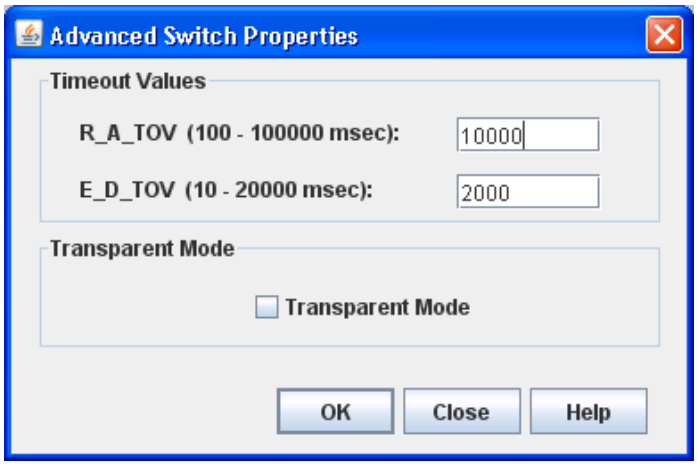

Figure 20. Advanced Switch Properties dialog

Timeout values

The switch timeout values determine the timeout values for all ports on the switch. Table 13 describes the switch timeout parameters. The timeout values must be the same for all switches in the fabric.

Notes:

Mismatched timeout values will disrupt the fabric. These values should not be changed unless absolutely necessary. Therefore, the switch *must* be offline to change these values. Use the Switch Properties dialog to take the switch offline.

Table 13. Timeout values

Parameter	Description
R_A_TOV	Resource Allocation Timeout—represents the maximum time a frame could be delayed in the Fabric and still be delivered. The default is 10000 milliseconds.
E_D_TOV	Error Detect Timeout—represents the maximum round trip time that an operation between two N_Ports could require. The default is 2000 milliseconds.

Transparent mode

The Transparent Mode option enables you to toggle between transparent mode and full-fabric Fibre Channel mode. If the Transparent mode option is selected in the Advanced Switch Properties dialog, the switch converts to a pass-thru module and operates in transparent mode. If the Transparent mode option is not selected, the switch remains in full-fabric mode and can be managed along with other switches in the fabric.

Managing system services

The System Services dialog (Figure 21) provides a central location to enable or disable the system services such as embedded web applet, command line interface, Network Time Protocol (NTP), and Common Information Model (CIM). To display the System Services dialog, open the Switch menu and select **Services**.

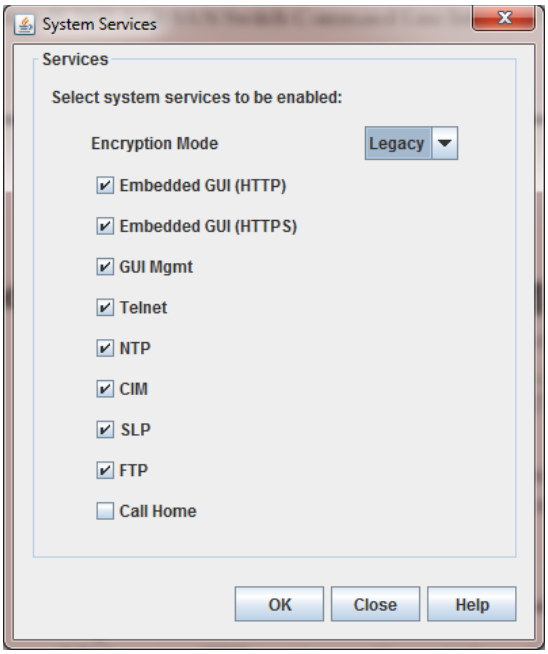

Figure 21. System Services dialog

Important:

Use caution when disabling the Embedded GUI, GUI Mgmt, and Telnet services—it is possible to disable all access to the switch except through a serial connection.

The following sections describe the system services.

Encryption Mode

This service applies Legacy (default) or Strict security affecting encryption algorithms, key lengths, and Diffie-Hellman groups. Legacy mode uses encryption algorithms with a strength of 80 bits or greater, and keys with a length of 1,024 or greater, thus excluding the following:

- IP security association encryption: des-cbc
- 512-bit public/private keys

Strict mode uses encryption algorithms with a strength of 112 bits or greater, and keys with a length of 2,048 or greater, thus excluding the following:

- IP security association authentication: hmac-md5, aes-xcbc-mac encryption
- IP security association encryption: des-cbc, blowfish-cbc, twofish-cbc encryption
- IKE peer/policy integrity: md5_96, aes_xcbc_96 encryption
- Diffie-Hellman groups: 1, 2, 5
- 1,024-bit public/private keys

Before you can use QuickTools in Strict mode, you must enable Transport Layer Security (TLS) 1.2 in the Internet browser and in Java 2 Runtime Environment 8. For more information, see “Configuring the Browser and Java for Strong Encryption” on page 2-7.

At startup, the switch assesses IP security associations, IKE peers, IKE policies, certificates, and keys against the Encryption Mode service. Under Strict mode, if these elements use excluded encryption algorithms, key lengths, or Diffie-Hellman groups, the switch applies the configurations unchanged, but generates an alarm indicating the conflict. To resolve the alarm, you must reconfigure the association, peer, policy, certificate, or key to comply with Strict mode limits.

After changing to Encryption Mode=Strict, external clients may not be able to connect to the switch if they do not support the same encryption algorithms. Upgrade the following applications as needed:

- openssl
- SSH clients
- SNMPv3 clients
- SMI-S/CIM clients
- LDAP/RADIUS servers
- Web browsers/HTTPs clients
- sFTP, HTTPs servers

Embedded GUI (HTTP)

This service allows users to point a browser at the switch and use QuickTools over a nonsecure connection. The default is disabled.

Embedded GUI (HTTPS)

This service allows users to point a browser at the switch and use QuickTools over a secure connection. The default is enabled.

GUI Mgmt

This service allows out-of-band management of the switch from a management application (GUI). If disabled, the switch cannot be specified as the entry switch for a fabric in the GUI, but can still be managed through an in-band connection.

Telnet (command line interface)

This service allows users to manage the switch through a Telnet command line interface session. Disabling Telnet access to the switch is not recommended. The default is not selected.

NTP (Network Time Protocol)

This service allows the switch to obtain its time and date settings from an NTP server. Configuring all of your switches and your workstations to use NTP will synchronize date and time settings and prevent difficulties with SSL certificates and event logs.

CIM (Common Information Model)

This service allows management of the switch through third-party applications that use CIM.

SLP (Service Location Protocol)

This service allows users to enable and disable SLP.

FTP (File Transfer Protocol)

This service allows file transfers to the switch using FTP. FTP is required for out-of-band firmware uploads that will complete faster than in-band firmware uploads. The default is not selected.

Call Home

This service allows users to configure switches to send alerts and events to pagers and e-mail. You can configure the type of events and where the alerts are sent.

Configuring the network

Network configuration includes the following elements:

- Network IP configuration
- IPv4 and IPv6 addressing
- Network Domain Name Service (DNS) configuration

Network properties

Use the Network Properties dialogs (Figure 22) to configure IP and DNS parameters. The Network Properties dialog has two tabs: IP and DNS. Click the **IP** tab to view the Network Properties IP dialog. Click the **DNS** tab to view the Network Properties DNS dialog. After making changes, click **OK** to put the new values into effect.

To view the Network Properties dialog, choose one of the following:

- On the faceplate display for the switch you will configure. On the **Switch** menu, click **Network Properties**.
- Right-click a switch graphic on the faceplate display, and select **Network Properties** on the shortcut menu.

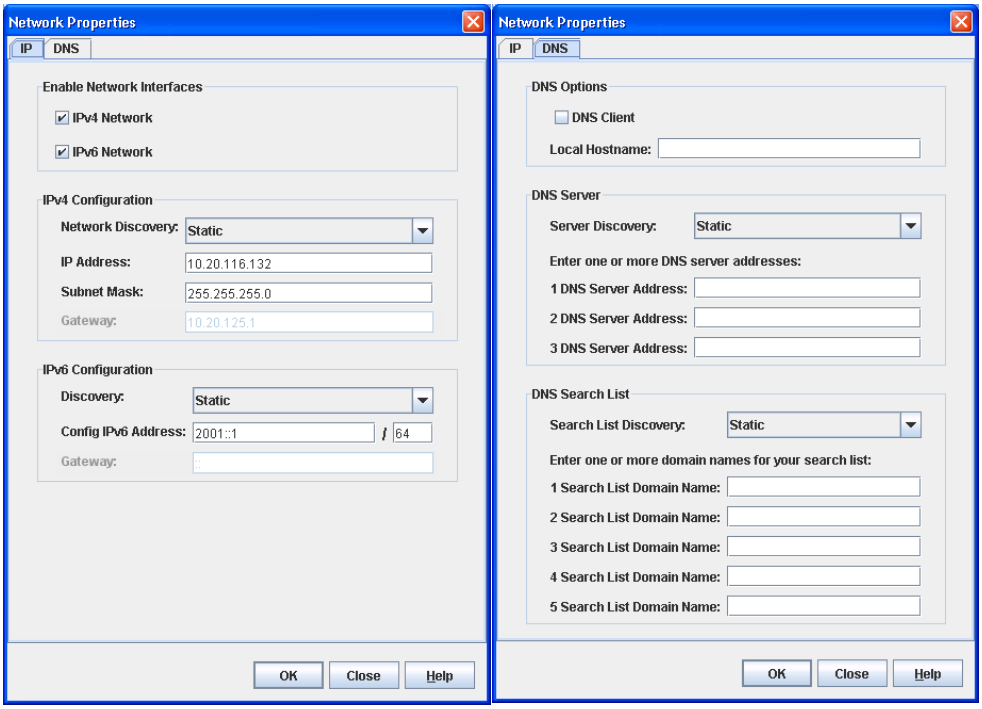

Figure 22. Network Properties dialogs

The IP configuration identifies the switch on the Ethernet network, determines which network discovery method to use, and enables/disables the IPv4 and IPv6 network addressing.

IPv4 and IPv6 addressing

The 9.1 firmware supports the IPv4 and IPv6 address families. An IPv4 address is 32 bits, and consists of four blocks of decimal numbers, with each block separated by a period. Each block can have up to three numbers. The single zero character displayed in a block represents all zeros for that block. An example of an IPv4 address is 255.255.255.0. All four blocks contain numbers. Table 14 describes the IPv4 and IPv6 configuration parameters.

An IPv6 address allows for a much wider range of IP addresses assigned to a host than an IPv4 address. An IPv6 address is 128 bits, and consists of eight blocks of hexadecimal numbers, with each block separated by a colon. The maximum number of numerals in each block is four. One or more blocks with all zeroes are represented by two colon characters. The total number of blocks always adds up to eight. To determine how many contiguous blocks contain only zeroes, subtract the number of populated blocks from eight. For example, the IPv6 address 2eee:49:24:7a:54:3434 is equivalent to 2eee:0000:0000:49:24:7a:54:3434. The number of blocks containing zeroes in this example is two (8-6=2).

Notes:

Switches without IPv6 addressing enabled cannot communicate with hosts or switches using the IPv6 addressing.

Table 14. Network Properties—IP configuration

Parameter	Description
iPv4 Network	Enable this option to permit the IPv4 addressing format to be used anytime you are required to enter an IP address.  **CAUTION:** Disabling this option will prevent you from using an IPv4 IP address for system services.
iPv6 Network	Enable this option to permit IPv6 addressing format to be used anytime you are required to enter an IP address.  **CAUTION:** Disabling this option will prevent you from using an IPv6 IP address for system services.

Table 14. Network Properties—IP configuration (Continued)

Parameter	Description
Network Discovery	Choose one of the following methods by which to assign the IP address: • Static—uses the IP configuration parameters entered on the Network Properties dialog. • BootP—acquires the IP configuration from a BootP server. If no IP address is obtained, the switch reverts to the previously configured IP address. • RARP (Reverse Address Resolution Protocol)—acquires the IP address from a RARP server. A RARP request is broadcast with up to three retries, each at 5 second intervals. If no IP address is obtained, the switch reverts to the previously configured IP address. • DHCP (Dynamic Host Configuration Protocol)—acquires the IP configuration from a DHCP server. If no satisfactory lease is obtained, the DHCP client attempts to use the previously configured lease. If the previous lease cannot be used, no IP address will be assigned to this switch to avoid an IP address conflict.
IP Address	Internet Protocol (IP) address for the Ethernet port. The default value is 10.0.0.1.
Subnet Mask	Subnet mask address for the Ethernet port. The default value is 255.0.0.0.
Gateway	IPv4 gateway address; cannot be edited
Discovery	Choose one of the following methods by which to assign the IP address: • Static—uses the IP configuration parameters entered on the Network Properties dialog • Dhcpv6 (Dynamic Host Configuration Protocol version 6)—acquires the IP configuration from a DHCP server. If no satisfactory lease is obtained, the DHCP client attempts to use the previously configured lease. If the previous lease cannot be used, no IP address will be assigned to this switch to avoid an IP address conflict. • NDP (Neighbor Discovery Protocol)—part of the Stateless Address Auto configuration protocol. It replaces the Address Resolution Protocol used with IPv4.
Config IPv6 Address	IPv6 address for the Ethernet port
Gateway	IPv6 gateway address; cannot be edited

Network DNS configuration

The Network Properties dialog has two tabs: IP and DNS. Click the **DNS** tab to view the Network Properties DNS dialog (Figure 22). Use the Network Properties DNS dialog to enable the DNS Client on the switch and the DNS server to map domain names to IP addresses. Table 15 describes the DNS configuration parameters.

Table 15. Network Properties—DNS configuration

Parameter	Description
DNS Client	Domain Name Service client
Local Hostname	The name of local host
Server Discovery	Choose one of the following methods by which to assign the IP address: • Static—uses the IP configuration parameters entered on the Network Properties dialog. • DHCP (Dynamic Host Configuration Protocol)—acquires the IP configuration from a DHCP server. If no satisfactory lease is obtained, the DHCP client attempts to use the previously configured lease. If the previous lease cannot be used, no IP address will be assigned to this switch to avoid an IP address conflict. • Dhcpv6 (Dynamic Host Configuration Protocol version 6)—acquires the IP configuration from a DHCP server. If no satisfactory lease is obtained, the DHCP client attempts to use the previously configured lease. If the previous lease cannot be used, no IP address will be assigned to this switch to avoid an IP address conflict.
DNS Server Addresses	The IP address of the DNS server
Search List Discovery	Choose one of the following methods by which to assign the IP address: • Static—uses the IP configuration parameters entered on the Network Properties dialog. • DHCP (Dynamic Host Configuration Protocol)—acquires the IP configuration from a DHCP server. If no satisfactory lease is obtained, the DHCP client attempts to use the previously configured lease. If the previous lease cannot be used, no IP address will be assigned to this switch to avoid an IP address conflict. • Dhcpv6 (Dynamic Host Configuration Protocol version 6)—acquires the IP configuration from a DHCP server. If no satisfactory lease is obtained, the DHCP client attempts to use the previously configured lease. If the previous lease cannot be used, no IP address will be assigned to this switch to avoid an IP address conflict.
Search List Domain Names	The suffix that is appended to the user-specified hostname for the search.

Configuring SNMP

Configuring the Simple Network Management Protocol includes:

- SNMP properties configuration
- SNMP trap configuration
- SNMP v3 security

SNMP properties configuration

Use the SNMP Properties dialog shown in Figure 23 to change SNMP configuration parameters. After making changes, click the **OK** button to put the new values into effect. To open the SNMP Properties dialog, choose one of the following:

- Open the faceplate display for the switch you will configure. Open the Switch menu, select **SNMP**, and select **SNMP Properties**.
- Right-click a switch graphic in the faceplate display, and select **SNMP Properties** from the popup menu.

Notes:

Since Read Community, Trap Community, and Write Community settings are like passwords and are write-only fields, the current settings are displayed as asterisks.

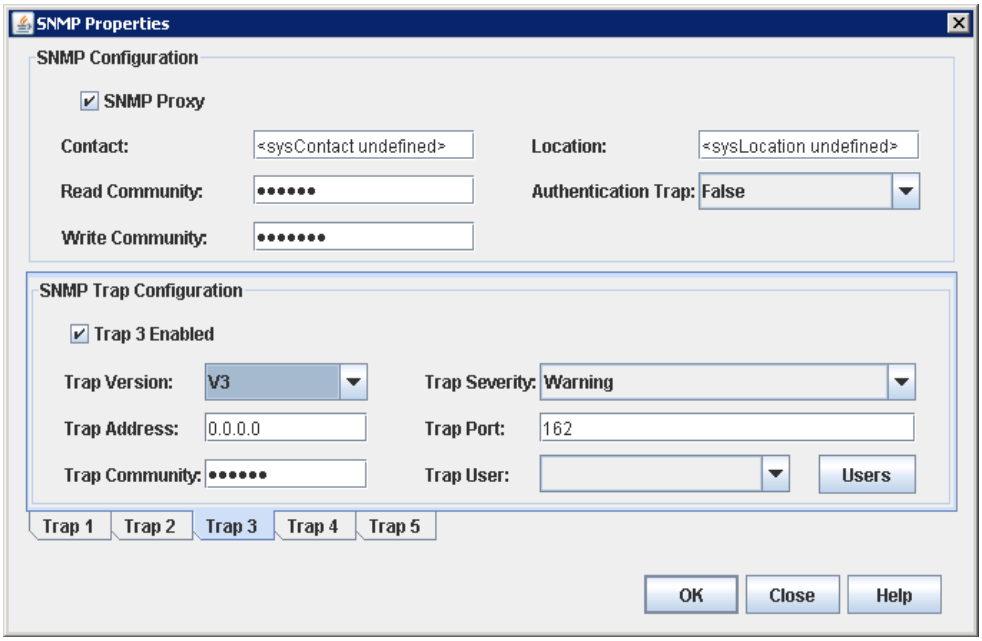

Figure 23. SNMP Properties dialog

The SNMP configuration defines how authentication traps are managed. Table 16 describes the SNMP configuration parameters. The illegal characters for the user-defined fields are the pound sign (#), semi-colon (;), and comma (,).

Table 16. SNMP configuration parameters

Parameter	Description
Contact	Specifies the name (up to 64 characters) of the person who is to be contacted to respond to trap events. The default is “undefined”.
Read Community	Read community password (up to 32 characters) that authorizes an SNMP agent to read information from the switch. This field is write only. The value on the switch and the SNMP management server must be the same. The default is “public”.
SNMP Proxy	If enabled, you can use SNMP to monitor and configure any switch in the fabric.
Location	Specifies the name (up to 64 characters) for the switch location. The default is “undefined”.
Authentication Trap	Enables or disables the reporting of SNMP authentication failures. If enabled, a notification trap is sent when incorrect community string values are used. The default value is "False".
Write Community	Write community password (up to 32 characters) that authorizes an SNMP client to write information to the switch. This field is write only. The value on the switch and the SNMP management server must be the same. The default is “private”.

SNMP trap configuration

The SNMP trap configuration defines how traps are set. Choose from the tabs **Trap1–Trap 5** to configure each trap. Table 17 describes the SNMP configuration parameters.

Table 17. SNMP trap configuration parameters

Parameter	Description
Trap Version	Specifies the SNMP version (1, 2, or 3) with which to format traps.
Trap 1 Enabled	Enables or disables the trap. If disabled, traps are not sent to trap monitoring stations and the trap settings are not configurable.
Trap Address[a]	Specifies the IP address to which SNMP traps are sent. A maximum of 5 trap addresses are supported. The default address for trap 1 is 10.0.0.254. The default address for traps 2–5 is 0.0.0.0.
Trap Community	Trap community password (up to 32 characters) that authorizes an SNMP agent to receive traps. This field is write only. The value on the switch and the SNMP management server must be the same. The default is “public”.
Trap Port[1]	The port number on which the trap is sent. The default is 162.
Trap Severity	Specifies a severity level to assign to the trap. Open the drop-down list and choose a level. The **Trap 1 Enabled** option on the SNMP Properties dialog must be enabled to access this drop-down list. Trap severity levels include Unknown, Emergency, Alert, Critical, Error, Warning, Notify, Info, Debug, and Mark.
Trap User	The Trap User field becomes active when the **V3** option is selected. Click the **Users** button to modify the contents of the Trap User drop-down list.
Users	The **Users** button becomes active when the **V3** option selected in the Trap Version drop-down list. Click the **Users** button to open the SNMPv3 dialog from which to add/remove users from the list. Changes made to the user list will be updated in the user drop-down in the SNMP Properties dialog.

[a] Trap address (other than 0.0.0.0) and trap port combinations must be unique. For example, if trap 1 and trap 2 have the same address, then they must have different port values. Similarly, if trap 1 and 2 have the same port value, they must have different addresses.

SNMP v3 security

Simple Network Management Protocol Version 3 (SNMPv3) is an interoperable standards-based protocol for network management. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network. SNMP v3 security is an additional layer of security offered with the 9.1 firmware. The SNMP v3 security is available to a switch that has a secure connection, and can be configured only on the entry switch. The security features provided in SNMPv3 are:

- Message integrity—ensuring that a packet has not been tampered with during transit.
- Authentication—determining the message is from a valid source.
- Encryption—scrambling the contents of a packet to prevent it from being seen by an unauthorized source.

The SNMP v3 Manager dialog allows you to add, remove, and edit an SNMP v3 user. To display the SNMP v3 Manager dialog shown in Figure 24, open the Switch menu, select **SNMP**, and select **SNMP v3 Manager**.

Click the **Add** button to open the SNMP v3 User Editor dialog shown in Figure 25, and add an SNMP v3 user. After SNMP v3 users are configured and saved, they are displayed in the SNMPv3 Users list window in the SNMP v3 Manager dialog. Select a user from the list, and that user's settings are displayed on the right in the Selected SNMPv3 User area. The **Remove** and **Edit** buttons become active when you select a user from the SNMP v3 Users list. Click the **Remove** button to delete the selected user. Click the **Edit** button to open the SNMP v3 User Editor Edit User dialog in which to change the selected user's configuration.

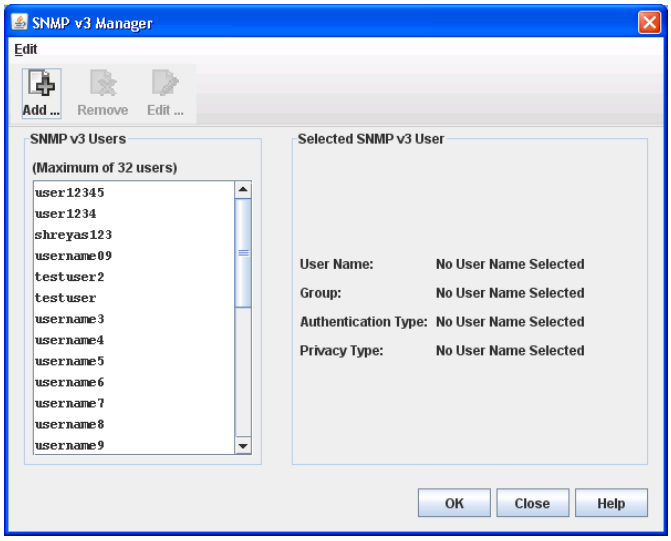

Figure 24. SNMP v3 Manager dialog

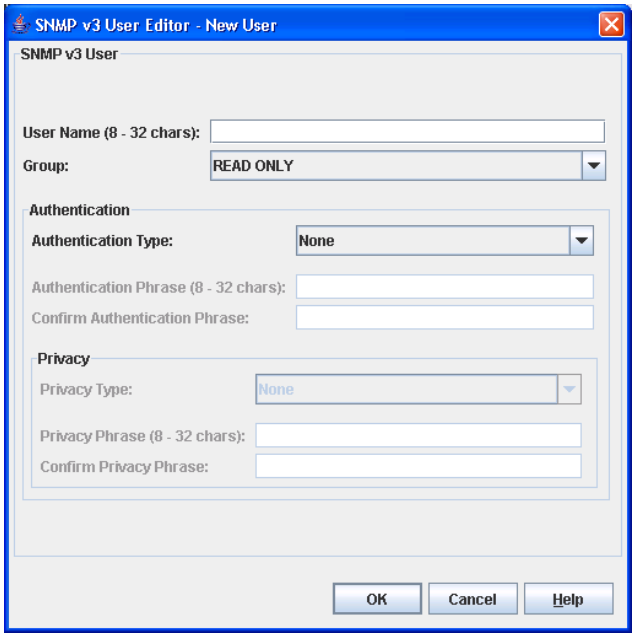

Figure 25. SNMP v3 User Editor dialog

Table 18 describes the SNMP v3 User Editor dialog parameters. After configuring the user, click the **OK** button to save the settings and close the dialog.

Table 18. SNMP v3 User Editor dialog

Parameter	Description
User Name	Name for this SNMP v3 user.
Group	Read Only. This parameter permits the user to view only SNMP v3 user settings. Read Write permits user to view and change SNMP v3 user settings.
Authentication Type	None, MD5, SHA. MD5 and SHA require an authentication phrase. If None, no authentication phrase is required. MD5 is available only when the Encryption Mode = Legacy. For more information about Encryption Mode, see "Managing system services" on page 4-62.
Authentication Phrase	A unique string or phrase to serve as an password-like authentication phrase.
Confirm Authentication Phrase	Re-enter the same unique string or phrase to serve as a password-like authentication phrase.
Privacy Type	None, DES, AES. If None, no privacy phrase is required. DES is available only when the Encryption Mode = Legacy. For more information about Encryption Mode, see "Managing system services" on page 4-62.
Privacy Phrase	A unique string or phrase to serve as a password-like privacy phrase.
Confirm Privacy Phrase	Re-enter the unique string or phrase to serve as a password-like privacy phrase.

SNMPv3 users for which Authentication Type=MD5 or Privacy Type=DES are invalid when Encryption Mode = Strict. Before setting Encryption Mode = Strict, delete the noncompliant user accounts and create new user accounts as needed.

Archiving a switch

You can create an .XML archive file containing the configuration parameters. Basically, any data received by QuickTools is archived. This archive file can be used to restore the configuration on the same switch or on a replacement switch. You can also use the archive file as a template for configuring new switches to add to a fabric. Passwords are not archived. Security Group secrets are not included in the archive and must be re-configured using the CLI after a restore operation.

Archived parameters include the following:

- Switch properties and statistics
- IP configuration
- SNMP configuration
- Port properties and statistics
- Alarm configuration
- Zoning configuration
- Nicknames configuration
- User account information (but not restored)
- Configured device security (only with SSL connection to the switch)
- RADIUS Server information (only with SSL connection to the switch)

To archive a switch, do the following:

1. Open the Switch menu and select **Archive**.
2. In the Save dialog, enter a file name.
3. Click the **Save** button.

Restoring a switch

Restoring a switch loads the archived configuration parameters to the switch. The switch configuration must be archived before it can be restored. The archive must be compatible with the switch to be restored. That is, you can only restore an Lenovo Flex System FC3171 8 Gb SAN Switch with an archive from an Lenovo Flex System FC3171 8 Gb SAN Switch. For more information, see "Archiving a switch" on page 4-74.

CAUTION:

The switch being restored should be physically disconnected from the fabric. Restoring a switch in a fabric can severely disrupt the fabric. After the restore process is complete, the switch can be reconnected to the fabric.

To restore a switch, do the following:

1. Log in to the fabric through the switch you want to restore. You cannot restore a switch over an ISL.
2. Open the Switch menu and select **Restore** to display the Restore dialog shown in Figure 26. The Restore dialog offers a **Full Restore** and a **Selective Restore** tab.

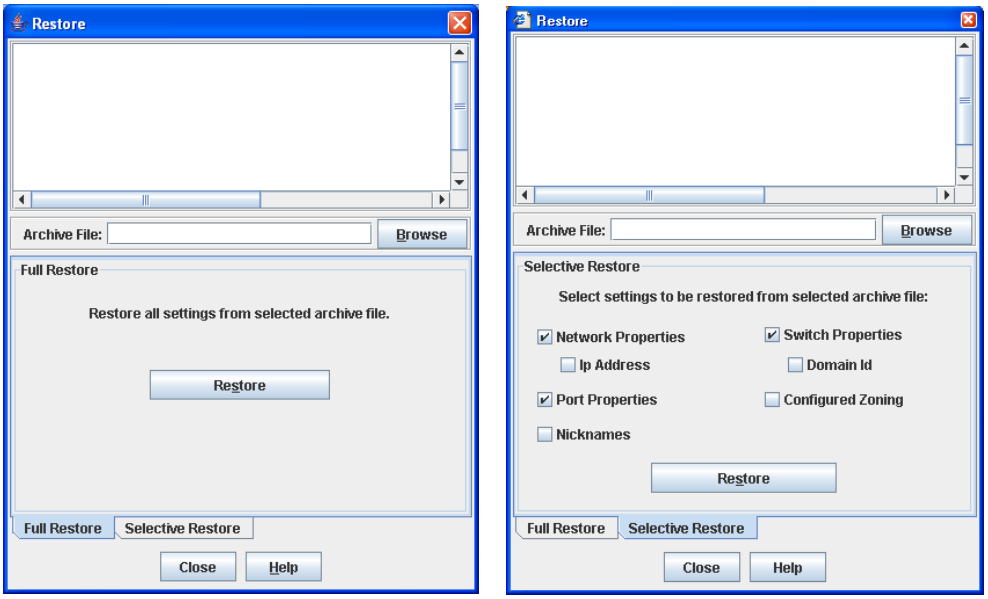

Figure 26. Restore Dialogs–full and selective

3. Enter the archive file name or browse for the file. This archive file must be one that was produced by the QuickTools archive function. Configuration backup files created with the Config Backup command are not compatible with the QuickTools restore function. The Config Backup command does not archive the primary or secondary secrets for any security groups.
4. To restore all configuration settings, click the **Full Restore** tab, and then click the **Restore** button. To restore selected configuration settings, click the **Selective Restore** tab and select one or more of the following options, and then click the **Restore** button:
   - **Network Properties**—restores all settings presented in the Network properties dialog except the IP address. See "Network properties" on page 4-65.
   - **IP Address**—restores switch IP address in addition to the other network properties.
   - **Port Properties**—restores all settings presented in the Port properties dialog. See "Port symbolic name" on page 5-100.
   - **Nicknames**—restores the last saved nickname configuration.
   - **Switch Properties**—restores all settings presented in the Switch Properties dialog except the domain ID. See "Setting switch properties" on page 4-57.
   - **Domain ID**—restores switch domain ID in addition to the other switch properties.
   - **Configured Zoning**—restores all configured zone sets, zones, and aliases in the switch's zoning database excluding the active zone set.

- **Auth Server Info**—restores all Authentication Server information
- **Call Home**—restores all Call Home configuration and profiles settings

5. If you select the **Configured Zoning** or **Full Restore** option and the file contains zone sets, a dialog prompts you to activate one of those zone sets. Click the **Yes** button, and select a zone set from the drop-down list in the Select Zone Set to be Activated dialog.
6. Click the **OK** button and view the results in the top pane of the Restore dialog.

Restoring the factory default configuration

You can restore the switch and port configuration settings to the factory default values. To restore the factory configuration on a switch, open the Switch menu and select **Restore Factory Defaults**. Table 19 lists the factory default switch configuration settings.

Restoring the switch to the factory default configuration does not restore the account name and password settings. To restore user accounts, you must select the **Reset User Accounts to Default** option in the maintenance menu. See "Recovering a Switch" in the Installation Guide for your switch for information about maintenance mode and the maintenance menu.

Table 19. Factory default configuration settings

Setting	Value
Symbolic Name	IBM8Gb
Administrative State	Online
Domain ID	1
Domain ID Lock	False
In-band Management	True
Broadcast Support	Enable
Resource Allocation Timeout (R_A_TOV)	10000 milliseconds
Interop Mode	True
I/O Stream Guard	Disabled
Device Scan Enabled	True
Error Detect Timeout (E_D_TOV)	2000 milliseconds
SNMP Enabled	True
SNMP Proxy	True
IP Address	10.0.0.1
FDMI Enabled	True
FDMI HBA Entry Level	1000
Subnet Mask Address	255.0.0.0
Gateway Address	10.0.0.254
Network Discovery	Static

Table 19. Factory default configuration settings (Continued)

Setting	Value
Remote Logging	False
Remote Logging Host Ip Address	10.0.0.254
NTP Client Enabled	False
NTP Server IP Address	10.0.0.254
Contact	Undefined
Location	Undefined
Trap Enabled	False
Trap Port	162
Trap Address	Trap 1: 10.0.0.254; Traps 2-5: 0.0.0.0
Trap Community	Public
Read Community	Public
Write Community	Private
Port State	Online
Port Speed	Auto-detect
Port Type	GL

Downloading a support file

The Download Support File menu option assembles all log files and switch memory data into a core dump file (dump_support.tgz). This file can be sent to technical support personnel for troubleshooting switch problems. The menu option is not accessible (displayed) for switches that do not support the download support file function.

To create a support file, do the following:

1. Open the Switch menu, and select **Download Support File**.
2. In the Download Support File dialog, click the **Browse** button and define a location for the support file; or type the path in the text field.
3. Select an sFTP client support option in the Status window that confirms trust during downloading or uploading files.
4. Click the **Start** button to begin the process of creating and downloading the support file to your workstation. Observe the status in the Status area.
5. After the support file is saved to your workstation, click the **Close** button to close the Download Support File dialog.

Installing feature license keys

A feature license key is a password that you can purchase from your distributor or authorized reseller to upgrade your switch. Currently, there are no feature upgrades available for the Lenovo Flex System FC3171 8 Gb SAN Switch.

Installing firmware

Installing firmware involves loading, unpacking, and activating the firmware image on the switch. QuickTools does this in one operation. To provide consistent performance throughout the fabric, ensure that all switches are running the same version of firmware.

During a hot reset operation, fabric services will be unavailable for a short period (30-75 seconds). To ensure that an NDCLA operation is successful, verify that all administrative changes to the fabric (if any) are complete.

CAUTION:

Changes to the fabric may disrupt the NDCLA process.

Common administrative operations that change the fabric include:

- Zoning modifications
- Adding, moving or removing devices attached to the switch. This operation includes powering up or powering down attached devices.
- Adding, moving or removing ISLs or other connections.

After an NDCLA operation is complete, management connections must be re-initiated:

- QuickTools sessions will re-connect automatically
- Telnet sessions must be restarted manually.

The applicable code versions are:

- Future firmware releases will install nondisruptively unless specifically indicated in the release notes.
- An NDCLA operation to previous switch firmware versions is not supported.

The Load Firmware dialog (Figure 27) allows you to select and install a firmware image file. To open the Load Firmware dialog for an individual switch, open the Switch menu and select **Load Firmware**. When the Load Firmware dialog is opened, the path displayed in the Firmware Image Folder field is automatically searched for firmware image files that can be installed. The default path to search for firmware image files is the user's working directory. To change the path, click the **Browse** button and select a new path. Click the **Rescan** button to search the folder displayed in the Firmware Image Folder field. The firmware image files found are listed in and can be selected from the Version drop-down list.

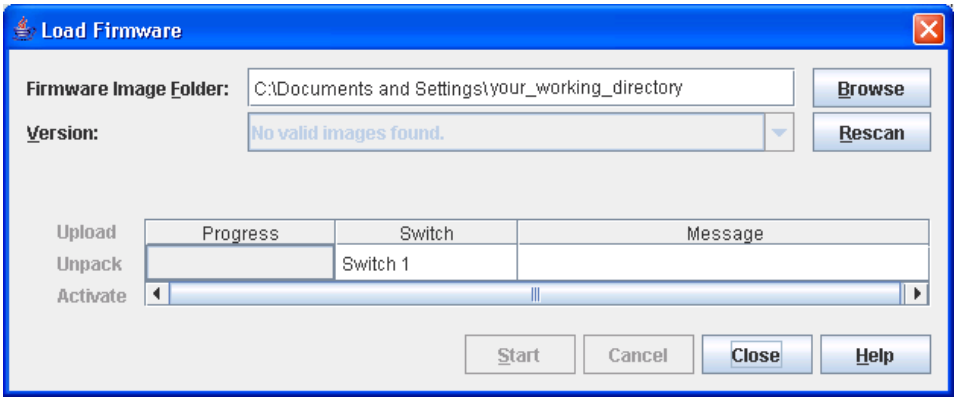

Figure 27. Load Firmware dialog

Notes:

Some NDCLA restrictions may apply when upgrading some versions of firmware. Please contact the appropriate technical support for specific details *before* upgrading firmware. Also, review the firmware documentation and release notes to understand any restrictions, limitations, or special notices related to the firmware release.

To install firmware, do the following:

1. In the faceplate display, open the Switch menu and select **Load Firmware**.
2. In the Load Firmware dialog, click the **Browse** button next to the Firmware Image Folder field to browse for and select the folder containing firmware file to be loaded.
3. Select the firmware file from the Firmware Image Folder.
4. Click the **Start** button to begin the firmware load process. You will be shown a message indicating the type of reset required to activate the firmware.
5. Click the **OK** button to continue firmware installation.
6. Click the **Close** button to close the Load Firmware dialog.

Configuring server authentication

The server authentication feature allows you to configure the device and user authentication order parameters by type of server (RADIUS or LDAP).

Authentication information

The Auth Information dialog box (Figure 28) allows you to choose add, edit, or remove a Radius server or an LDAP server. To view the Auth Information dialog (Table 28), on the **Switch** menu, click **Auth Servers**.

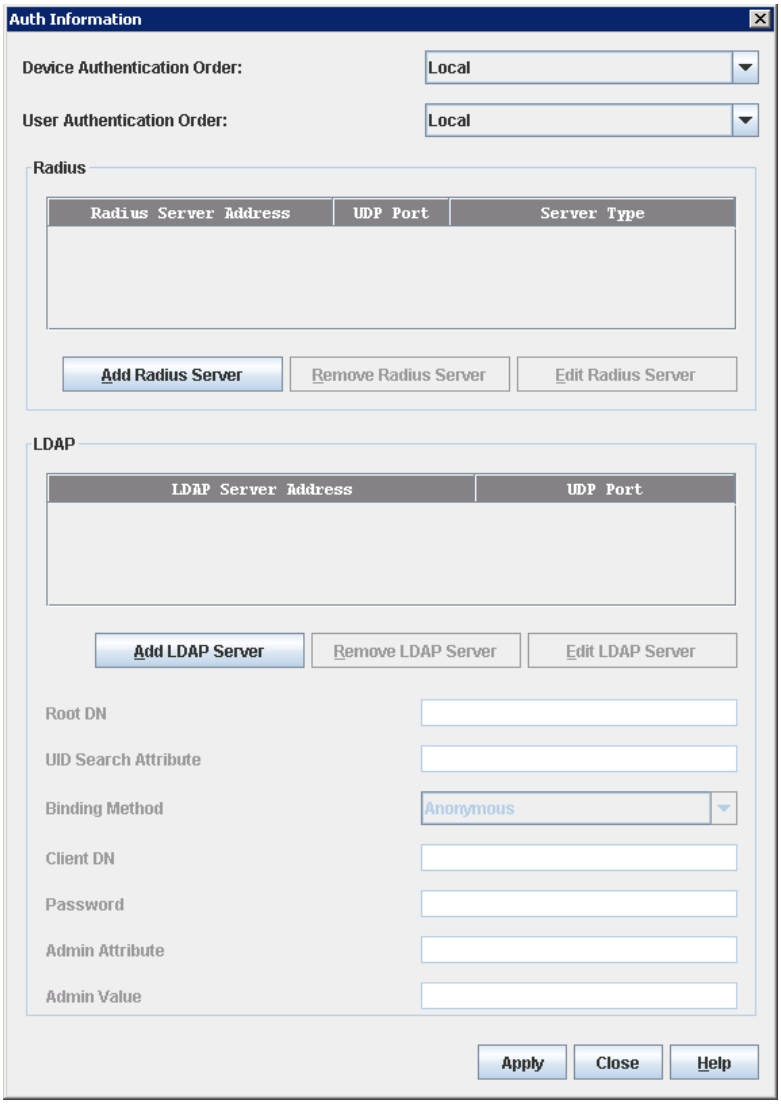

Figure 28. Auth Information dialog

Table 20 lists the fields in the Auth Information dialog.

Table 20. Auth Information dialog fields

Setting	Value
Device Authentication Order	Device Authentication order used
User Authentication Order	User Authentication order used
Radius	Remote Authentication Dial-In User Service
Add Radius Server	Add a new Radius Server
Remove Radius Server	Remove an existing Radius Server
Edit Radius Server	Edit an existing Radius Server
LDAP	Lightweight Director Access Protocol
Add LDAP Server	Define a new Lightweight Director Access Protocol
Remove LDAP Server	Remove a Lightweight Director Access Protocol
Edit LDAP Server	Edit a Lightweight Director Access Protocol
Root DN	Root domain name
UID Search Attribute	Search attribute used UID
Binding Method	Type of binding used
Client DN	Client domain name
Password	Password required to configure authentication information
Admin Attribute	Admin attribute
Admin Value	Admin value

RADIUS server information

The Radius Server Information dialog (Figure 29) allows you to view or edit radius server information. To view the RADIUS Server Information dialog box (Table 29), on the **Auth Information** dialog box in the Radius area, click **Add Radius Server**.

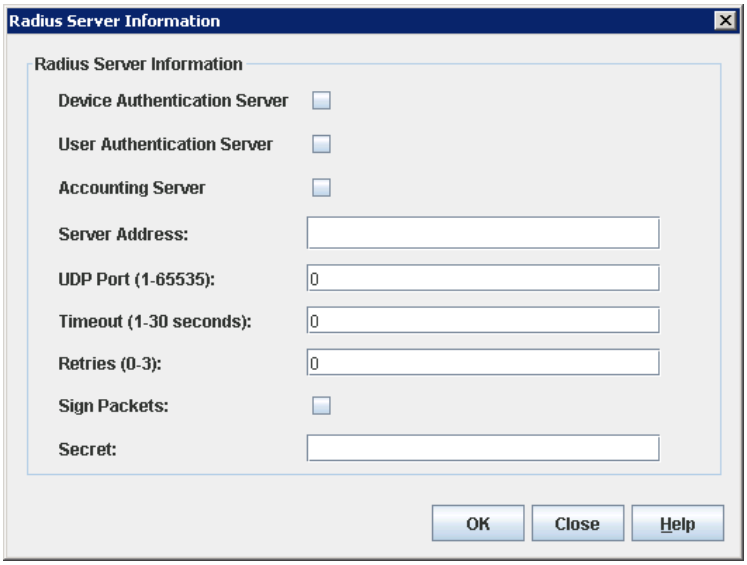

Figure 29. Radius Server Information dialog

Table 21 lists the fields in the Radius Server Information dialog.

Table 21. RADIUS Server Information dialog fields

Field	Description
Device Authentication Server	Option to activate device authentication
User Authentication Server	Option to activate user authentication
Accounting Server	Option to activate server authentication
Server Address	Radius server address
UDP Port	UDP port number
Timeout	Amount of time (1-30 seconds) to continue attempting to authenticate after first authentication attempt fails
Retries	Number of times (0-3) to continue attempting to authenticate after first authentication attempt fails
Sign Packets	Option to use sign packets
Secret	Authentication secret

LDAP server information

The LDAP Server dialog (Figure 30) allows you to add or edit an LDAP server. To view the LDAP Server dialog, on the **Auth Information** dialog box in the LDAP area, click **Add LDAP Server**.

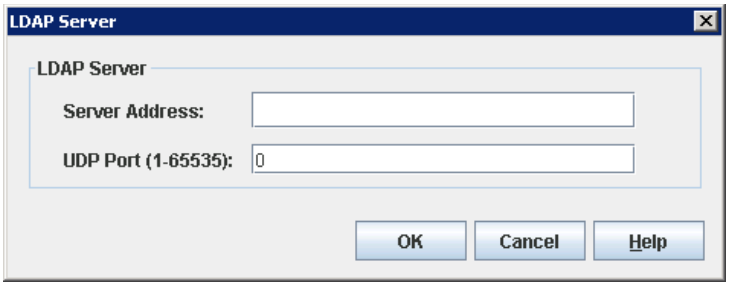

Figure 30. LDAP Server dialog

Table 22 lists the fields in the LDAP Server dialog box.

Table 22. LDAP Server dialog fields

Field	Description
Server Address	LDAP Server address
UDP Port	UDP port number

Notes:

The Lenovo Flex System FC3171 8 Gb SAN Switch uses secure LDAP (LDAP over SSL–LDAPS) to connect to the configured LDAP servers, regardless of the LDAP server's port number. The LDAP servers must be properly configured to support LDAPS connections to perform LDAP authentication.

Using server authentication

The server authentication feature allows you to configure the device and user authentication order parameters for the type of server used: RADIUS or LDAP.

Adding an authentication server

To add an authentication server:

1. On the **Switch** menu, click **Auth Servers** to view the Auth Information dialog.
2. Choose one of the following for the type of server used for authentication:
   - If using a RADIUS server type, click **Add Radius Server** to view the RADIUS Server Information dialog. To add a RADIUS server, select the device, user, and accounting server options. Type the server address, the UDP Port number, timeout value, number of retries upon authentication failure, select a sign packets option, and type the secret, and then click **OK**.
   - If using an LDAP server type, click **Add LDAP Server** to view the LDAP Server dialog. To add an LDAP server, type the server address and the UDP Port number for the server, and then click **OK**.
3. Click **Apply** to save the new server configuration, and close the Auth Information dialog.

Editing an authentication server

To edit an authentication server:

1. On the **Switch** menu, click **Auth Servers** to view the Auth Information dialog.
2. Click the server to edit In either the Radius window or LDAP window.
3. Click **Edit Radius Server** or **Edit LDAP Server** to view the RADIUS Server Information or LDAP Server dialog.
4. Make the changes and click **OK**.
5. Click **Apply** to save the changes without closing the Auth Information dialog; or click **Close** to save the changes and close the Auth Information dialog.

Removing an authentication server

To remove an authentication server:

1. On the **Switch** menu, click **Auth Servers** to view the Auth Information dialog.
2. Click the server to be removed in either the Radius window or LDAP window.
3. Click **Remove Radius Server** or **Remove LDAP Server**.
4. Click **Apply** to save the changes without closing the Auth Information dialog; or click **Close** to save the changes and close the Auth Information dialog.

Using Call Home

The Call Home feature allows you to configure switches to send alerts regarding events and faults to Email addresses. Examples of Email destinations are pagers, cell phones, NOC (Network Operations Center) operators/applications, and support organizations. You can configure the type of events and where the alerts are sent. Use the Call Home Setup dialog (Figure 31) to configure call home parameters. To display the Call Home Setup dialog, open the Switch menu, select **Call Home**, and select **Setup**.

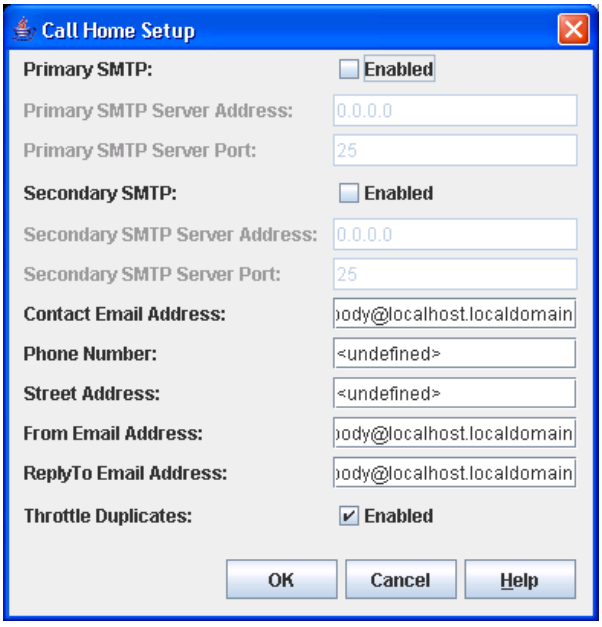

Figure 31. Call Home Setup dialog

Table 23 lists the fields in the Call Home Setup dialog.

Table 23. Call Home Setup dialog fields

Setting	Value
Primary SMTP: (active)	The "(active)" indicates the Primary SMTP (Simple Mail Transfer Protocol) is the SMTP server that CallHome will use when transmitting Email messages. CallHome operates as an SMTP client, or more correctly, an SMTP sending agent. After any system configuration, the Primary SMTP server will always become the active SMTP, provided it is enabled and has a non-default address defined (0.0.0.0 is the default).
Primary SMTP Server Address:	This setting is the IP address of the primary (first) SMTP server.
Primary SMTP Server Port:	This setting is the service port number that the primary SMTP server is listening on to accept connections from SMTP sending agents.
Secondary SMTP:	The Secondary SMTP is the second SMTP server. If the primary SMTP is not enabled/defined, or if there was a failure in communicating with the primary SMTP server, the Secondary SMTP server will become the (active) SMTP server—the one used by Call Home for the next attempt to transmit Email.
Secondary SMTP Server Address:	The IP address of the secondary (second) SMTP server.
Secondary SMTP Server Port:	The service port number that the secondary SMTP server is listening on to accept connection from SMTP sending agents.
Contact Email Address:	The Email address of the point-of-contact for the switch. This Email address will be included in the text of Email messages using the FullText format under the section for Contact Information.
Phone Number:	The phone number of the point-of-contact for the switch. This value will be included in the text of Email messages using the FullText format under the section for Contact Information.
Street Address:	The address of the point-of-contact for the switch. This value will be included in the text of Email messages using the FullText format under the section for Contact Information.

Table 23. Call Home Setup dialog fields (Continued)

Setting	Value
From Email Address:	The Email address that will be provided to the SMTP server to indicate the sender of the Email being transmitted. In Emails sent by Call Home, this address will appear in the message heading as the "From: " address. This value is required to send Emails. If there are any problems encountered in routing the Email to any of the intended recipients, the notice of the problem will be sent to this address. It is an important address for receiving Email notices concerning problems. This address is also the default address used when replies are sent to an Email by a recipient. If the "Reply-To: " Email address is supplied it will override the sending of replies to the "From: " Email address by recipients. However, any notifications of Email problems sent by any SMTP server used to route the message to the final recipient will always send those notifications to the "From: " address.
ReplyTo Email Address:	The Email address used by mail reading programs to determine the address that an Email should be addressed to for a reply to a received message. This value will override the use of the "From: " address as the recipient for a reply message.
Throttle Duplicates:	This boolean setting indicates if duplicate messages should be suppressed and accumulated. If "True", then after an Email has been transmitted, Call Home will not transmit Email for switch events that would result in duplicate Emails during a specified time window (default is 15 seconds). The time window can be only be configured using the command line interface. During this time window, these duplicate switch events will be accumulated to keep track of how many have occurred. After the time window has expired, an Email message for the event will be transmitted that also includes the count of how many duplicate events were accumulated and the time of the last received event. If additional switch events are received, then duplicate Email messages will be sent.

Using the Call Home profile manager

Use the Call Home Profile Manager dialog (Figure 32) to manage all profiles on a switch. You can add new profiles, remove profiles, edit profiles, and make copies of existing profiles. To display the Call Home Profile Manager dialog, open the Switch menu, select **Call Home**, and select **Profile Manager**. The Profiles list shows all profiles on the switch. The Email List shows all Email addresses associated with the selected profile in the Profiles list. The Apply Changes to Multiple Switches in Fabric option allows you to propagate all profiles on the switch to one or more switches in the fabric. See "Applying All Profiles on a switch to other switches" on page 4-91 for more information.

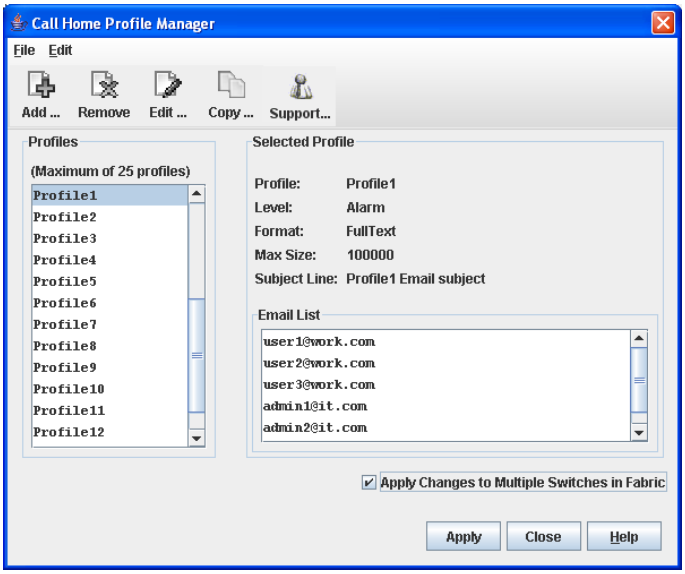

Figure 32. Call Home Profile Manager dialog

Using the Call Home profile editor

Use the Call Home Profile Editor dialog when creating a new profile, and editing/copying an existing profile. The Call Home Profile Editor dialog is displayed after clicking the Add, Edit, or Copy buttons on the Call Home Profile Manager dialog. Alternatively, you can open the Edit menu, and select **Add New Profile**, **Edit Profile,** or **Copy Profile** The name in the title bar changes to reflect adding a new profile, making a copy of an existing profile, or editing an existing profile. Enter a name for the profile, select an event level threshold, a format type for the message text being sent (short/full), enter the size of the message being sent, enter the subject of the Email, and enter the Email address(es) of the recipients. Click the **Add** button to add the Email address(es) to the list. Click the **OK** button to save the changes.

You can use the Call Home Profile Editor dialog to make a copy of an existing profile. In the Call Home Profile Manager dialog, select a profile in the list of existing profiles. To open the Call Home Profile Editor dialog, click the **Copy** button or open the Edit menu and select **Copy Profile**. The dialog is pre-populated with all of the information from the selected profile, except the name. Enter a unique name for the profile copy and click the **OK** button to save the new profile.

You can use the Call Home Profile Editor dialog (Figure 33) to create a new Tech Support profile and edit an existing Tech Support profile. See "Using the Call Home Profile Editor - Tech Support Center Profile Dialog" for more information.

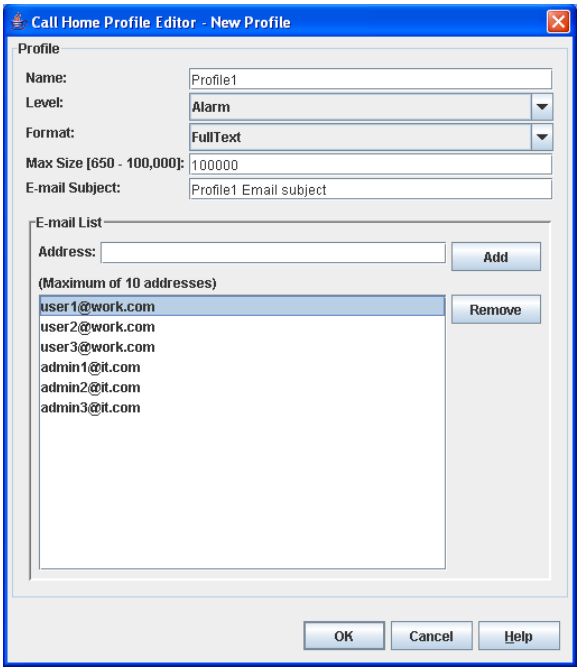

Figure 33. Call Home profile editor dialog

Using the Call Home profile editor—Tech Support Center Profile dialog

You can use the Call Home Profile Editor—Tech Support Center Profile dialog (Figure 34) to create, edit, or remove a Tech Support Center profile. You can open the Call Home Profile Editor - Tech Support Center Profile dialog two ways: click the **Support** button on the tool bar in the Call Home Profile Manager dialog, or open the Edit menu and select **Create Tech Support Center Profile**. The name in the title bar changes to reflect the Tech Support profile function (create or edit).

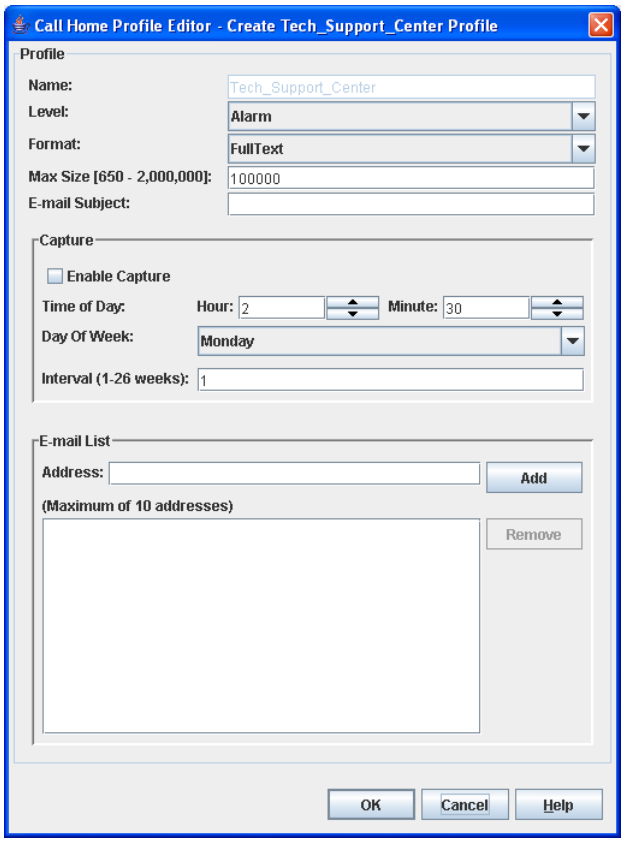

Figure 34. Call Home profile editor—Tech Support Center Profile dialog

Table 24 lists the fields in the Call Home Editor—Tech Support Center Profile dialog.

Table 24. Call Home profile editor—Tech Support Center profile dialog fields

Field	Description
Name	The name automatically assigned to the profile. This profile cannot be changed or deleted, but the settings can be modified.
Level	The severity level of the event (Alarm, Critical, Warning). The level of events processed by the profile to produce Emails that will be sent to the Email addresses listed in the profile.
Max Size (650-2,000,000)	The maximum number of bytes allowed for a Email message compiled for the profile. Most Email messages are relatively small, under 2KB. However, Emails that are produced by a capture operation can be as large as 1MB due to the inclusion of file attachments.
E-mail Subject	The subject line in the Email that will be sent. The string that is appended to the CallHome generated string for the Email message subject line.
Enable Capture	Select to enable or disable the capture operations for the profile. Only the Tech Support Center profile is allowed to define and execute capture operations on the switch.
Time of Day	The time of day, in HH:MM format, when the capture operation will be executed on the switch. Only the Tech Support Center profile is allowed to define and execute capture operations on the switch. The default is 02:30.
Day of Week	The day of the week, specified as Sunday, Monday, Tuesday, Wednesday, Thursday, Friday or Saturday, when the capture operation will be executed on the switch. The default is Monday.
Interval (1-26 weeks)	The number of weeks that must pass between executions of the capture operation. The default is 1.
Address	The Email address of the recipient being added to the Tech Support Center profile. A maximum of 10 addresses is allowed and displayed in the addresses window.

Applying All Profiles on a switch to other switches

You can apply all profiles on a switch to one or more switches in a fabric. The Call Home Profile Multiple Switch Apply dialog (Figure 35) is displayed after selecting the **Apply Changes to Multiple Switches in Fabric** option on the Call Home Profile Manager dialog. The Available Switches list shows all switches in the fabric. Switch names that are greyed-out do not have current Call Home firmware, and cannot receive any profiles. The Selected Switches list shows the switch names that you selected to receive all profiles from the switch. In the Available Switches list, select the switches in the fabric to receive all profiles, and click the double-arrow button to move them to the Selected Switches list. Click the **OK** button to start the process. The Results area indicates success or failure of applying all the profiles on a switch to the switches you selected.

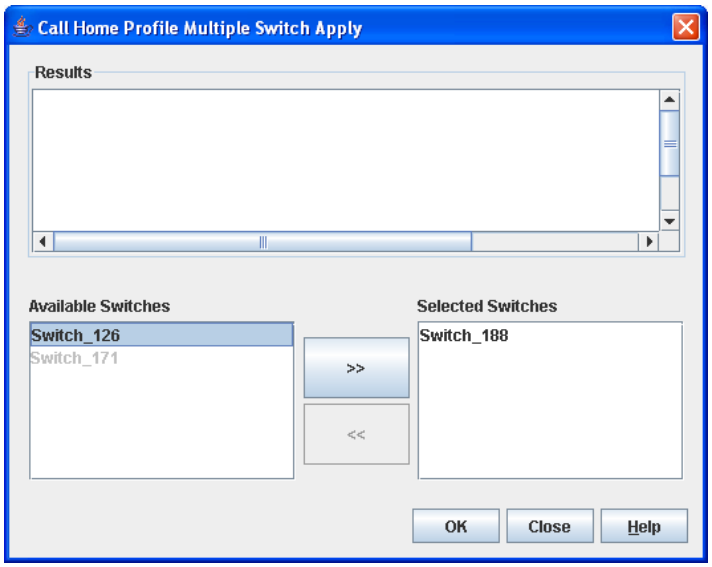

Figure 35. Call Home Profile Multiple Switch Apply dialog

Using the Call Home message queue

Use the Call Home Message Queue dialog (Figure 36) to access the logged call home statistics. Click the **Update Stats** button to refresh with the most recent switch Call Home information. Click the **Clear Queue** button to clear the current statistics.

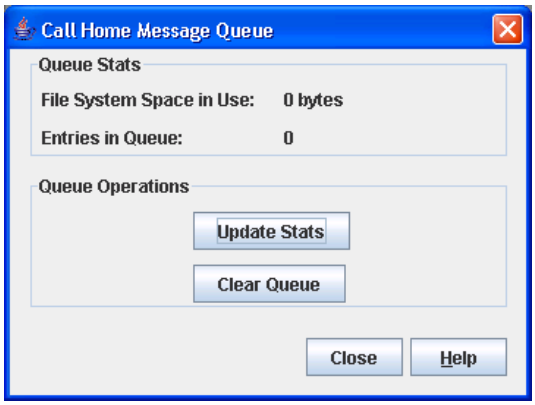

Figure 36. Call Home Message Queue dialog

Testing Call Home profiles

Use the Call Home Test Profile dialog (Figure 37) to test the Call Home parameters currently configured. Select a profile in the window, and click the **Test** button. To display the Call Home Test Profile dialog, open the Switch menu, select **Call Home**, and select **Test Profile**.

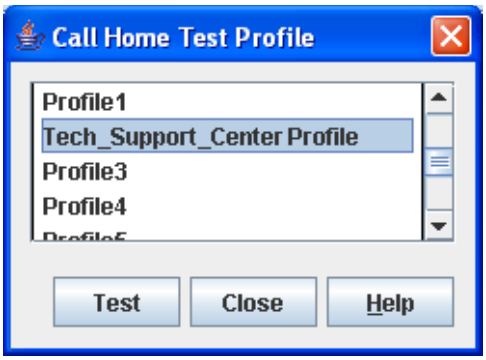

Figure 37. Call Home Profile Manager dialog

Change over

Changes the inactive SMTP server to become the active SMTP server. To make the inactive SMTP become the active SMTP, open the Switch menu, select **Call Home**, and select **Change Over**. Click the **OK** button to confirm the change over.

Chapter 5. Managing ports

The data windows provide port information and port statistics for selected ports. This chapter describes the following tasks that manage ports and devices:

- Using the Port Information data window
- Using the Port Statistics data window
- Viewing and configuring ports
- Resetting a port
- Testing ports
- Mapping ports

Using the Port Information data window

The Port Information data window, shown in Figure 38, displays detailed port information for the selected ports. To open the Port Information data window, click the **Port Info** data window tab.

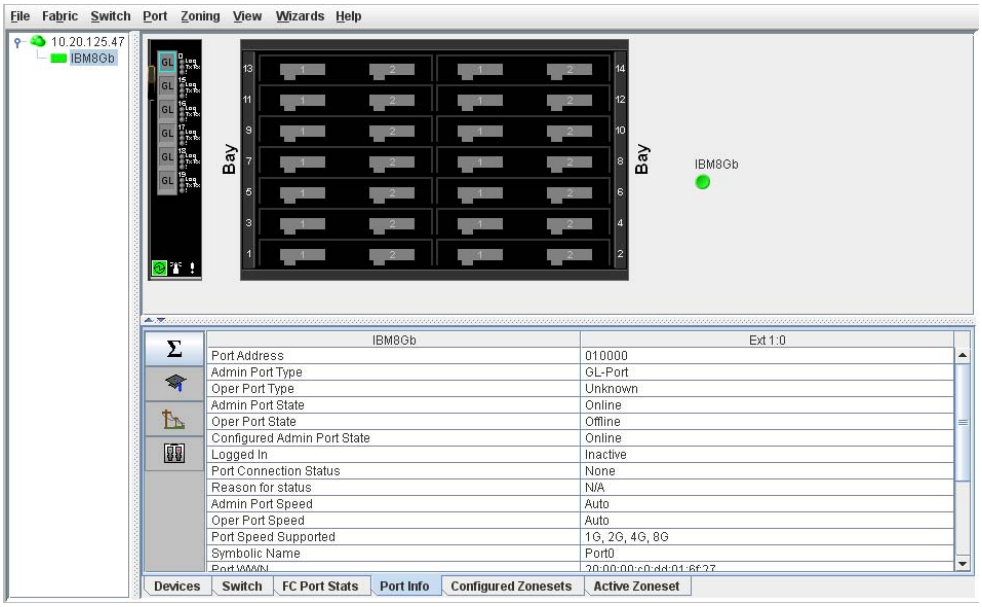

Figure 38. Port Information data window

Information in the Port Information data window is grouped and viewed by the Summary, Advanced, Extended Credits, and Media buttons (from top to bottom) as shown in Figure 39. Click a button to display the corresponding information in the data window on the right.

Figure 39. Port Information data window buttons

The Port Information data window entries are listed in Table 25.

Table 25. Port Information Data Window entries

Entry	Description
Summary Group	
Port Address	Port Fibre Channel address
Administrative Port Type	The administrative port type (G, GL, F, FL, or Donor). This value is persistent; it will be maintained during a switch reset. During port auto-configuration, it will be used to determine which operational port states are allowed.
Operational Port Type	The port type that is currently active. This value will be set during port auto-configuration based on the administrative port type.
Administrative Port State	The port state (Online, Offline, Diagnostics, or Down) that has been set by the user. This state may be different from the configured administrative state if the user has not saved it in the switch configuration. This state is used at the time it is set to try to set the port operational state. This value is not persistent and will be lost on a switch reset.
Operational Port State	The port state that is currently active. This value may be different from the administrative port state, for example due to an error condition.
Configured Administrative Port State	The port state (Online, Offline, Diagnostics, or Down) that is saved in the switch configuration, either by the user or at the factory. This value is persistent; it will be maintained during a switch reset, and will be used after a reset to set the port operational state.
Logged In	Indicates whether logged in or not
Port Connection Status	Port connection status. Status can be None, Connecting, Connected or Isolated

Table 25. Port Information Data Window entries (Continued)

Entry	Description
Reason for Status	Why E_Port is isolated
Administrative Port Speed	The speed requested by the user
Operational Port Speed	The speed actually being used by the port
Port Speed Supported	The speeds supported by the port (2 Gbps, 4 Gbps, or 8 Gbps)
Symbolic Name	Port symbolic name
Port WWN	Port world wide name
POST Status	Status from the most recent Power On Self Test
POST Fault Code	Fault code from the most recent Power On Self Test
Test Status	Status from the most recent port test
Test Fault Code	Fault code from the most recent port test
Advanced Group	
MFS Mode	Multiple Frame Sequence bundling status
Configured I/O Stream Guard	The requested RSCN message suppression status. Status can be enabled, disabled, or automatically determined by the switch.
Operational I/O Stream Guard	The operational RSCN message suppression status.
Device Scan	Device scan status. Enabled means the switch queries the connected device during login for FC-4 descriptor information.
Auto Performance Tuning	Enables the switch to dynamically control the MFS_Enable, VI_Enable and LCF_Enable features based on the operational state of the port
AL Fairness	Controls how frequently the switch can arbitrate for access. Applies only to ports running in loop (FL) mode
Port Binding	N/A—does not apply to this switch
Extended Credits Group	
Extended Credits Requested	Requested number of requested credits
Max Credits Available	The maximum number of credits granted to a port that can be used when extending port credits
Credits to Donate	The number of credits available to be donated by the selected port
Donor Group	The donor group of the selected port

Table 25. Port Information Data Window entries (Continued)

Entry	Description
Valid Donor Groups	The number of separate groups within which extended credits may be donated and assigned
Media Group	
Media Type	The transceiver fibre type, such as single mode, multi-mode, copper
Media Speed	The maximum transceiver speed
Media	The transceiver type
Media Transmitter	The transceiver transmitter type, such as long-wave, shortwave, electrical
Media Distance	The maximum transceiver transmission distance
Media Vendor	The company that manufactured the SFP
Media Vendor ID	The IEEE registered company ID
Media Part Number	The part number assigned to the SFP
Media Revision	Transceiver hardware version

Using the Port Statistics data window

The Port Statistics data window, shown in Figure 40, displays statistics about port performance. To open the Port Statistics data window, select one or more ports and click the Port Stats data window tab.

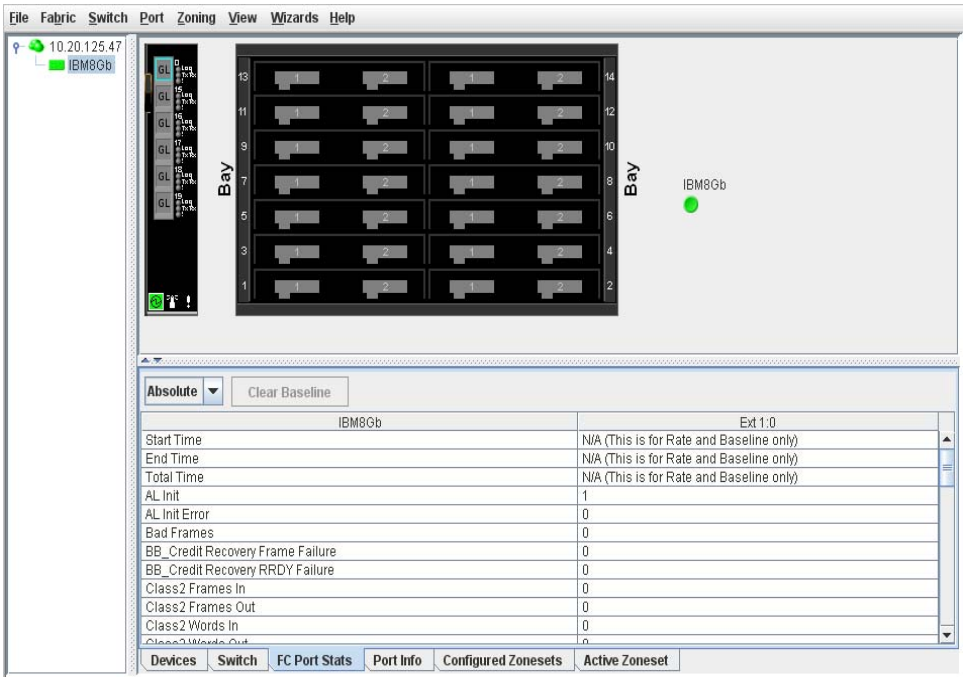

Figure 40. Port Statistics Data Window

The Statistics drop-down list is available on the Port Statistics data window, and provides different ways to view detailed port information. Click the down arrow to open the drop-down list, and select **Absolute** to view the total count of statistics since the last switch or port reset. Select **Rate** to view the number of statistics counted per second over the polling period. Select **Baseline** to view the total count of statistics since the last time the baseline was set. When viewing baseline statistics, click the **Clear Baseline** button to set the current baseline. The baseline will also be set when the switch status changes from unreachable to reachable.

Table 26 describes the Port Statistics data window entries.

Table 26. Port Statistics Data Window entries

Entry	Description
Start Time	The beginning of the period over which the statistics apply. The start time for the Absolute view is not applicable. The start time for the Rate view is the beginning of polling interval. The start time for the Baseline view is the last time the baseline was set.
End Time	The last time the statistics were updated on the display.
Total Time	Total time period from start time to end time.
Al Init	Number of times the port entered the initialization state.
AL Init Error	Number of times the port entered initialization and the initialization failed. Increments count when port has a sync loss.
Bad Frames	Number of frames that were truncated due to a loss of sync or the frame didn't end with an EOF.
BB_CreditRecovery FrameFailure	Number of times more frames were lost during a credit recovery period than the recovery process could resolve. This value causes a Link Reset to recover the credits.
BB_CreditRecovery RRDYFailure	Number of times more R_RDYs were lost during a credit recovery period than the recovery process could resolve. This value causes a Link Reset to recover the credits.
Class 2 Frames In	Number of class 2 frames received by this port.
Class 2 Frames Out	Number of class 2 frames transmitted by this port.
Class 2 Words In	Number of class 2 words received by this port.
Class 2 Words Out	Number of class 2 words transmitted by this port.
Class 3 Frames In	Number of class 3 frames received by this port.
Class 3 Frames Out	Number of class 3 frames transmitted by this port.
Class 3 Toss	Number of class 3 frames that were discarded by this port. A frame can be discarded because of detection of a missing frame (based on SEQ_CNT), detection of an E_D_TOV timeout, receiving a reject frame, or receiving a frame on an offline port.
Class 3 Words In	Number of class 3 words received by this port.
Class 3 Words Out	Number of class 3 words transmitted by this port.
Decode Errors	Number of invalid transmission words detected during decoding. Decoding is from the 10-bit characters and special K characters.

Table 26. Port Statistics Data Window entries (Continued)

Entry	Description
Ep Connects	Number of E_Port logins.
FBusy	Number of class 2 and class 3 fabric busy (F_BSY) frames generated by this port in response to incoming frames. This value usually indicates a busy condition on the fabric or N_port that is preventing delivery of this frame.
Flow Errors	Number of times a frame is received and all the switch ports receive buffers are full. The normal Fabric Login exchange of flow control credit should prevent this from occurring. The frame will be discarded.
FReject	Number of frames, from devices, that have been rejected. Frames can be rejected for any of a large number of reasons.
Invalid CRC	Number of invalid Cyclic Redundancy Check (CRC) frames detected.
Invalid Destination Address	Number of address identifier (S_ID, D_ID) errors. AL_PA equals non-zero AL_PA found on F_Port.
Link Failures	Number of optical link failures detected by this port. A link failure is a loss of synchronization or loss of signal while not in the offline state. A loss of signal causes the switch to attempt to re-establish the link. If the link is not re-established, a link failure is counted. A link reset is performed after a link failure.
LIP (AL_PD,AL_PS)	Number of F7, AL_PS LIPs, or AL_PD (vendor specific) resets performed.
LIP(F7,AL_PS)	This LIP reinitializes the loop. An L_port, identified by AL_PS, may have noticed a performance degradation and is trying to restore the loop.
LIP(F7,F7)	A loop initialization primitive frame that acquires an AL_PA.
LIP(F8,AL_PS)	This LIP denotes a loop failure detected by the L_port identified by AL_PS.
LIP(F8,F7)	A loop initialization primitive frame used to indicate that a Loop Failure has been detected at its receiver and does not have a valid AL_PA.
Login Count	Number of device logins that have occurred on the switch.
Logout Count	Number of device logouts that have occurred on the switch.
Long Frame Count	Number of incidents in which one or more frames greater than the maximum size (2,136 bytes) are received
Loop Timeouts	Number of loop timeouts.
Loss Of Sync	Number of synchronization losses (>100 ms) detected by this port. A loss of synchronization is detected by receipt of an invalid transmission word.
Loop Timeouts	Number of loop timeouts.
Primitive Sequence Errors	Number of bad primitives received by the port.

Table 26. Port Statistics Data Window entries (Continued)

Entry	Description
Rx Link Resets	Number of link reset primitives received from an attached device.
Rx Offline Sequences	Number of offline sequence primitives received by the port.
Short Frame Count	Number of incidents in which one or more frames smaller than the minimum size (24 bytes) are received
Total Errors	Total number of primitive and non-primitive port link errors.
Total Link Resets	Number of link-reset primitives transmitted and received by the port.
Total LIPs Received	Number of loop initialization primitive frames received.
Total LIPs Transmitted	Number of loop initialization primitive frames transmitted.
Tx Offline Sequences	Number of offline primitives transmitted by the port.
Total Rx Frames	Total number of frames received by the port.
Total Rx Words	Total number of words received by the port.
Total Tx Frames	Total number of frames transmitted by the port.
Total Tx Words	Total number of words transmitted by the port.
Tx Link Resets	Number of link reset primitives sent from this port to an attached port.
TotalTXErrors	Total number of errors transmitted by the port.
TotalRXErrors	Total number of errors received by the port.
Total Offline Sequences	Total number of offline sequences transmitted and received by the port.

Viewing and configuring ports

Port color and text provide information about the port and its operational state. To display port number and status information for a port, position the cursor over a port on the faceplate display. The status information changes depending on the View menu option selected. Green indicates active; gray indicates inactive. Context-sensitive popup menus are displayed when you right-click a port icon in the faceplate display. Use the drop-down lists in the Port Properties dialog to change the following parameters:

- Port symbolic name
- Port states
- Port types
- Port speeds
- Port transceiver media status
- I/O Stream Guard
- Device scan

The port settings or characteristics are configured using the Port Properties dialog shown in Figure 41. To open the Port Properties dialog, select one or more ports, open the Port menu, and then select **Port Properties**.

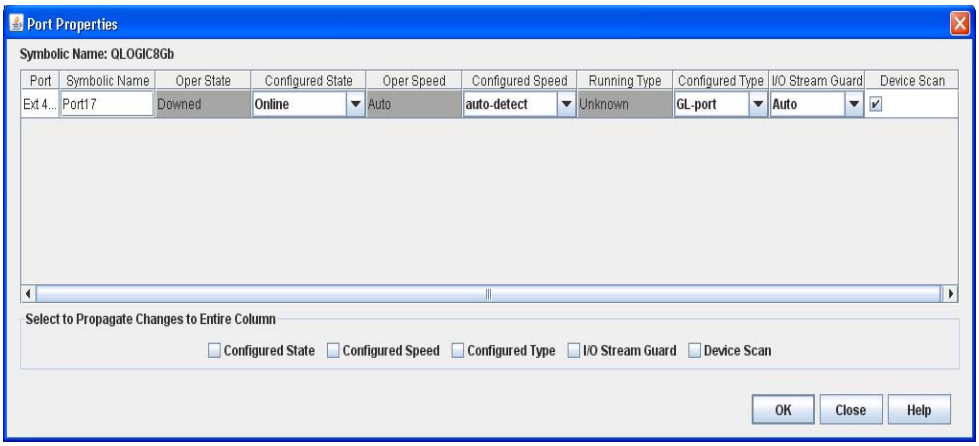

Figure 41. Port Properties dialog

Notes:

Use the **Select to Propagate Changes to Entire Column** options to propagate the same change to all selected ports; select the options before making a change to a port.

Port symbolic name

To change the symbolic name of a port, do the following:

1. Open the faceplate display and select a port.
2. Open the Port menu and select **Port Properties** to open the Port Properties dialog.
3. Click inside the Symbolic Name field, and enter a new name for the port in the port symbolic name.
4. Click the **OK** button.

Port states

The port operational state refers to the actual port state and not the administrative state you may have assigned. The port administrative state refers to the user-requested state. Refer ”Port operational states” on page 5-101 to for more information. Port administrative states have two forms: the configured administrative state and the current administrative state. Refer ”Port administrative states” on page 5-101 to for more information.

Port operational states

To view the operational state on each port in the faceplate display, open the View menu and select **View Port States**. Table 27 lists the possible operational states and their meanings.

Table 27. Port operational states

State	Description
	Online—port is active and ready to send data.
None	Inactive—port operational state is offline, but administrative state is online.
	Isolated—E_Port has lost its connection. See Table 25 for information about why the E_Port has isolated.
	Offline—port is active, can receive signal, but cannot accept a device login.
	Diagnostics—port is in diagnostics mode in preparation for testing.
	Downed—the port is disabled, power is removed from the lasers, and can't be logged in.

Port administrative states

The port administrative state determines the operational state of a port. The port administrative state has two forms: the configured administrative state and the current administrative state.

- Configured administrative state—the state that is saved in the switch configuration and is preserved across switch resets. QuickTools always makes changes to the configured administrative state.
- Current administrative state—the state that is applied to the port for temporary purposes and is not preserved across switch resets. The current administrative state is set with the Set Port command using the command line interface.

Table 28 describes the port administrative states. To change the port administrative state, do the following:

1. Select one or more ports in the faceplate display.
2. Open the Port menu and select **Port Properties** to open the Port Properties dialog.
3. Select the **Port State** option from the drop-down list.
4. Click the **OK** button to write the new port state request to the switch.

Table 28. Port administrative states

State	Description
Online	Activates and prepares port to send data.
Offline	Prevents port from receiving signal and accepting a device login.
Diagnostics	Prepares port for testing and prevents the port from accepting a device login.
Downed	Disables the port.

Port types

To display port type status, open the View menu, and select **View Port Types**. Table 29 lists the possible port types and their meanings. The ports can be configured to self-discover the proper type to match the device or switch to which it is connected.

To change the port type, do the following:

1. Select one or more ports in the faceplate display.
2. Open the Port menu and select **Port Properties** to open the Port Properties dialog.
3. Select the **Port Type** option from the drop-down list.
4. Click the **OK** button to write the new port type to the switch.

Table 29. Port types

State	Description
F_Port	Fabric port—supports a single public device (N_Port).
FL_Port	Fabric loop port —self discovers a single device (N_Port) or a loop of up to 126 public devices (NL_Port).
G_Port	Generic port—self discovers as an F_Port or an E_Port.
GL_Port	Generic loop port—self discovers as an F_Port, FL_Port, or an E_Port. GL_Port is the default port type. A single device on a public loop will attempt to configure as an F_Port first, then if that fails, as an FL_Port.
E_Port	Expansion port—the mode that a G_Port or GL_Port is in when attached by an ISL (inter-switch link) to another fibre channel switch.
Donor	Donor port—allows buffer credits to be used by another port.

Port speeds

The external switch ports can support 1, 2, 4, or 8 Gbps. The internal ports only support 2, 4, and 8 Gbps. All ports can be configured for either a fixed transmission speed or to sense (auto-detect) the transmission speed of the device to which it is connected. To display the speed of each port, open the View menu and select **View Port Speeds**. Table 30 lists the possible port speeds.

To change the port transmission speed, do the following:

1. Select one or more ports in the faceplate display.
2. Open the Port menu and select **Port Properties** to open the Port Properties dialog.
3. Select the **Port Speed** option from the drop-down list.
4. Click the **OK** button to write the new port speed to the switch.

Table 30. Port speeds

State	Description
Auto-Detect	Matches the transmission speed of the connected device. This state is the default.
2 Gbps	Sets the transmission speed to 2 Gbps.
4 Gbps	Sets the transmission speed to 4 Gbps
8 Gbps	Sets the transmission speed to 8 Gbps

Port transceiver media status

To display transceiver media status, open the View menu and select **View Port Media**. Table 31 lists the port media states and their meanings.

Table 31. Port transceiver media view

Media Icon	Description
	Optical SFP, online (green/black), logged-in, active, and ready to send data.
	Optical SFP, offline (gray/black), not logged-in, active, can receive signal, but cannot accept a device login
	Optical SFP, unlicensed (dark gray/black)
	Optical SFP, unknown, unlicensed (dark gray/blue)
None	Empty port; no transceiver installed (gray) or unlicensed (dark gray)

I/O Stream Guard

The I/O Stream Guard feature suppresses the Registered State Change Notification (RSCN) messages on a port basis. I/O Stream Guard should be enabled only on ports connected to initiator devices. To configure the I/O Stream Guard option using the Port Properties dialog, open the Port menu, and select **Port Properties**. Select the option that corresponds to one of the following options:

- Enable—suppresses the reception of RSCN messages from other ports for which I/O Stream Guard is enabled.
- Disable—allows free transmission and reception of RSCN messages.
- Auto—suppresses the reception of RSCN messages when the port is connected to an initiator device with a QLogic HBA. For older QLogic adapters, such as the QLA2200, Device Scan must be enabled. The default is Auto. See "Device scan" on page 5-104.

Device scan

The Device Scan feature queries the connected device during login for FC-4 descriptor information. Disable this parameter only if the scan creates a conflict with the connected device.

Auto performance tuning and AL fairness

The Auto Perf Tuning and AL Fairness settings are configured using the Advanced Port Properties dialog shown in Figure 42. The Auto Perf Tuning option enables the switch to dynamically control the MFS_Enable, VI_Enable and LCF_Enable features based on the operational state of the port.

The AL Fairness option controls how frequently the switch can arbitrate for access. Once a port has arbitrated and won access to the loop, it does not try again until all others have had an opportunity to arbitrate for the loop. This setting applies only to ports running in loop (FL) mode.

To open the Advanced Port Properties dialog, select one or more ports, open the Port menu, and select **Advanced Port Properties**.

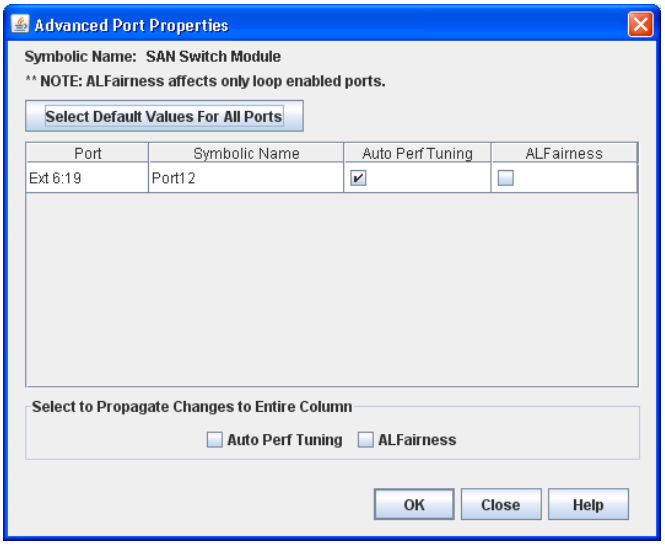

Figure 42. Advanced Port Properties dialog

Resetting a port

The Reset Port option reinitializes the port using the saved configuration. To reset a port, do the following:

1. In the faceplate display, select the port(s) to be reset.
2. Open the Port menu and select **Reset Port**.
3. Click the **OK** button to reset the selected port(s).

Testing ports

The port diagnostic tests verify correct port operation by sending a frame out through the loop, and then verifying that the frame received matches the frame that was sent. Only one port can be tested at a time for each type of test.

The Port Diagnostics dialog shown in Figure 43 presents the following tests:

- SerDes level (Internal)—the SerDes level test verifies port circuitry. The SerDes level test sends a test frame from the ASIC through the SerDes chip and back to the ASIC for the selected ports. The port passes the test if the frame that was sent by the ASIC matches the test frame that was received. This test requires that the port be in diagnostics mode, and therefore, disrupts communication.
- SFP level (External)—the SFP level test verifies port circuitry. The SFP level test sends a test frame from the ASIC through the SerDes chip, through the SFP transceiver fitted with an external loopback plug, and back to the ASIC for the selected ports. The port passes the test if the test frame that was sent by the ASIC matches the test frame that was received. This test requires that the port be in diagnostics mode, and therefore, disrupts communication.
- Node-to-Node (Online)—the Node-to-Node test verifies communications between the port and its device node or device loop. The port being tested must be online and connected to a remote device. The port passes the test if the frame that was sent by the ASIC matches the frame that was received. This test requires that the port be online, and therefore, does not disrupt communication.

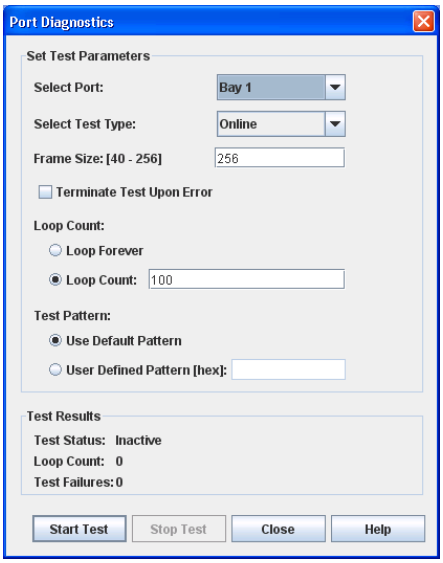

Figure 43. Port Diagnostics dialog

To run a diagnostics test on a port, do the following:

1. In the faceplate display, select a port, open the Port menu and select **Port Diagnostics.**
2. Choose one of the following:
   - Select **Online Port Diagnostics** to open the Port Diagnostics dialog. Select the port to test in the Select Port drop-down list. The test type is **Online** by default.
   - Select **Offline Port Diagnostics** to open the Port Diagnostics dialog (this option will disrupt traffic). Select the port number and **Internal** or **External** test type in the drop-down list.
3. Enter a frame size (default is 256).
4. Enable or disable the **Terminate Test Upon Error** option.
5. Select a **Loop Count** option. The Loop Forever option runs the test until you click the **Stop Test** button. The Loop Count option runs the test a specific number of times.
6. Select a Test Pattern option. Accept the default test pattern, or select the **User Defined** option and enter a value.
7. Click the **Start Test** button to begin the test. Observe the results in the Test Results area.

Notes:

If the Test Status field in the Test Results area indicates Failed, note the Test Fault Code displayed in the Port Information data window and contact Tech Support.

Mapping ports

When the switch is in transparent mode, the Map Ports dialog enables you to configure data traffic routes from server bay ports to one or more uplink ports. Server bay ports are called TH_Ports (transparent host). An uplink port that attaches to an external server must be configured as a TH_Port. At least one uplink port must connect to a fabric switch that supports NPIV. An uplink port that connects to a fabric switch is a TF_Port (transparent fabric). By default, the six uplink (external) ports are TF_Ports.

You can assign a TH_Port to multiple TF_Ports using the Map Port dialog box. For redundancy, a backup port mapping can also be specified. Leaving a TH_Port unmapped has the same effect as unplugging a Fibre Channel cable. You can map multiple primary and backup ports for any TH_Port. A port designated as primary will be the first path chosen. If there are multiple primary ports, the TH_Ports are distributed (using an algorithm) across the TF_Ports. Ports designated as backup ports become active only when all primary ports fail.

To open the Map Ports dialog box (Figure 44), open the Port menu, and then select **Map Ports**.

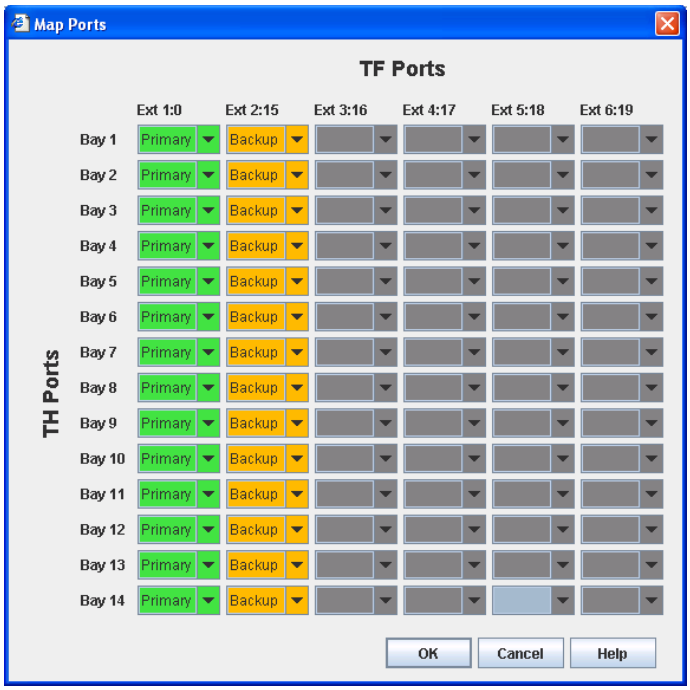

Figure 44. Map Ports dialog

Table 32 shows the default primary and backup TF_Port mappings.

Table 32. Default primary and backup TF_Port mapping

TF_Ports	**0**	**15**	**16**	**17**	**18**	**19**
TH_Port 1						
TH_Port 2						
TH_Port 3						
TH_Port 4						
TH_Port 5						
TH_Port 6						
TH_Port 7						
TH_Port 8						
TH_Port 9						
TH_Port 10						
TH_Port 11						
TH_Port 12						
TH_Port 13						
TH_Port 14						

Primary

Backup

Notes:

The port map affects the operational state of TH_Ports. If a TH_Port is not mapped to a TF_Port, the TH_Port will be listed as offline. If a TH_Port is mapped to a TF_Port, but the TF_Port is offline or nonexistent, the TH_Port will be listed as downed. If a TH_Port is mapped to a TF_Port and the TF_Port is online, the TH_Port will be listed as online. Any TH_Port (external or internal) port must be mapped to a TF_Port to activate the connection and allow data to pass. Without a connection, the TH_Port is downed.

Appendix A. Getting help and technical assistance

If you need help, service, or technical assistance or just want more information about Lenovo products, you will find a wide variety of sources available from Lenovo to assist you.

Use this information to obtain additional information about Lenovo and Lenovo products, and determine what to do if you experience a problem with your Lenovo system or optional device.

Note: This section includes references to IBM web sites and information about obtaining service. IBM is Lenovo's preferred service provider for the BladeCenter, System x, Flex System, and NeXtScale System products.

Before you call

Before you call, make sure that you have taken these steps to try to solve the problem yourself.

If you believe that you require warranty service for your Lenovo product, the service technicians will be able to assist you more efficiently if you prepare before you call.

- Check all cables to make sure that they are connected.
- Check the power switches to make sure that the system and any optional devices are turned on.
- Check for updated software, firmware, and operating-system device drivers for your Lenovo product. The Lenovo Warranty terms and conditions state that you, the owner of the Lenovo product, are responsible for maintaining and updating all software and firmware for the product (unless it is covered by an additional maintenance contract). Your service technician will request that you upgrade your software and firmware if the problem has a documented solution within a software upgrade.
- If you have installed new hardware or software in your environment, check http://www.ibm.com/systems/info/x86servers/serverproven/compat/us to make sure that the hardware and software is supported by your product.
- Go to http://www.ibm.com/supportportal to check for information to help you solve the problem.
- Gather the following information to provide to the service technician. This data will help the service technician quickly provide a solution to your problem and ensure that you receive the level of service for which you might have contracted.
  - Hardware and Software Maintenance agreement contract numbers, if applicable
  - Machine type number (Lenovo 4-digit machine identifier)
  - Model number
  - Serial number
  - Current system UEFI and firmware levels
  - Other pertinent information such as error messages and logs

- Go to http://www.ibm.com/support/entry/portal/Open_service_request to submit an Electronic Service Request. Submitting an Electronic Service Request will start the process of determining a solution to your problem by making the pertinent information available to the service technicians. The IBM service technicians can start working on your solution as soon as you have completed and submitted an Electronic Service Request.

You can solve many problems without outside assistance by following the troubleshooting procedures that Lenovo provides in the online help or in the Lenovo product documentation. The Lenovo product documentation also describes the diagnostic tests that you can perform. The documentation for most systems, operating systems, and programs contains troubleshooting procedures and explanations of error messages and error codes. If you suspect a software problem, see the documentation for the operating system or program.

Using the documentation

Information about your Lenovo system and preinstalled software, if any, or optional device is available in the product documentation. That documentation can include printed documents, online documents, readme files, and help files.

See the troubleshooting information in your system documentation for instructions for using the diagnostic programs. The troubleshooting information or the diagnostic programs might tell you that you need additional or updated device drivers or other software. Lenovo maintains pages on the World Wide Web where you can get the latest technical information and download device drivers and updates. To access these pages, go to http://www.ibm.com/supportportal.

Getting help and information from the World Wide Web

Up-to-date information about Lenovo products and support is available on the World Wide Web.

On the World Wide Web, up-to-date information about Lenovo systems, optional devices, services, and support is available at http://www.ibm.com/supportportal. The most current version of the Flex System product documentation is available at http://pic.dhe.ibm.com/infocenter/flexsys/information/index.jsp.

Software service and support

Through IBM Support Line, you can get telephone assistance, for a fee, with usage, configuration, and software problems with your Lenovo products.

For more information about Support Line and other IBM services, see http://www.ibm.com/services or see http://www.ibm.com/planetwide for support telephone numbers. In the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

Hardware service and support

IBM is Lenovo's preferred service provider for the BladeCenter, System x, Flex System and NeXtScale System products.

You can receive hardware service through your Lenovo reseller or from IBM. To locate a reseller authorized by Lenovo to provide warranty service, go to http://www.ibm.com/partnerworld and click Business Partner Locator. For IBM support telephone numbers, see http://www.ibm.com/planetwide. In the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

In the U.S. and Canada, hardware service and support is available 24 hours a day, 7 days a week. In the U.K., these services are available Monday through Friday, from 9 a.m. to 6 p.m.

Taiwan product service

IBM is Lenovo's preferred service provider for the BladeCenter, System x, Flex System and NeXtScale System products. Use this information to contact IBM Taiwan product service.

台灣 IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路 7 號 3 樓
電話：0800-016-888

IBM Taiwan product service contact information:

IBM Taiwan Corporation
3F, No 7, Song Ren Rd.
Taipei, Taiwan
Telephone: 0800-016-888

Appendix B. Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area.

Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

Lenovo (United States), Inc.
1009 Think Place - Building One
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk.

Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Trademarks

Lenovo, the Lenovo logo, BladeCenter, Flex System, NeXtScale System, and System x are trademarks of Lenovo in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Important notes

Processor speed indicates the internal clock speed of the microprocessor; other factors also affect application performance.

Processor speed indicates the internal clock speed of the microprocessor; other factors also affect application performance.

CD or DVD drive speed is the variable read rate. Actual speeds vary and are often less than the possible maximum.

When referring to processor storage, real and virtual storage, or channel volume, KB stands for 1 024 bytes, MB stands for 1 048 576 bytes, and GB stands for 1 073 741 824 bytes.

When referring to hard disk drive capacity or communications volume, MB stands for 1 000 000 bytes, and GB stands for 1 000 000 000 bytes. Total user-accessible capacity can vary depending on operating environments.

Maximum internal hard disk drive capacities assume the replacement of any standard hard disk drives and population of all hard-disk-drive bays with the largest currently supported drives that are available from Lenovo.

Maximum memory might require replacement of the standard memory with an optional memory module.

Each solid-state memory cell has an intrinsic, finite number of write cycles that the cell can incur. Therefore, a solid-state device has a maximum number of write cycles that it can be subjected to, expressed as `total bytes written` (TBW). A device that has exceeded this limit might fail to respond to system-generated commands or might be incapable of being written to. Lenovo is not responsible for replacement of a device that has exceeded its maximum guaranteed number of program/erase cycles, as documented in the Official Published Specifications for the device.

Lenovo makes no representations or warranties with respect to non-Lenovo products. Support (if any) for the non-Lenovo products is provided by the third party, not Lenovo.

Some software might differ from its retail version (if available) and might not include user manuals or all program functionality.

Glossary

Active Zone Set
The zone set that defines the current zoning for the fabric.

Active Firmware
The firmware image on the switch that is in use.

Administrative State
State that determines the operating state of the port or switch. The configured administrative state is stored in the switch configuration. The configured administrative state can be temporarily overridden using the command line interface.

Alarm
A message generated by the switch that specifically requests attention. Alarms are generated by several switch processes. Some alarms can be configured.

Alias
A named set of ports or devices. An alias is not a zone, and cannot have a zone or another alias as a member.

AL_PA
Arbitrated Loop Physical Address

Arbitrated Loop
A Fibre Channel topology where ports use arbitration to establish a point-to-point circuit.

Arbitrated Loop Physical Address (AL_PA)
A unique one-byte value assigned during loop initialization to each NL_Port on a loop.

ASIC
Application Specific Integrated Circuit

Auto Save
Zoning parameter that determines whether changes to the active zone set that a switch receives from other switches in the fabric will be saved to permanent memory on that switch.

BootP
A type of network server.

Buffer Credit
A measure of port buffer capacity equal to one frame.

Class 2 Service
A service that multiplexes frames at frame boundaries to or from one or more N_Ports with acknowledgment provided.

Class 3 Service
A service that multiplexes frames at frame boundaries to or from one or more N_Ports without acknowledgment.

Configured Zone Sets
The zone sets stored on a switch (excluding the active zone set).

Default Visibility
Zoning parameter that determines the level of communication among ports/devices when there is no active zone set.

Domain ID
User defined number that identifies the switch in the fabric.

Encryption Mode
Switch service that determines which encryption algorithms, key lengths, and certificates can be used. See Legacy Mode and Strict Mode.

Event Log
Log of messages describing events that occur in the fabric.

Expansion Port
E_Port that connects to another FC-SW-2 compliant switch.

Fabric Name
User defined name associated with the file that contains user list data for the fabric.

Fabric Port
An F_Port

Flash Memory

Memory on the switch that contains the chassis control firmware.

Frame

Data unit consisting of a start-of-frame (SOF) delimiter, header, data payload, CRC, and an end-of-frame (EOF) delimiter.

Hard Zone

Hard zoning divides the fabric for purposes of controlling discovery and inbound traffic.

Inactive Firmware

The firmware image on the switch that is not in use.

In-band Management

The ability to manage a switch through another switch over an inter-switch link.

Initiator

The device that initiates a data exchange with a target device.

Inter-Switch Link

The connection between two switches using E_Ports.

Legacy Mode

An encryption mode that uses encryption algorithms of 80 bits or greater, and keys with a length of 1,024 or greater.

LIP

Loop Initialization Primitive sequence

Logged-in LED

A port LED that indicates device login or loop initialization status.

Management Information Base

A set of guidelines and definitions for SNMP functions.

Management Workstation

PC workstation that manages the fabric through the fabric management switch.

Mesh Topology

A fabric in which each chassis has at least one port directly connected to each other chassis in the fabric.

MIB

Management Information Base

Multistage Topology

A fabric in which two or more edge switches connect to one or more core switches.

NL_Port

Node Loop Port. A Fibre Channel device port that supports arbitrated loop protocol.

N_Port

Node Port. A Fibre Channel device port in a point-to-point or fabric connection.

OK LED

A switch LED that indicates that the switch logic circuitry is receiving proper DC voltages.

Orphan Zone Set

Zones that are currently not in a zone set are considered to be part of the orphan zone set. The orphan zone set is not an actual zone set, but rather a way of displaying the zones that are not currently in a zone set.

Pending Firmware

The firmware image that will be activated upon the next switch reset.

POST

Power On Self Test

Power On Self Test (POST)

Diagnostics that the switch chassis performs at start up.

Principal Switch

The switch in the fabric that manages domain ID assignments.

QuickTools

Switch management web applet.

SFP

Small Form-Factor Pluggable.

Small Form-Factor Pluggable

A transceiver device, smaller than a GigaBit Interface Converter, that plugs into the Fibre Channel port.

SNMP

Simple Network Management Protocol

Soft Zone

Soft zoning divides the fabric for purposes of controlling discovery. Members of the same soft zone automatically discover and communicate freely with all other members of the same zone.

Strict Mode

An encryption mode that uses encryption algorithms of 112 bits or greater, and keys with a length of 2,048 or greater.

Switch Fault LED

A switch LED that indicates the status of the internal switch processor and the results of the Power On Self Test.

Target

A storage device that responds to an initiator device.

User Account

An object stored on a switch that consists of an account name, password, authority level, and expiration date.

VCCI

Voluntary Control Council for Interference

World Wide Name (WWN)

A unique 64-bit address assigned to a device by the device manufacturer.

WWN

World Wide Name

Zone

A set of ports or devices grouped together to control the exchange of information.

Zone Set

A set of zones grouped together. The active zone set defines the zoning for a fabric.

Zoning Database

The set of zone sets, zones, and aliases stored on a switch.

Index

Q

R

S

T

U

V

W

Z

Part Number: 00WA192

Printed in USA

(1P) P/N: 00WA192