McDATA® 4Gb SAN Switch
for HP p-Class BladeSystem user guide

hp ®

invent

Legal and notice information

McDATA® 4Gb SAN Switch for HP p-Class BladeSystem user guide

Contents

Tables

About this guide

This manual describes the McDATA® Web Server™ and McDATA Element Manager™ management tools for the McDATA 4Gb SAN Switch. McDATA Element Manager is referred to as Element Manager throughout this document. The McDATA 4Gb SAN Switch is a 10-port non-blocking Fibre Channel (FC) switch. This manual defines the features, components, and performance characteristics of the McDATA 4Gb SAN Switch.

The embedded McDATA Web Server and the Element Manager applications are the focus of this manual which is organized as follows:

- "Using McDATA Web Server/Element Manager" on page 11 describes how to use McDATA Web Server and Element Manager, their menus, and displays.
- "Managing Fabrics" on page 21 describes fabric management tasks of the McDATA Web Server.
- "Managing switches" on page 49 describes switch management tasks of the McDATA Web Server and Element Manager.
- "Managing ports" on page 85 describes port management tasks of the McDATA Web Server and Element Manager.

A glossary of terms and an index are also provided.

Intended audience

This manual introduces the switch management products and explains their installation and use. It is intended for users responsible for installing and using switch management tools.

Prerequisites

Prerequisites for using this product include:

- Knowledge of operation systems
- Knowledge of related hardware/software

Related documentation

In addition to this guide, please refer to the following documents for this product:

- *McDATA 4Gb SAN Switch for HP p-Class BladeSystem release notes AA-RW1ZD-TE*
- *McDATA 4Gb SAN Switch for HP p-Class BladeSystem quick setup instructions A8001-90002*
- *McDATA 4Gb SAN Switch for HP p-Class BladeSystem installation guide AA-RW1XC-TE*
- *McDATA 4Gb SAN Switch for HP p-Class BladeSystem command line interface guide, AA-RWEJA-TE*
- *HP StorageWorks HA-Fabric Manager user guide AA-RS2CH-TE*
- *HP StorageWorks HA-Fabric Manager release notes AA-RUR6J-TE*

These and other HP documents can be found on the HP documents web site: http://www.hp.com/support/.

Document conventions and symbols

Table 1 Document conventions

Convention	Element
Medium blue text: Figure 1	Cross-reference links and e-mail addresses
Medium blue, underlined text (http://www.hp.com)	Web site addresses
Bold font	• Key names • Text typed into a GUI element, such as into a box • GUI elements that are clicked or selected, such as menu and list items, buttons, and check boxes
Italics font	Text emphasis
`Monospace font`	• File and directory names • System output • Code • Text typed at the command-line
`Monospace, italic font`	• Code variables • Command-line variables
`Monospace, bold font`	Emphasis of file and directory names, system output, code, and text typed at the command line

⚠ **WARNING!** Indicates that failure to follow directions could result in bodily harm or death.

△ **CAUTION:** Indicates that failure to follow directions could result in damage to equipment or data.

🗒 **IMPORTANT:** Provides clarifying information or specific instructions.

🗒 **NOTE:** Provides additional information.

☆ **TIP:** Provides helpful hints and shortcuts.

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 acknowledgement 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/>.

HP technical support

Telephone numbers for worldwide technical support are listed on the HP support web site: http://www.hp.com/support/.

Collect the following information before calling:

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

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

HP strongly recommends that customers sign up online using the Subscriber's choice web site: http://www.hp.com/go/e-updates.

- Subscribing to this service provides you with e-mail updates on the latest product enhancements, newest versions of drivers, and firmware documentation updates as well as instant access to numerous other product resources.
- After signing up, you can quickly locate your products by selecting **Business support** and then **Storage** under Product Category.

HP-authorized reseller

For the name of your nearest HP-authorized reseller:

- In the United States, call 1-800-282-6672.
- Elsewhere, visit the HP web site: http://www.hp.com. Then click **Contact HP** to find locations and telephone numbers.

Helpful web sites

For other product information, see the following HP web sites:

- http://www.hp.com
- http://www.hp.com/go/storage
- http://www.hp.com/support/
- http://www.docs.hp.com
- http://h71028.www7.hp.com/enterprise/cache/80316-0-0-0-121.html

1 Using McDATA Web Server/Element Manager

This section describes how to use the McDATA Web Server and Element Manager applications and their menus. McDATA Web Server is a graphical user interface that provides both fabric and switch module management functions. Because McDATA Web Server resides in the switch firmware, no installation is needed. You can run one instance of the McDATA Web Server at a time by opening the switch IP address with an internet browser. McDATA Web Server is best used to manage a single fabric consisting only of McDATA 4Gb SAN switches.

Element Manager is a graphical user interface for managing a single McDATA 4Gb SAN Switch through either the High Availability Fabric Manager (HAFM) or the Enterprise Fabric Connectivity Manager (EFCM) application. HAFM, EFCM and Element Manager are essential tools for managing multiple fabrics or a single fabric consisting of McDATA 4Gb SAN switches, HP StorageWorks M-Series switches, or McDATA switches. References to HAFM in this document also apply to EFCM.

IMPORTANT: Element Manager is available only with the Element Manager Product Features Enablement (PFE) key. See "Installing Product Feature Enablement keys" on page 82 for information about installing a PFE key. To obtain the McDATA 4Gb SAN Switch serial number and PFE key, follow the step-by-step instructions on the *firmware feature entitlement request certificate* for the PFE key. You can obtain a PFE key from the web at: www.webkey.external.hp.com.

NOTE: Unless stated otherwise, the features described in this document apply to McDATA Web Server and Element Manager

The following topics are covered:

Workstation requirements

The requirements for fabric management workstations running the McDATA Web Server web applet are listed in Table 2.

Table 2 Workstation requirements

Operating System	Microsoft® Windows Server 2000, Windows Server 2003 SP1, Windows XP®
	Red Hat® Enterprise Linux® 3 and 4
Memory	256 MB or more
Processor	500 MHz or faster
Hardware	RJ-45 Ethernet port,
Internet Browser	Microsoft Internet Explorer® 5.0 and later Netscape® Navigator® 6.0 and later Mozilla™ 1.5 or later Mozilla Firefox® 1.0.7 or later Java 2 Runtime Environment to support the McDATA Web Server

Starting McDATA Web Server

To start McDATA Web Server after the switch is operational, enter the switch IP address in an internet browser. The workstation used to manage the switch must be able to connect to the default switch IP address 10.0.0.1.

1. At the workstation, enter the default switch IP address (10.0.0.1) in an internet browser. If your workstation does not have the Java 2 Run Time Environment program, you will be prompted to download it.
2. Enter the login name (default is `admin`) and password (default is `password`) in the Add a New Fabric dialog.
3. Click **Add Fabric**. If you do not have a secure Ethernet connection, the Non Secure Connection Check dialog will prompt you to establish a non-secure connection.
4. The Password Change Required dialog prompts you to change the default password. Click the **OK** button. This dialog will prompt you to change the default password each time you log in until you change it. See "Managing user accounts" on page 49 for information about changing the password.
5. Select **Switch > Network Properties**.
6. Change the **IP Address**, **Subnet Mask**, and **Gateway** settings to reflect your desired network configuration in the Network Properties dialog.
7. Click **OK**.
8. Close the browser window to close the McDATA Web Server application. The switch is now ready to be managed through your network.
9. Repeat steps 1—4 using the switch's newly configured IP address to launch the McDATA Web Server application once your configured switch is connected to the network.

Starting Element Manager in HAFM

To use Element Manager, the HAFM client application must be running on your workstation, or you must be accessing HAFM on the HAFM Appliance. See your HAFM documentation for information about starting and using HAFM. To start Element Manager in HAFM, add the switch IP address to the discovery list. Locate and double click the switch in the fabric map to open. You can also select the switch and select **Element Manager** from the application list. HAFM displays the Element Manager window shown in Figure 1.
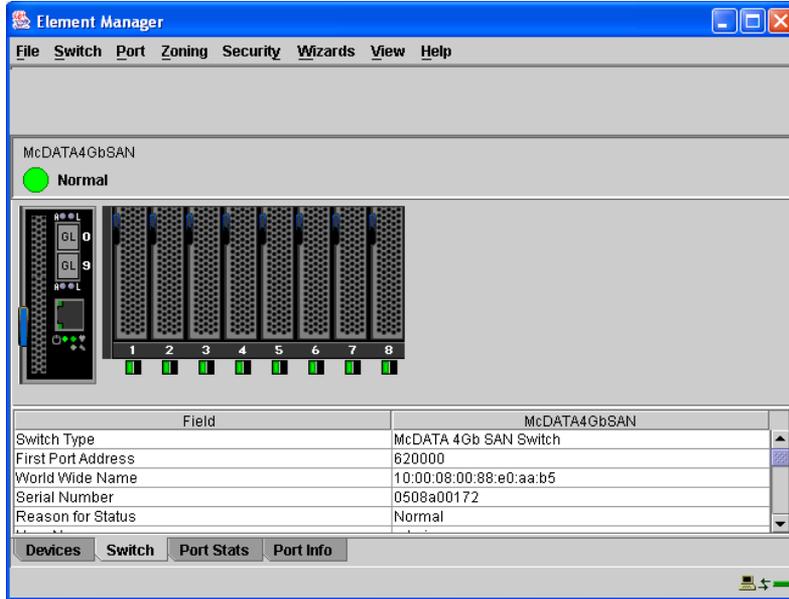
Figure 1 Element Manager window

Exiting McDATA Web Server or Element Manager

To exit a McDATA Web Server session, close the browser window. To exit a Element Manager session, select **File > Exit.**

Setting preferences

You can customize the following preference settings for McDATA Web Server and Element Manager:

- Change the location of the working directory in which to save files.
- Change the location of the browser used to view the online help.
- 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 "Displaying the event browser" on page 31. If the Event Browser is enabled using the Preferences dialog as shown in Figure 2, the next time McDATA Web Server is started, all events will be displayed. If the Event Browser is disabled when McDATA Web Server 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, page 93
  - Port states, page 92
  - Port speeds, page 94
  - Port transceiver media status, page 94
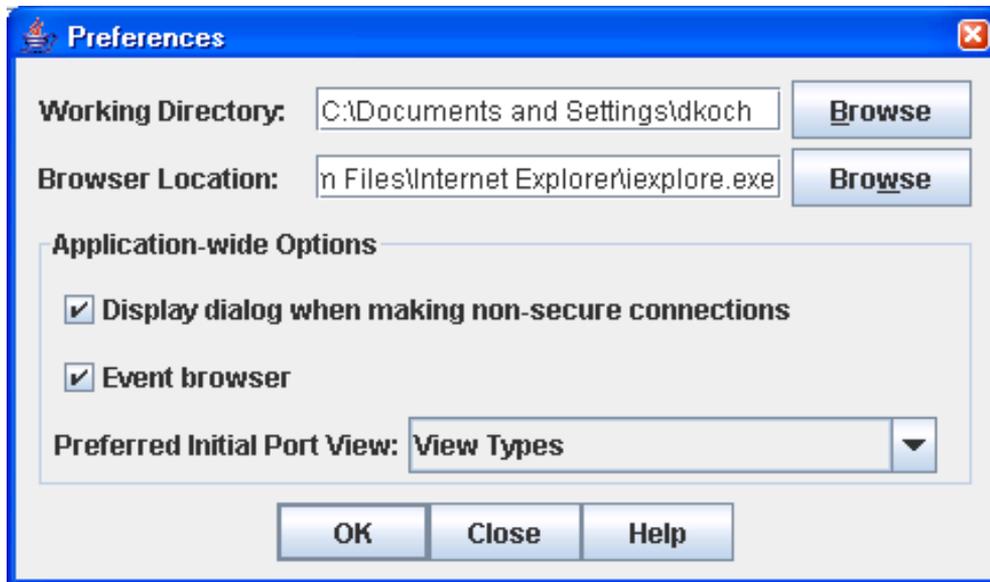
Figure 2 Preferences dialog

To set preferences:

1. Select **File > Preferences** to open the Preferences dialog.
2. Enter or browse for paths to the working directory and browser.
3. Choose the preferences you want in the Application-wide Options area.
4. Click **OK** to save the changes.

Using online help

Online help is available for the McDATA Web Server and Element Manager applications and their functions. Online help is also context-sensitive, that is, the online help opens to the topic that describes the dialog you have open. To open online help, choose one of the following:

- Select **Help > Help Topics.**
- Click **Help** in dialogs to display context-sensitive help in dialogs.
- Press the **F1** function key

Viewing software version and copyright information

Select **Help > About** to view software version and copyright information.

Enabling call home

The call-home feature enables the server platform to automatically connect with a support center to report system problems. The support center server accepts calls from the server platform, logs reported events, and notifies one or more support center representatives. The default state is disabled. To configure telephone numbers and other information for the call-home feature, see your HAFM Manual for details.

You must enable call-home event notification through HAFM before enabling this function through the Element Manager for the individual switch. At the bottom of HAFM desktop window is an icon that indicates whether the call-home feature is enabled. An X over the phone icon indicates that the call-home feature is disabled.

To enable call-home support for system problems using Element Manager:

1. Select **File > HAFM Settings**.
2. Select **Call Home Support** in the pull-down menu to mark the check box. To disable call home support, select the option to remove the check mark from the check box.

Enabling e-mail support

The e-mail support function on the Element Manager enables e-mail notification for events that occur on a selected switch. The default state is disabled. e-mail addresses and the simple mail transfer protocol (SMTP) server address for e-mail notification of director events must be configured through HAFM. See your HAFM Manual for instructions on configuring e-mail.

NOTE: e-mail recipients are configured in HAFM through the Email Event Notification Setup dialog box. A valid SMTP address is configured in this dialog box.

To enable e-mail support using Element Manager:

1. Select **File > HAFM Settings**.
2. Select **Email Support** in the pull-down menu to mark the check box. To disable e-mail support, select the option to remove the check mark from the check box.

User interface

The McDATA Web Server and Element Manager applications share a common interface as shown in Figure 3. The interface consists of a menu bar, fabric tree, graphic window, data windows (some with buttons), and data window tabs. The switch faceplate is displayed in the graphic window and shows the front of a single switch and its ports. 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 Element Manager application uses a modified faceplate display with fewer menus, no fabric tree, and fewer data window tabs.
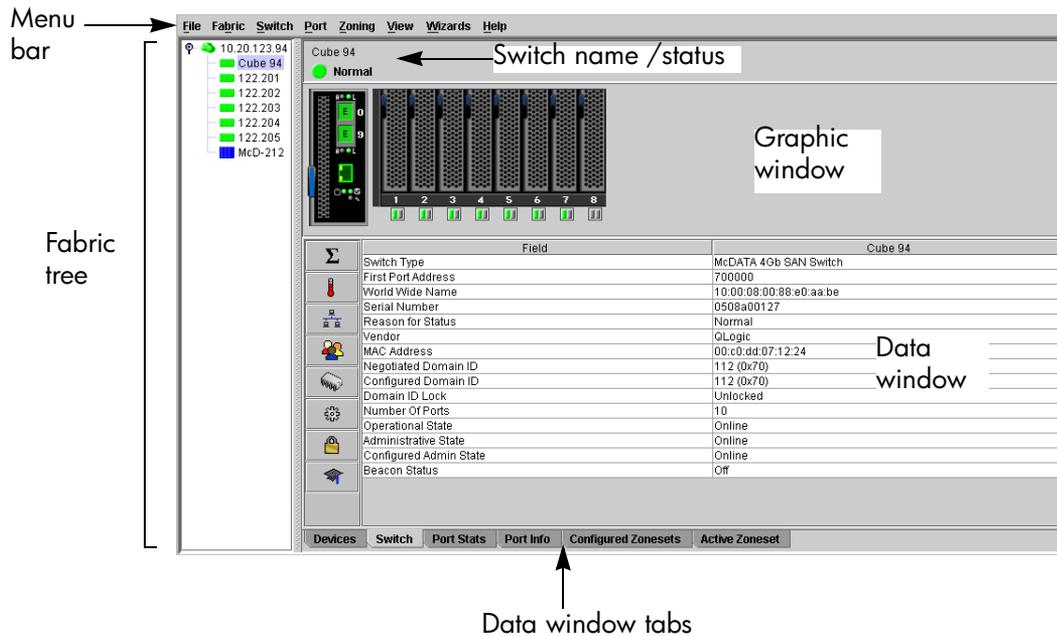
Figure 3 McDATA Web Server interface

Menu bar

The McDATA Web Server and Element Manager menu bar options are listed in Table 3.

Table 3 Menu Bar Options

Menu	McDATA Web Server Options	Element Manager Options
File	Preferences	Preferences HAFM Settings Exit
Fabric	Nicknames Rediscover Fabric Show Event Browser	Not applicable
Switch	Archive Restore User Accounts Set Date/Time Switch Properties Advanced Switch Properties Services Network Properties SNMP Properties Toggle Beacon Load Firmware Reset Switch Restore Factory Defaults Features Radius Servers[1] Download Support File	Archive Restore User Accounts Set Date/Time Switch Properties Advanced Switch Properties Services Switch Binding Security Consistency Checklist Network Properties SNMP Properties Toggle Beacon Port Threshold Alarm Configuration Load Firmware Reset Switch Restore Factory Defaults Features Radius Servers[1] Download Support File
Port	Port Properties Advanced Port Properties Reset Port Port Diagnostics	Port Properties Advanced Port Properties Reset Port Port Binding Port Diagnostics
Zoning	Edit Zoning Edit Zoning Config Activate Zone Set Deactivate Zone Set Restore Default Zoning	Edit Zoning Config
Security[1]	Not applicable	Edit Security Edit Security Config Activate Security Set Deactivate Security Set
View	Refresh View Port Types View Port States View Port Speeds View Port Media	Refresh Show Event Browser View Port Types View Port States View Port Speeds View Port Media

Table 3 Menu Bar Options (Continued)

Menu	McDATA Web Server Options	Element Manager Options
Wizards	Configuration Wizard	Same as McDATA Web Server
Help	Help Topics About	Same as McDATA Web Server

1. Requires SANtegrity PFE key and Secure Sockets Layer (SSL) enabled. See System services, page 73.

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 following common tasks and dialogs:

- Refreshing a switch
- Selecting all ports or blades
- Properties dialogs (Port, Blade, Switch, Network, and SNMP)
- Services dialog
- Diagnostics dialogs (Port and Blade)

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**, then press **R**. The shortcut key combinations are not case-sensitive.

McDATA Web Server Fabric tree

McDATA Web Server enables you to manage McDATA 4Gb SAN Switches and observe other switches in the fabric. The fabric tree, shown in Figure 4, provides access to the faceplate display of each McDATA 4Gb SAN Switch in the fabric, and displays the presence of other switches in the fabric. Click a switch name or icon of a McDATA 4Gb SAN Switch to display that switch faceplate in the graphic window. The window width of the fabric tree can be adjusted by clicking and dragging the moveable 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 through the McDATA 4Gb SAN Switch.

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.
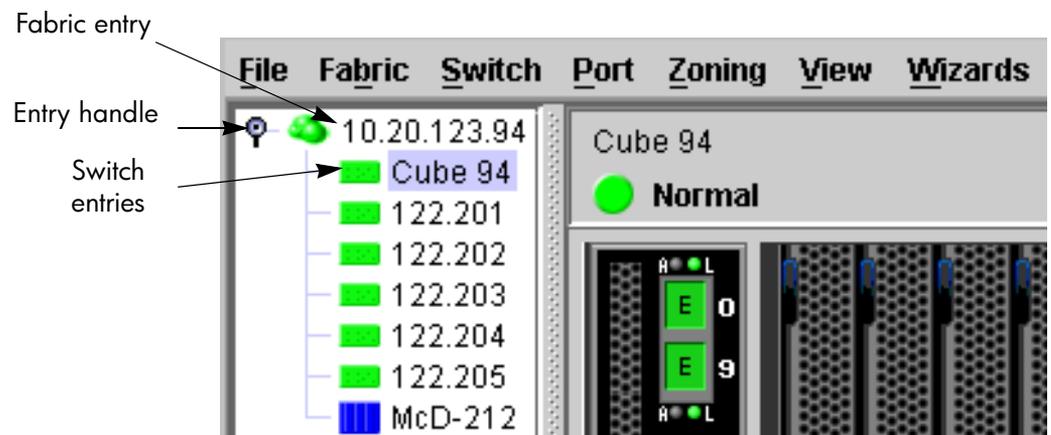
Figure 4 McDATA Web Server fabric tree

Graphic window

The graphic window shows the switch faceplate display. The window height can be adjusted by clicking and dragging the window border that it shares with the data window.

Data windows and tabs

The data window 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.

Click on the following tabs to open the corresponding data window:

- **Devices**—Displays information about devices (hosts and storage targets) connected to the switch. See "Devices data window" on page 34 for more information.
- **Switch**—Displays current network and switch configuration data for the selected switches. See "Switch status and operational information" on page 60 for more information.
- **Port Statistics**—Displays performance data for the selected ports. See "Port statistics data window" on page 88 for more information.
- **Port Information**—Displays information for the selected ports. See "Port statistics data window" on page 88 for more information.
- **Configured Zonesets**—Displays all zone sets, zones, and zone membership in the zoning database. This data window is available in McDATA Web Server only. See "McDATA Web Server Configured Zonesets data window" on page 64.
- **Active Zoneset**—Displays the active zone set for the fabric including zones and their member ports. This data window is available only in McDATA Web Server. See "Displaying the configured and active zone sets" on page 44 for more information about this data window. See "Zoning concepts" on page 37 for information about zone sets and zones.
- **Configured Security**—Displays all security definitions currently saved in the database (Element Manager only).
- • **Active Security**—Displays the active security set (Element Manager only).

Selecting switches

Switches are selectable in the fabric tree (McDATA Web Server only). Click a McDATA 4Gb SAN Switch to display its faceplate display in the graphic window. See "Managing switches" on page 49 for detailed switch information.

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 "Managing ports" on page 85 for detailed port information.

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

- To select a port, click the port.
- To select all ports, right-click on the faceplate image and select **Select All Ports** from the popup menu.
- To un-select all ports, click the faceplate anywhere away from a port.
- To un-select a particular port, hold down the **Control** key while clicking each port.

2 Managing Fabrics

This section describes the following tasks that manage fabrics using McDATA Web Server:

Securing a fabric

Fabric security consists of the following:

Security consistency checklist

IMPORTANT: The security consistency checklist is available only with Element Manager, which requires the Element Manager PFE key. See "Installing Product Feature Enablement keys" on page 82 for more information about installing a PFE key. To obtain the McDATA 4Gb SAN Switch serial number and PFE key, follow the step-by-step instructions on the *firmware feature entitlement request certificate* for the PFE key. You can obtain a PFE key from the web at: www.webkey.external.hp.com.

The Security Consistency Checklist dialog enables you to compare security-related features on switches to check for inconsistencies. Any changes must be made through the appropriate dialog, such as Network Properties dialog, Switch Properties dialog, or SNMP Properties dialog. Select **Switch > Security Consistency Checklist** to open the Security Consistency Checklist dialog.

Connection security

📝 **IMPORTANT:** The SSL and SSH services can be managed only with Element Manager, which requires the Element Manager PFE key, and the CLI. See "Installing Product Feature Enablement keys" on page 82 for more information about installing a PFE key. To obtain the McDATA 4Gb SAN Switch serial number and PFE key, follow the step-by-step instructions on the *firmware feature entitlement request certificate* for the PFE key. You can obtain a PFE key from the web at: www.webkey.external.hp.com.

Connection security provides an encrypted data path for switch management methods. The switch supports the Secure Shell (SSH) protocol for the CLI and the Secure Socket Layer (SSL) protocol for management applications such as McDATA Web Server, Element Manager, and Common Information Module (CIM). See "System services" on page 73 for information about enabling the SSH and SSL services.

The SSL handshake process between the workstation and the switch involves the exchanging of certificates. These certificates contain the public and private keys that define the encryption. The switch certificate is valid for one year beginning with its creation date and time. The workstation validates the switch certificate by comparing the workstation date and time to the switch certificate creation date and time. For this reason, it is important to synchronize the workstation and switch with the same date, time, and time zone. If a certificate has not been created by the user, the switch will automatically create one. If SSL connection security is required, also consider using the Network Time Protocol (NTP) service to synchronize date/time between workstations and switches.

User account security

User account security is the process by which your user account and password are authenticated with the list of valid user accounts and passwords. The switch validates your account and password when you attempt to add a fabric using McDATA Web Server or log in to a switch through Telnet. Your system administrator defines accounts, passwords, and authority levels that are stored on the switch. See "Managing user accounts" on page 49 for more information.

The Admin account possesses Admin authority which grants full access to all tasks of the McDATA Web Server menu system. The switch validates your user account and McDATA Web Server grants access to its menus according to your authority level. If you do not have Admin authority, you are limited to monitoring tasks.

📝 **NOTE:** If a user is logged into a switch using McDATA Web Server or CLI, and an administrator changes user access rights and passwords, existing login sessions will not be affected by the new settings. Login access and privileges are only checked for a new login request.

Remote authentication

📝 **IMPORTANT:** Remote authentication is available only with the McDATA SANtegrity Enhanced PFE key and can be managed only with the CLI and Element Manager. Element Manager also requires a PFE key. See "Installing Product Feature Enablement keys" on page 82 for more information about installing a PFE key. To obtain the McDATA 4Gb SAN Switch serial number and PFE key, follow the step-by-step instructions on the *firmware feature entitlement request certificate* for the PFE key. You can obtain a PFE key from the web at: www.webkey.external.hp.com.

Remote Authentication Dial In User Service (RADIUS) provides a method to centralize the management of authentication passwords in larger networks. It has a client/server model, where the server is the password repository and third party authentication point and the clients are all of the managed devices. RADIUS can be configured for devices and/or user accounts. See "Configuring RADIUS servers" on page 54 for information about configuring RADIUS servers.

The RADIUS server dialogs are available only on a secure fabric and on the entry switch (out-of-band switch). Refer "System services" on page 73 for information about enabling the SSL service.

Device security

> **IMPORTANT:** Device security is available only with the McDATA SANtegrity™ Enhanced PFE key and can be managed only with the CLI and Element Manager. Element Manager also requires a PFE key. See "Installing Product Feature Enablement keys" on page 82 for more information about installing a PFE key. To obtain the McDATA 4Gb SAN Switch serial number and PFE key, follow the step-by-step instructions on the *firmware feature entitlement request certificate* for the PFE key. You can obtain a PFE key from the web at: www.webkey.external.hp.com.

Device security provides for the authorization and authentication of devices that you attach to a switch. You can configure a switch with a group of devices against which the switch authorizes new attachments by devices, other switches, or devices issuing management server commands. Device security is configured through the use of security sets and groups. A group is a list of device worldwide names that are authorized to attach to a switch. There are three types of groups: one for other switches (ISL), another for devices (port), and a third for devices issuing management server commands (MS). A security set is a set of up to three groups with no more than one of each group type. The security configuration is made up of all security sets on the switch.

In addition to authorization, the switch can be configured to require authentication to validate the identity of the connecting switch, device, or host. Authentication can be performed locally using the switch security database, or remotely using a RADIUS server. With a RADIUS server, the security database for the entire fabric resides on the server. In this way, the security database can be managed centrally, rather than on each switch. You can configure up to five RADIUS servers to provide failover.

You can configure the RADIUS server to authenticate just the switch or both the switch and the initiator device if the device supports authentication. When using a RADIUS server, every switch in the fabric must have a network connection. A RADIUS server can also be configured to authenticate user accounts.

Managing device security involves the following tasks:

- Creating security sets, groups, and members
- Editing a security configuration on a switch
- Viewing properties of a security set, group, or member
- Archiving a security configuration on a switch to a file
- Activating and deactivating a security set

The security database is made up of all security sets on the switch. The security database has the following limits:

- Maximum number of security sets is 4.
- Maximum number of security groups is 16.
- Maximum number of members in a group is 1000.
- Maximum total number of group members is 1000.

Edit Security dialog

Use the Edit Security dialog to edit the security configuration on the switch. You can also open and edit a security configuration saved to a file. Editing security files consists of renaming and removing security sets, groups, and members. The Security dialogs are available only on a secure SSL fabric and on the entry switch (out-of-band switch).

To open the Edit Security dialog shown in Figure 5, choose one of the following:

- Click **Security** in the tool bar.
- Select **Security > Edit Security**.

📝 **NOTE:** The Security menu and button are only displayed if SSL is enabled. Select **Switch > Services > SSL** to enable SSL. See "System services" on page 73 for more information.

Use the Edit menu options or popup menu options to access Edit Security dialog options. Select a security item in the graphic window and select an option in the Edit menu, or right-click on a security item in the graphic window, and select an option from the popup menus.

The orphan security set contains the security groups and members that don't belong to a user-defined security set. Excluding the orphan security set, you can only have 1 group type in a security set. The three types of security groups are:

- ISL—Default (E_Port authentication)
- MS (Management Server CT authentication)
- Port (F_Port authentication)
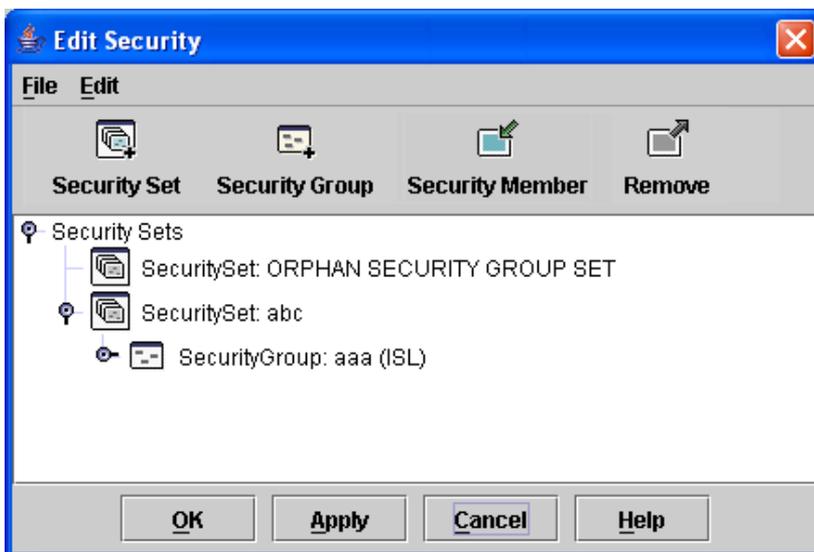
Figure 5 Edit Security dialog

Use the File menu in the Edit Security dialog to:

- Edit the security configuration on the switch.
- Open or edit security files.
- Save or rename security files

Use the Edit menu in the Edit Security dialog to:

- Create security sets, security groups, and security group members.
- Rename or remove a security group from a security set or a member from a security group.
- Remove a group from all security sets.
- Remove all security sets, groups, or members.
- View properties for the selected security set, group, or group member.

Create Security Set dialog

Use the Create Security Set dialog shown in Figure 6 to create a new security set. There is a maximum of 4 security sets.

Figure 6 Create Security Set dialog

To add a security set from the faceplate display:

1. Click **Security** on the tool bar, or select **Security > Edit Security** to open the Edit Security dialog.
2. To open the Create a Security Set dialog, choose one of the following:
   - Click **Security Set** in the Edit Security dialog tool bar.
   - Right-click in the graphic window of the Edit Security dialog, and select **New Security Set** from the popup menu.
3. Enter a name for the new security set. The naming conventions for security sets are:
   - Must start with a letter.
   - All alphanumeric chars [aA—zZ] [0—9].
   - The symbols $_ - and ^ are the only symbols allowed.
4. Click **OK** to save the change.

Create Security Group dialog

Use the Create Security Group dialog, shown in Figure 7, to add a security group to a security set. To open the Create a Security Group dialog, choose one of the following:

   - Click **Security Group** in the Edit Security dialog tool bar.
   - Right-click in the graphic window of the Edit Security dialog, and select **Create a Security Group** from the popup menu.

Figure 7 Create Security Group dialog

The naming conventions for all security groups are listed below.

- Must start with a letter
- All alphanumeric chars [aA—zZ] [0—9]
- The symbols $_ - and ^ are the only symbols allowed.

An empty (no members) security group in the active security set will prevent all connections for that security group type. For example, an empty ISL security group will cause the switch to refuse all logins from other switches. To add a security group to a security set:

1. Click **Security** on the tool bar in the faceplate display or select **Security > Edit Security** to open the Edit Security dialog.
2. Choose one of the following methods to open the Create a Security Group dialog:
   - Click a security set and click **Security Group** in the tool bar in the graphic window.
   - Right-click on a security set and select **Create a Security Group** from the popup menu.
3. Enter a security group name and select a security group type (**ISL**, **Port**, or **MS**). Remember, only one security group type (1 ISL, 1 Port, 1 MS) in each security set is allowed. The naming conventions for security groups are:
   - Must start with a letter
   - All alphanumeric chars [aA—zZ] [0—9]
   - The symbols $_ - and ^ are the only symbols allowed.
4. Click **OK** to save the change.

Create Security Group Member dialog

Use the Create Security Group Member dialog, shown in Figure 8, to add a member to a security group. Choose options from the Group Member (or manually enter a hex value) and **Authentication** drop-down lists, and enter values in the **Secret** and **Binding** (ISL groups only) fields.

Figure 8 Create a Security Group Member dialog

The conventions for ISL security group members are listed below:

- You can enter member World Wide Name (WWN), which must be 16 hex characters, or 23 characters with valid WWN format xx:xx:xx:xx:xx:xx:xx:xx.
- The authentication choices are None and CHAP (Challenge Handshake Authentication Protocol).
- The **Secret** field is disabled if authentication is set to None. If authentication is CHAP, the **Secret** field is enabled. The secondary hash and secret are not supported when connecting to other McDATA products.
- **Generate** is only enabled when authentication is set to CHAP.
- Valid binding entries are 97–127.

The conventions for Port security group members are listed below:

- You can enter member World Wide Name (WWN), which must be 16 hex characters, or 23 characters with valid WWN format xx:xx:xx:xx:xx:xx:xx:xx.
- The authentication choices are None and CHAP.
- The **Secret** field is disabled if authentication is set to None. If authentication is CHAP, the **Secret** field is enabled. The secondary hash and secret are not supported when connecting to other McDATA products.
- **Generate** is only enabled when authentication is set to CHAP.

The conventions for MS security group members are listed below:

- You can enter member World Wide Name (WWN), which must be 16 hex characters, or 23 characters with valid WWN format xx:xx:xx:xx:xx:xx:xx:xx.
- The CT (common transport) authentication choices are None, MD5, and SHA-1.
- The **Secret** field is disabled if authentication is set to None, otherwise the **Secret** field enabled.
- **Generate** is only enabled when authentication is CHAP.
- Secret is 16 byte length for MD5 authentication, and 20 bytes if authentication is SHA-1.

To add a member to a security group:

1. Choose one of the following to open the Edit Security dialog from the faceplate display:
   - Click **Security** on the tool bar.
   - Select **Security > Edit Security**.
2. Choose one of the following to open the Create a Security Group Member dialog:
   - Click a security group in the graphic window of the Edit Security dialog. Click **Security Member** in the tool bar.
   - Right-click on a security group in the graphic window of the Edit Security dialog. Select **Create Members** from the popup menu.
3. Open the **Group Member** drop-down list and select a Node World Wide Name. The switch must be a member of any group in which authentication is used. You can also enter a hex value.
4. Open the **Authentication** drop-down list, and select a type of protocol to be used for the authentication process for that member.
   - ISL authentication options are **None** (0 bytes), **CHAP** (16 bytes)
   - MS (CT—Common Transport) authentication options are **None** (0 bytes), **MD5** (16 bytes), **SHA** (20 bytes)
   - Port authentication options are **None** (0 bytes), **CHAP** (16 bytes)
5. Enter an authentication password to be assigned that member in the Secret area. Or, click **Generate** to randomly generate a secret.
6. Enter the domain ID (97–127) for the switch for the ISL group member in the **Binding** field (ISL groups only). The WWN of the switch must be at the entered domain ID when attempting to enter the fabric, otherwise it will become isolated.
7. Click **OK** to save the changes.

Editing the security configuration on a switch

To edit a security configuration on the switch from the faceplate display:

1. Choose one of the following to open the Edit Security dialog:
   - Click **Security** on the tool bar.
   - Select **Security > Edit Security**.

   By default, the security configuration on the switch is displayed in the Edit Security dialog.
2. Choose one of the following from the Edit Security dialog:
   - Select **File > Open File**. Browse for and select the security file.
   - Press **Control+O** (letter o). Browse for and select the security file.
3. Click **Open** to display the security file in the Edit Security dialog.
4. Select the security item to edit in the graphic window, and choose one of the following:
   - **Rename a security set, or group**. Select a rename option from the Edit menu. Enter a new name in the Rename dialog. Click **OK** to save the changes.
   - **Edit security group member.** Select an **Edit Security Group Member** option from the Edit menu. Enter a new Group Member (WWN) in the Edit Security Group Member dialog. Choose an option in the **Authentication** drop-down list. Click **OK** to save the changes.
   - **Remove a security set, group, or member**. Select the item to remove, and select a remove option from the Edit menu. Click **OK** in the Remove dialog to remove that item from the security file and save the changes.
   - **Clear security**. Select the Security Sets directory name. Select **Edit > Clear Security**. Click **OK** in the Remove dialog to remove all security sets and save the changes. You can also right-click on the Security Sets (top level) directory name, select **Clear Security** from the popup menu, and click **OK** to remove all security sets.
5. To save the changes, choose one of the following:
   - Click **Apply** to save the changes and keep the Edit Security dialog open. Click **OK** to close the Edit Security dialog.
   - Click **OK** to save changes and close the Edit Security dialog.

Viewing properties of a security set, group, or member

To view the properties of a security set, group, or member from the faceplate display:

1. Click **Security** on the tool bar, or select **Security > Edit Security** to open the Edit Security dialog.
2. Choose one of the following:
   - Click a security set, security group, or security group member. Select **Edit > Properties**.
   - Right-click on a security item In the graphic window. Select **Properties** from the popup menu.
3. View the security information for the selected item in the Properties dialog.
4. Click **OK** to close the dialog.

Security Config dialog

Use the Security Config dialog, shown in Figure 9, to save the active security configuration on the switch to non-volatile or to temporary memory, and to require the domain ID of a switch be validated before attaching to the fabric.
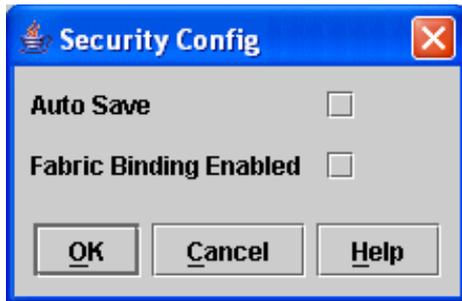
Figure 9 Security Config dialog

To configure switch security from the faceplate display:

1. Select **Security > Edit Security Config** to open the Security Config dialog.
2. Select the **Auto Save** option to enable (default) or disable Auto Save mode.

   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. If the local switch is reset, it may isolate.
3. Select the **Fabric Binding Enabled** option to require the expected domain ID of a switch to be verified before being allowed to attach to the fabric.

> 📝 **NOTE:** The fabric binding feature must be enabled on all switches in the fabric. When enabling this feature, it is best to set the switch state to offline, enable the fabric binding feature on all switches, and then set the switch state to online.

4. Click **OK** to save the settings and close the Security Config dialog.

Archiving a security configuration to a file

To archive (save) a security configuration to a file from the faceplate display:

1. Click **Security** on the tool bar, or select **Security > Edit Security** to open the Edit Security dialog.
2. Make desired changes to the security settings using the security dialogs.
3. Select **File > Save As**.
4. Enter a name and location for the security file (.xml extension) in the Save dialog.
5. Click **Save** to save the security file.

Activating a security set

Only one security set can be active at one time. To activate a security set from the faceplate display:

1. Select **Security > Activate Security Set** to open the Activate Security Set dialog.
2. Select a security set from the drop-down list.
3. Click **Activate** to activate the security set.

Deactivating a security set

Only one security set can be active at one time. To deactivate an active security set from the faceplate display:

1. Select **Security > Deactivate Security Set**.
2. Select a security set from the drop-down list in the Deactivate Security Set dialog.
3. Click **Yes** to confirm that you want to deactivate the active security set in the Deactivate Security Set dialog.

Configured Security data window

The Configured Security data window displays a graphical representation of all security sets, security groups, and security group members in the database. Click the **Configured Security** data window tab in the faceplate display to open the Configured Security data window.

Active Security data window

The Active Security data window displays a graphical representation of the active security set, its groups, and members in the database. Click the **Active Security** data window tab in the faceplate display to open the Active Security data window.

Fabric services

Fabric services security includes 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, that are basically 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 using the System Services or SNMP Properties dialogs. 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. See "Enabling SNMP configuration" on page 30 for more information. SNMP is enabled by default.

In-band management is the ability to manage switches across Inter-switch Links (ISL) using McDATA Web Server, 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 an Ethernet connection. See "Enabling in-band management" on page 30 for more information.

Enabling SNMP configuration

To enable SNMP configuration from the faceplate display:

1. Select **Switch > SNMP Properties** to open the SNMP Properties dialog.
2. Select the **SNMP Enabled** option in the SNMP Configuration area.
3. Click **OK** to save the change to the database.

Enabling in-band management

To enable in-band management from the faceplate display:

1. Select **Switch > Switch Properties** to open the Switch Properties dialog.
2. Select the **In-band Management Enable** option.
3. Click **OK** 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 again view the actual fabric configuration. The **Rediscover Fabric** option clears out the current fabric information being displayed, and rediscovers all switch information. Select **Fabric > Rediscover Fabric** to rediscover a fabric. The rediscover function is more comprehensive than the refresh function.

Displaying the event browser

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

To display the Event Browser in McDATA Web Server, choose one of the following:

- Select **Fabric > Show Event Browser**.
- Click **Events** on the tool bar.

To display the Event Browser in Element Manager, select **View > Show Event Browser**.

Entries in the Event Browser shown in Figure 10, 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 McDATA Web Server is running.

📝 **NOTE:** If the Event Browser is enabled using the Preferences dialog, the next time McDATA Web Server is started all events from the switch log will be displayed. If the Event Browser is disabled when McDATA Web Server is started and later enabled, only those events from the time the Event Browser was enabled and forward will be displayed. See "Setting preferences" on page 14 for more information.
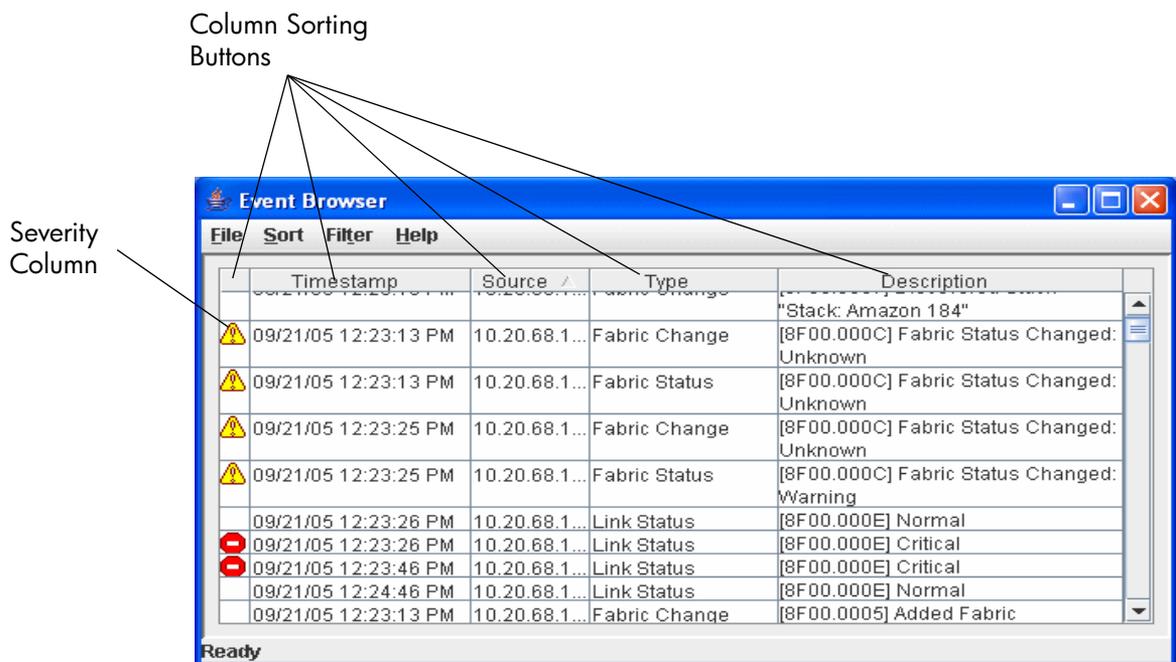
Figure 10 Events browser

Severity is indicated in the severity column using icons as described in Table 4.

Table 4 Severity levels

Severity Icon	Description
	Alarm — an alarm is a serviceable event. This 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 support file for 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.
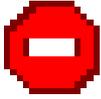
NOTE: Events (Alarms, Critical, Warning, and Informative) generated by the web applet are not saved on the switch. They are permanently discarded when you close a McDATA Web Server session, but you can save these events to a file on the workstation before you close McDATA Web Server and read it later with a text editor or browser.

Events generated by the switch are stored on the switch, and will be retrieved when the application is restarted.

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. Successive sort operations of the same type alternate between ascending and descending order. To sort the Event Browser, choose one of the following:

- Click the **Severity**, **Timestamp**, **Source**, **Type**, or **Description** columns.
- Select **Sort > By Severity**, **By Timestamp**, **By Source**, **By Type**, or **By Description**.

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 opens the Filter Events dialog shown in Figure 11. 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:ss 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 2 or 4 digits. For example, 12/12/03 will be interpreted December 12, 2003.
- **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.
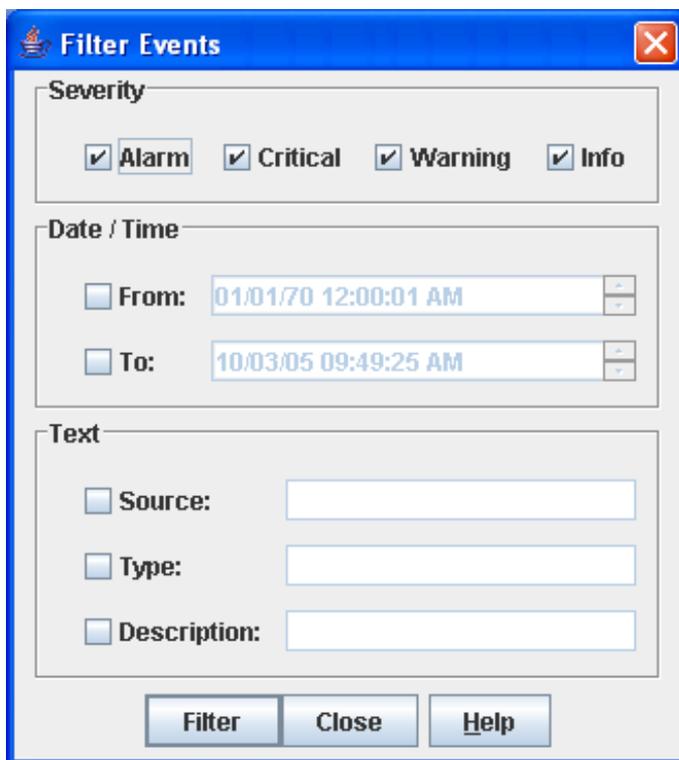
Figure 11 Filter events dialog

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:

1. Filter and sort the Event Browser to obtain the desired display. See "Sorting the event browser" on page 32 and "Filtering the event browser" on page 33 for more information.
2. Select **File > Save As**.
3. Select a pathname to which to save the event log and click **Save**. 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.

Working with 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, page 34
- Displaying detailed device information, page 35
- Managing device port nicknames, page 35

Devices data window

The Devices data window shown in Figure 12 displays information about devices connected to the switch. To display the Devices data window, click the **Devices** tab below the data window.
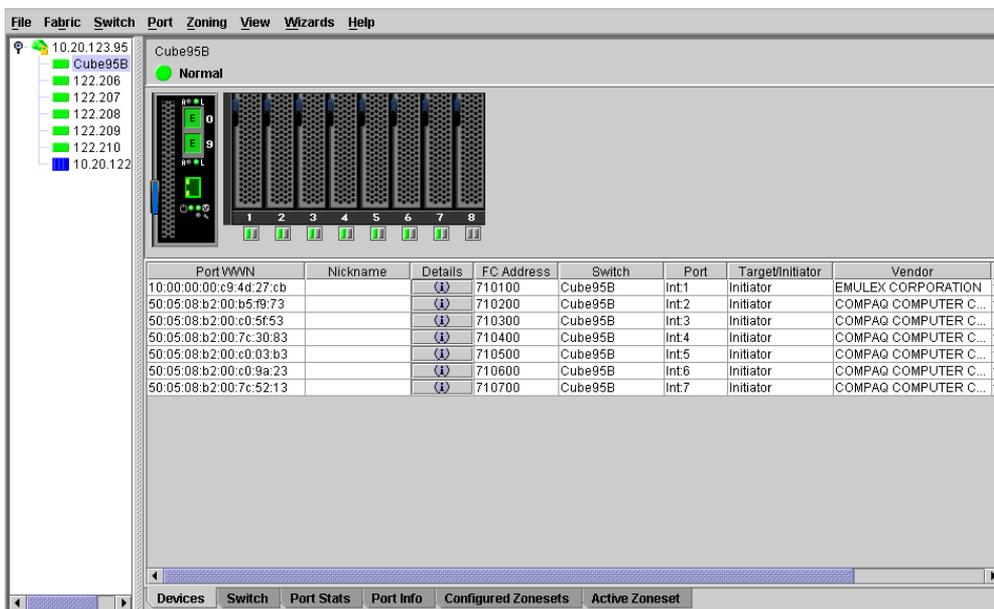
Figure 12 Devices data window

Table 5 describes the entries in the Devices data window.

Table 5 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. See "Managing device port nicknames" on page 35 for more information.
Details	Click the **(i)** to display additional information about the device. See "Displaying detailed device information" on page 35.
FC Address	Fibre Channel address
Switch	Switch name
Port	Switch port number
Target/Initiator	Device type: target or initiator
Vendor	HBA/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 display more information as shown in Figure 13.
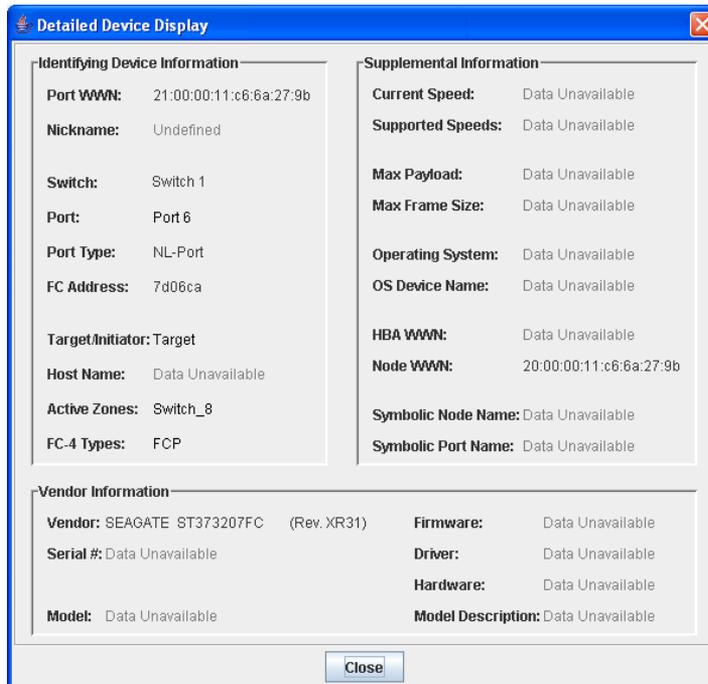
Managing device port nicknames

Using McDATA Web Server, 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 that 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 McDATA 4Gb SAN 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 McDATA 4Gb SAN Switches in the fabric after you click the **Apply** button.

📝 **NOTE:** Nicknames are stored on each switch and are not compatible with nickname files from switches with 5.x firmware.

McDATA Web Server manages nicknames separately from HAFM. This means that HAFM cannot reference nicknames created by McDATA Web Server; neither can McDATA Web Server reference nicknames created by HAFM. However, HAFM does share nicknames with Element Manager.

Creating a nickname

To create a device port nickname:

1. Select **Fabric >Nicknames** to open the Nicknames dialog.
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 on a device in the table. Select **Edit > Create Nickname** to open the Add Nickname dialog. Enter a nickname and WWN and click **OK**.
3. Click **Apply** to save the changes and exit the Nicknames dialog.
4. In the Save Nicknames dialog, click **Save**, then click **Close**.

Editing a nickname

to edit a device port nickname:

1. Select **Fabric >Nicknames** to open the Nicknames dialog.
2. Choose one of the following methods to edit 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 edit the nickname in the text field.
   - Click on a device in the table. Select **Edit > Edit Nickname** to open the Edit Nickname dialog. In the Edit Nickname dialog, edit the nickname and click **OK**.
3. Click **Apply** to save the changes and exit the Nicknames dialog.
4. In the Save Nicknames dialog, click **Save**, then click **Close**.

Deleting a nickname

To delete a device port nickname:

1. Select **Fabric >Nicknames** to open the Nicknames dialog.
2. Choose one of the following methods:
   - Double-click a cell in the **Nicknames** column, and delete the nickname text.
   - Click a device in the table. Select **Edit > Delete Nickname**.
3. Click **Apply** to save the changes and exit the Nicknames dialog.
4. In the Save Nicknames dialog, click **Save**, then click **Close**.

Exporting nicknames to a file

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

1. Select **Fabric >Nicknames** to open the Nicknames dialog.
2. Select **File > 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 that is used by McDATA Web Server. To import a nickname file:

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

Zoning a fabric

If HAFM is used to manage the fabric, it is recommended to use HAFM to manage the fabric zoning. If HAFM is not used and other McDATA switch models are in the fabric, it is recommended to use HAFM Basic or EFCM Basic, or in earlier firmware versions, SANpilot or Embedded Web Server to manage the fabric zoning. If all switches in the fabric are McDATA 4Gb SAN switches, use McDATA Web Server to manage the fabric zoning. Zoning enables you to divide the ports and devices of the fabric into zones for more efficient and secure communication among functionally grouped nodes.

The McDATA 4Gb SAN Switch supports port/domain zoning in Standard/Open Fabric interop mode, other M-Series directors and edge switches do not. Therefore, only WWN zoning is supported in Standard/Open Fabric interop mode when McDATA 4Gb SAN Switch is attached to other McDATA switches. Fibre Channel address zoning is not supported by other McDATA switches, and is not recommended for use in McDATA 4Gb SAN Switch.

This subsection addresses the following topics:

Zoning concepts

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

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.

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. Zoning is hardware enforced only when a port/device is a member of no more than eight zones whose combined membership does not exceed 64. If this condition is not satisfied, that port behaves as a soft zone member.

Membership in a zone can be defined by switch domain ID and port number, device Fibre Channel 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.
- 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.

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 the active zone set. This zoning database resides in non-volatile or permanent memory and is therefore retained after a reset. See "Displaying the configured and active zone sets" on page 44 for information about displaying the zoning database. The orphan zone set is created automatically to hold the zones that are not in any set. The orphan zone set cannot be removed and is not saved on the switch.

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

Zoning database

Each switch has its own zoning database. The zoning database is made up of the active zone set that has been created on the switch or received from other switches. The switch maintains two copies of the 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. When a zone set is activated, it is propagated and saved to temporary memory in each switch in the fabric. If the Interop Auto Save parameter is enabled in the Zoning Config dialog, the zone set is saved to permanent memory on that switch.

NOTE: If the Interop 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 Interop 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. See "Configuring the zoning database" on page 42 for information about zoning configuration.

Zoning limits and properties

Zoning limits vary depending on the firmware installed on the switch. To view zoning limits and properties on a switch:

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

The zoning limits and definitions are:

- MaxZoneSets is 1. The maximum number of zone sets that can be configured on the switch. This will be enforced during the configuration of zoning and during a zoning database merge from the fabric.
- MaxZones is 2047. The maximum number of zones that can be configured on the switch. This will be enforced during the configuration of zoning and during a zoning database merge from the fabric.
- MaxTotalMembers is 10,000. The maximum number of total zone members that can be configured on the switch. This will be enforced during the configuration of zoning and during a zoning database merge from the fabric.
- MaxZonesInZoneSets is 2047. The maximum number of zone linkages to zone sets that can be configured on the switch. This will be enforced during the configuration of zoning and during a zoning database merge from the fabric. Every time a zone is added to a zone set this constitutes a linkage.
- MaxMembersPerZone is 4096. The maximum number of zone members that can be added to any zone on the switch. This will be enforced during the configuration of zoning and during a zoning database merge from the fabric.

Managing the zoning database

Managing the zoning database consists of the following:

Editing the zoning database

To edit the zoning database for a particular switch, open the Zoning menu and select **Edit Zoning** to open the Edit Zoning dialog shown in Figure 14. Changes can only be made to an inactive zone set, that is stored in flash (non-volatile) memory and retained after resetting a switch.
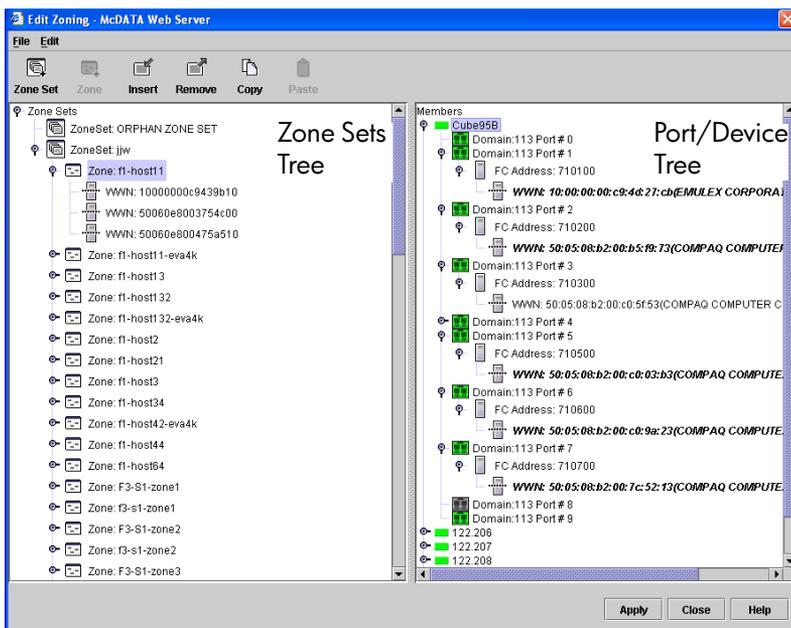
Figure 14 Edit zoning dialog

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 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.

📝 **NOTE:** If the Interop 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.
- Hold down the Shift key while clicking several consecutive icons.
- Hold down 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 6 describes the zoning tool bar operations.

Use the Edit Zoning dialog to define zoning changes, and click **Apply** to open the Error Check dialog. Click **Error Check** to check for zoning conflicts, such as empty zones or zone sets. Click **Save Zoning** to implement the changes. Click **Close** to close the Error Check dialog. Click **Close** in the Edit Zoning dialog to close the Edit Zoning dialog.

Table 6 Edit zoning dialog tool bar buttons and icons

Button/Icon	Description
Zone Set	Create Zone Set button—Create a new zone set
Zone	Create Zone button—Create a new zone
Insert	Add Member button—Add selected port/device to a zone
Remove	Remove Member button—Delete the selected zone from a zone set, or delete the selected port/device from a zone
Copy	Copy button—Copy selected zoning items to clipboard.
Paste	Paste button—Paste 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 to change the **Interop Auto Save** and **Default Zone** configuration parameters. The **Default Zone** parameter applies only when Interop Mode is set to McDATA Fabric Mode. Open the faceplate display. Select **Zoning > Edit Zoning Config** to open the Zoning Config dialog shown in Figure 15. Click **OK** after making changes to put the new values into effect.

Figure 15 Zoning Config dialog (McDATA Fabric Mode)

Interop auto save

The Interop 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 Interop Auto Save is enabled, the switch firmware saves changes to the active zone set in temporary memory and to the zoning database. If Interop Auto Save is disabled, changes to the active zone set are stored only in temporary memory that is cleared when the switch is reset.

> **NOTE:** Disabling the Interop Auto Save parameter can be useful to prevent the propagation of zoning information when experimenting with different zoning schemes. However, leaving the Interop Auto Save parameter disabled can disrupt device configurations should a switch have to be reset. For this reason, the Interop 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 applies only when the interop mode is set to McDATA Fabric Mode. The Default Zone parameter must be the same on all switches in the fabric and is, therefore, automatically distributed throughout the fabric.

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:

1. Select **Zoning > Edit Zoning** in the faceplate display.
2. Select **File > Save As** In the Edit Zoning dialog.
3. Enter a file name for the database file in the Save dialog.
4. Click **Save** 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.

To restore the zoning database from a file to a switch:

1. Select **Zoning > Edit Zoning** in the faceplate display to open the Edit Zoning dialog.
2. Select **File > Open File**. A popup window will prompt you to select an XML zoning database file.
3. Click **Open** after you select a file.

Restoring the default zoning database

Restoring the default zoning clears the switch of all zoning definitions. Restoring default zoning is a fabric-wide action. When you are in Standard mode and restore default zoning, no devices/ports are able to communicate with each other on the switches. When in McDATA mode, restoring default zoning, all devices/ports are able to communicate with each other if Default Zone is enabled, and no devices/ports are able to communicate with each other if Default Zone is disabled.

△ **CAUTION:** This command will deactivate the active zone set.

To restore the default zoning for a switch:

1. Select **Zoning > Restore Default Zoning** in the faceplate display.
2. Click **OK** 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:

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

Managing the active zone set

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

- Displaying the configured and active zone sets, page 44
- Creating a zone set, page 45
- Activating and deactivating a zone set, page 45
- Removing a zone set, page 45

📝 **NOTE:** Zoning database edits are made on an individual switch basis and are not propagated to other switches in the fabric when saved. When a zone set is activated, it is propagated and saved to temporary memory in each McDATA 4Gb SAN Switch in the fabric. If a McDATA 4Gb SAN Switch has the Interop Auto Save parameter enabled in the Zoning Config dialog, the zone set is saved to permanent memory on that switch.

Displaying the configured and active zone sets

You can display the contents of the configured zone set and active zone set with the Configured Zoneset data window and the Active Zoneset data window. The Configured Zonesets and Active Zoneset data windows use 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.

The Configured Zonesets data window, shown in Figure 16, displays all zone sets, zones, and zone membership in the zoning database. To open the Configured Zoneset data window, click the **Configured Zoneset** tab below the data window.
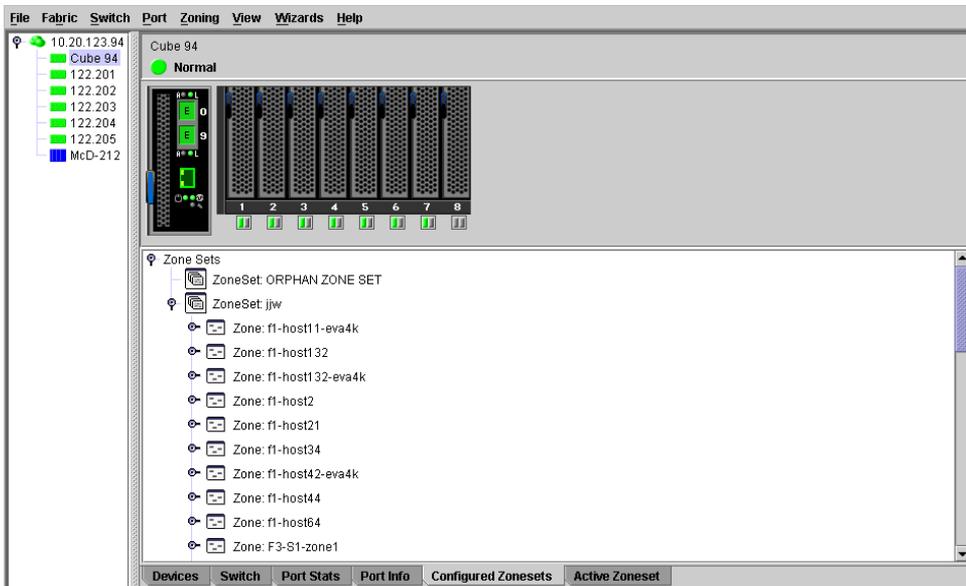
Figure 16 Configured zonesets data window

The Active Zoneset data window, shown in Figure 17, 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.
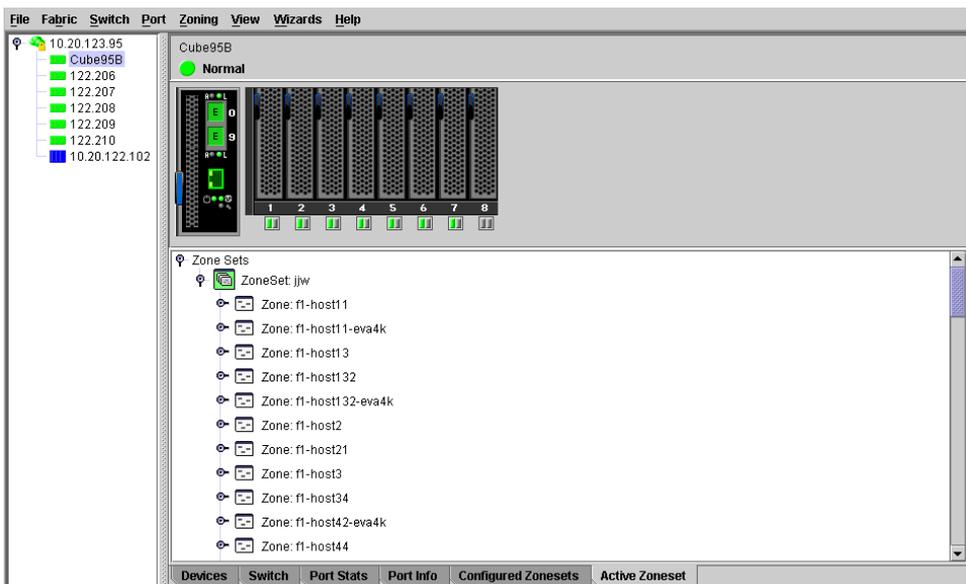
Figure 17 Active zone set data window

Creating a zone set

To create a zone set:

1. Select **Zoning > Edit Zoning** to open the Edit Zoning dialog.
2. Select **Edit > Create Zone Set** to open the Create Zone Set dialog.
3. Enter a name for the new zone set, and click **OK**. 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 the zone set, 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 **OK**. The new zone name is displayed in the Zone Sets dialog.
5. Click **Apply** 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 McDATA 4Gb SAN Switch in the fabric. To activate a zone set:

1. Select **Zoning > Activate Zone Set** to open the Activate Zone Set dialog.
2. Select a zone set from the **Select Zone Set** drop-down list.
3. Click **Activate** to activate the selected zone set.

The purpose of the deactivate function is to suspend all fabric zoning that results in no communication among devices. It is not necessary to deactivate the active zone set before activating a new one. To deactivate the active zone set:

1. Select **Zoning > Deactivate Zone Set** to open the Deactivate Zone Set dialog.
2. Acknowledge the warning about traffic disruption.
3. Click **Yes** to confirm that you want to deactivate the active zone set.

Removing a zone from a zone set

To remove a zone from a zone set:

1. Select **Zoning > Edit Zoning** in the faceplate display to open the Edit Zoning dialog.
2. Select the zone or zones to be removed in the Zone Sets tree.
3. Select **Edit > Remove** to remove the zone from the zone set.
4. Click **Apply** to save changes to the zoning database.

Alternatively, you can use shortcut menus to remove a zone from a zone set or from all zone sets in the database.

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.
- Member zones that are not members of other zone sets become members of the orphan zone set. The orphan zone set cannot be removed and is not saved on the switch.

To delete a zone set from the database:

1. Select **Zoning > Edit Zoning** in the faceplate display to open the Edit Zoning dialog.
2. Select the zone set to be removed in the Zone Sets tree.
3. Select **Edit > Remove** to remove the zone set.
4. Click **Apply** 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, page 46
- Adding zone members, page 47
- Renaming a zone or a zone set, page 47
- Removing a zone member, page 47
- Removing a zone from a zone set, page 48

NOTE: Changes you save to the zoning database on a switch are not propagated to other switches in the fabric unless you activate a zone set or edit the zoning databases on the individual switches in the fabric. When a zone set is activated, it is propagated and saved to temporary memory in each McDATA 4Gb SAN Switch in the fabric. If a switch has the Interop Auto Save parameter enabled in the Zoning Config dialog, the zone set is saved to permanent memory on that McDATA 4Gb SAN Switch. See "Configuring the zoning database" on page 42 for more information.

Creating a zone in a zone set

To create a zone in a zone set:

1. Select **Zoning > Edit Zoning** to open the Edit Zoning dialog.
2. Select a zone set in which to create a zone.
3. Select **Edit > Create a Zone**.
4. Enter a name for the new zone in the Create a Zone dialog

   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 -.
5. Click **OK**.

NOTE: If you enter the name of a zone that already exists in the database, the McDATA Web Server web applet will ask if you would like to add that zone and its membership to the zone set.

---

6. To add switch ports or attached devices to the zone, choose one of the following:
   - Select the zone set In the zone set tree. Select the port to add to the zone in the graphic window. Select **Edit > Add Members**.
   - Select a port by port number 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.
7. Click **Apply** to save changes to the zoning database.

Adding zone members

You can zone a port/device by switch domain ID and port number, or the device port WWN. Adding a port/device to a zone affects every zone set in which that zone is a member. Domain ID/port zoning is only supported in McDATA Fabric interop mode for other McDATA switches. To add ports/devices to a zone:

1. Select **Zoning > 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. Press and hold the **Control** key while selecting multiple ports/devices.
   - Select a port/device in the Port/Device tree. Press the Control key while selecting to select multiple ports/devices. Select a zone set in the left pane. Select **Edit > Add Members**.
   - Select a port/device in the Port/Device tree. Press and hold **Control** while selecting multiple ports/devices. Select a zone set in the left pane. Click **Insert**.

   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. Select **Edit > Create Members**.
   c. Select the **WWN or Domain/Port** option.
   d. Enter the hexadecimal value for the port/device according to the option selected: 16 digits for a WWN member or 4 digits for a Domain/ Port member (DDPP). Domain IDs can be 97–127 when interop mode is set to Standard or1–31 when interop mode is set to McDATA Fabric mode.
3. Click **OK** to display the Error Check dialog.
4. Click **Error Check** to check for zoning conflicts, such as empty zones or zone sets.
5. Click **Save Zoning** to implement the changes.
6. Click **Close** to close the Error Check dialog.
7. Click **Close** to close the Edit Zoning dialog.

📝 **NOTE:**   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 or a zone set

To rename a zone or zone set:

1. Select the zone/zone set to be renamed in the Edit Zoning dialog.
2. Select **Edit > Rename**.
3. Enter a new name for the zone/zone set in the Rename Zone/Rename Zone Set dialog.
4. Click **Yes** in the Rename Zone/Rename Zone Set dialog to save the change.
5. Click **Apply** in the Edit Zoning dialog to save the change.
6. Click **Close** to close the Edit Zoning dialog.

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. Select the zone member to be removed in the Edit Zoning dialog.
2. Select **Edit > Remove**.
3. Click **Yes** in the Remove dialog to save the change.
4. Click **Apply** in the Edit Zoning dialog to save the change.
5. Click **Close** to close the Edit Zoning dialog.

Removing a zone from a zone set

To remove a zone from a zone set:

1. Select the zone to be removed in the Edit Zoning dialog. The selected zone will be removed from that zone set only.
2. Select **Edit > Remove**.
3. Click **Yes** in the Remove dialog to save the change.
4. Click **Apply** in the Edit Zoning dialog to save the change.
5. Click **Close** to close the Edit Zoning dialog.

Zones that are removed from the active zone set are placed in the orphan zone set. The orphan zone set is created by the application automatically to hold the zones that are not in the active zone set. The orphan zone set cannot be removed and is not saved on the switch.

Merging fabrics and zoning

If you join two fabrics with an ISL, 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 Interop Auto Save is turned on.

Zone merge failure

If a zone merge is unsuccessful, the ISLs 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. See "Port information data window" on page 85 for more information. Refer to the *McDATA 4Gb SAN Switch for HP p-Class BladeSystem command line interface guide* for information about the `Show Port` command

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. See "Zoning limits and properties" on page 39 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.

📝 **NOTE:**   If you deactivate the active zone set in one fabric and the Interop 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.

See "Managing zones" on page 46 for information about adding and removing zone members. See "Resetting a port" on page 95 for information about resetting a port.

3 Managing switches

This section describes the following tasks that manage switches using the McDATA Web Server or Element Manager application.

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. Select **Switch > User Accounts** to open the User Account Administration dialog.

A user account consists of the following:

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

Switches come from the factory with the following user accounts:

Table 7 Factory user accounts

Account name	Password	Admin authority	Expiration
admin	password	true	never expires
images	images	false	never expires

The Admin account is the only user that can manage all user accounts with the User Account Administration dialogs. The Admin account can create, remove, or modify user accounts, and change account passwords. The Admin account can also view and modify the switch and its configuration with McDATA Web Server. The Admin account can not be removed.

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

The Images account is used to exchange files with the switch using the File Transfer Protocol (FTP) and can not be removed.

NOTE: 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

A switch can have a maximum of 15 user accounts. To create a new user account on a switch:

1. Select **Switch > User Accounts** in the faceplate display to open the User Account Administration dialog.
2. Click the **Add Account** tab to open the Add Account tab page shown in Figure 18.
3. Enter an account name in the **New Account Login** field. Account names are limited to 15 characters.
4. Select the **Admin Authority Enabled** option if the account is to have the ability to modify switch configurations.
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. Select the **Permanent Account** option if this account is to be permanent with no expiration date. Otherwise, select the **Account Will Expire** option and enter the number days in which the account will expire.
7. Click **Add Account** to add the newly defined account.
8. Click **Close** to close the User Account Administration dialog.

Figure 18 User Account Administration dialog – Add Account tab page

Removing a user account

To remove a user account on a switch:

1. Select **Switch > User Accounts** in the faceplate display to open the User Account Administration dialog.
2. Click the **Remove Account** tab to open the Remove Account tab page shown in Figure 19.
3. Select the account (login) name from the list of accounts at the top of the dialog.
4. Click **Remove Account**.
5. Click **Close** to close the User Account Administration dialog.
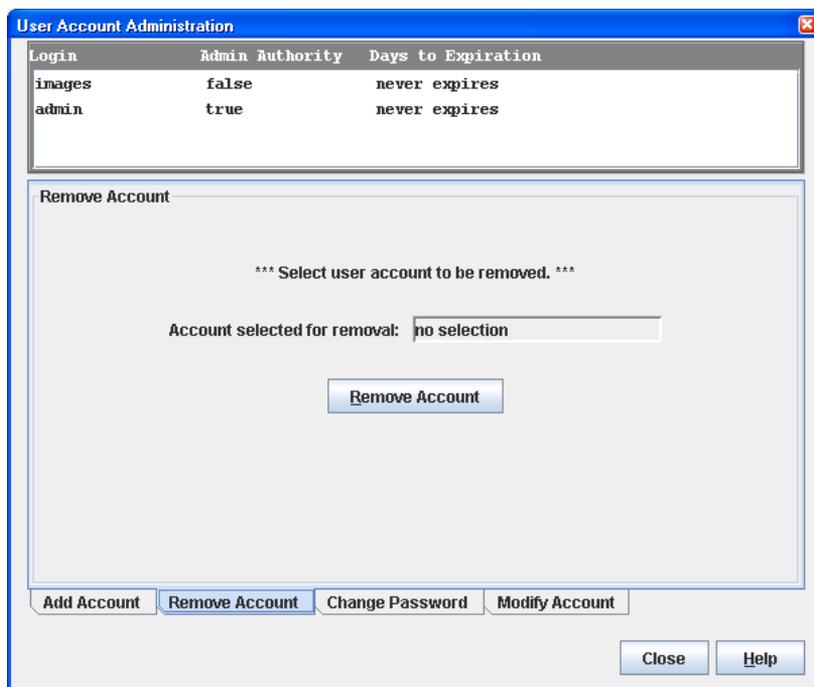
Figure 19 User Account Administration Dialog – Remove Account tab page

Changing a user account password

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. To change the password for an account on a switch:

1. Select **Switch > User Accounts** in the faceplate display to open the User Account Administration dialog.
2. Click the **Change Password** tab to open the Change Password tab page shown in Figure 20.
3. Select the account (login) name from the list of accounts at the top of the dialog.
4. Enter the old password, enter the new password, and re-enter the new password.
5. Click **Change Password**.
6. Click **Close** to close the User Account Administration dialog.

Figure 20 User Account Administration dialog – Change Password tab page

Modifying a user account

To modify a user account on a switch:

1. Select **Switch > User Accounts** in the faceplate display to open the User Account Administration dialog.
2. Click the **Modify Account** tab to open the Modify Account tab page shown in Figure 21.
3. Select the account (login) name from the list of accounts at the top of the dialog.
4. Select the **Admin Authority Enabled** option to grant admin authority to the account name.
5. Select an **Account Expiration Date** option. If the account is not to be permanent, enter the number of days until the account expires.
6. Click **Modify Account** to save the changes.
7. Click **Close** to close the User Account Administration dialog.
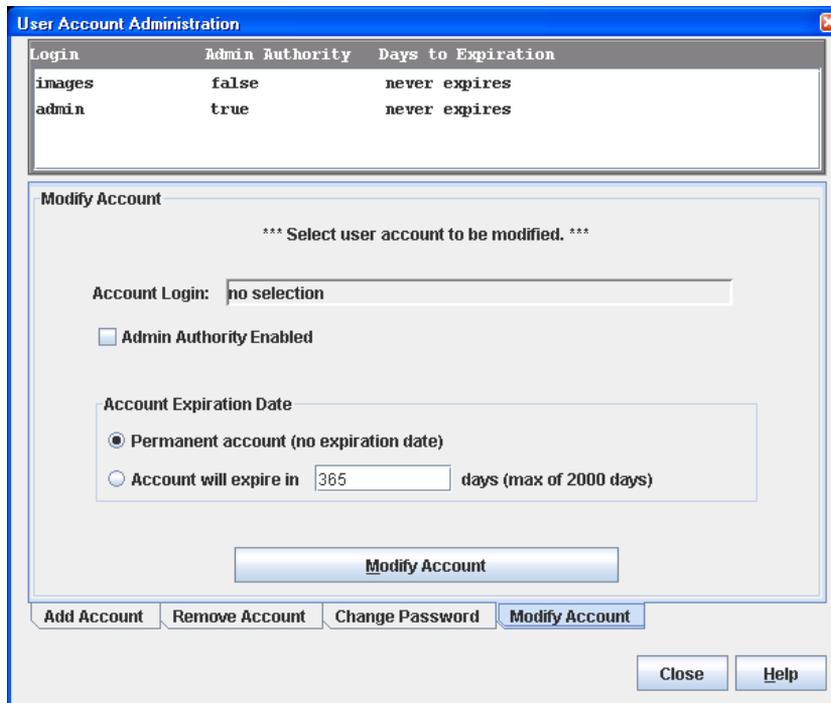
Figure 21 User Account Administration dialog - Modify Account tab page

Configuring RADIUS servers

> **IMPORTANT:** RADIUS server support is available only with the McDATA SANtegrity Enhanced PFE key and can be managed only with the CLI and Element Manager. Element Manager also requires a PFE key. See "Installing Product Feature Enablement keys" on page 82 for more information about installing a PFE key. To obtain the McDATA 4Gb SAN Switch serial number and PFE key, follow the step-by-step instructions on the *firmware feature entitlement request certificate* for the PFE key. You can obtain a PFE key from the web at: www.webkey.external.hp.com.

A RADIUS server authenticates users and devices using a challenge/response protocol over a secure SSL connection. Basic implementations consist of a central RADIUS server containing a database of authorized users as well as authentication information. A RADIUS client wishing to verify the authenticity of a user issues a challenge to the user and collects the response to the challenge. This information is forwarded to the RADIUS server for authentication and the server responds with the results, either an accept or reject.

The RADIUS client does not need to be configured with any user authentication information, this all resides on the RADIUS server and can be managed centrally and separately from the clients. In addition, no passwords are exchanged between the RADIUS server and its clients. Authentication of requests from a RADIUS client to the server and responses from the server to a client can also be authenticated. This requires sharing a secret between the server and client.

The accounting RADIUS supports the auditing of the users and switch services such as Telnet, FTP, and switch management applications. The RADIUS Accounting Server enables (True) or disables (False) the auditing of activity during a user session. The default is False. When enabled, user activity is audited whether UserAuthServer is enabled or not. The accounting server UDP port number is the ServerUDPPort value plus 1 (default 1813).

Configuring RADIUS servers involves the following tasks:

- Adding a RADIUS server, page 55
- Removing a RADIUS server, page 56
- Editing RADIUS server information, page 57
- Modifying RADIUS server authentication order, page 58

Adding a RADIUS server

A RADIUS server provides a method to centralize user and device authentication over a network.
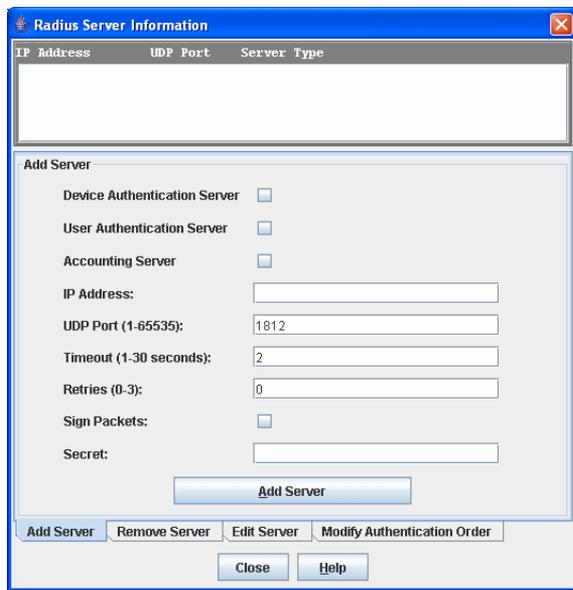
Figure 22 RADIUS Server Information dialog—Add Server tab page

To add a RADIUS server:

1. Select **Switch > Radius Servers** in the faceplate display. The **Radius Servers...** option will not be available unless the SSL service is enabled. See "System services" on page 73 for information about enabling the SSL service.

2. Click the **Add Server** tab in the Radius Server Information dialog shown in Figure 22.

3. Select **Device**, **User**, or **Account** for the server type.

4. Enter the remote IP address of the server in the **IP Address** field.

5. Enter the remote UDP port number of the Authentication RADIUS Server in the **UDP Port** field.

   The RADIUS Accounting Server UDP port will always be the value of Device/User Authentication Server UDP Port + 1. When enabled, the RADIUS Accounting Server audits user activity whether UserAuthServer is enabled or not. The RADIUS Accounting Server default is False.

6. Enter the timeout value in seconds (minimum of 1 second, maximum of 30 seconds) in the **Timeout** field. This is the number of seconds the RADIUS client will wait for a response from the RADIUS server before retrying, or giving up on a request.

7. Enter the number of retries in the **Retries** field. This is the maximum number of times the RADIUS client will retry a request sent to the primary RADIUS server.

8. Select **Sign Packet** to enable the switch to include a digital signature (Message-Authenticator) in all RADIUS access request packets sent to the RADIUS server. A valid Message-Authenticator attribute will be required in all RADIUS server responses.

9. Enter the server secret in the **Secret** field. A secret is required for all RADIUS servers. The secret is used when generating and checking the Message-Authenticator attribute.

10. Click **Add Server** to add the server.

11. Click **Modify Authentication Order** tab, and verify that **Device Authentication Order** and **User Authentication Order** options are set to **Radius** or **Radius Local**. See "Modifying RADIUS server authentication order" on page 58 for more information.

    a. **RADIUS**—Only attempts to authenticate using the RADIUS server (another computer that provides authentication).

    b. **RADIUS Local**—Attempts to authenticate using the RADIUS server. If the switch can not contact the RADIUS server due to a network or some other problem, the switch will authenticate using the local password database.

12. Click **Close** to close the Radius Server Information dialog.

Removing a RADIUS server

Removing a RADIUS server, disables the remote authentication of devices or users over the network.

Figure 23 RADIUS Server Information dialog—Remove Server tab page

To remove a RADIUS server:

1. Select **Switch > Radius Servers** in the faceplate display.
2. Click the **Remove Server** tab in the Radius Server Information dialog shown in Figure 23.
3. Select the server to be removed in server list at the top of the dialog.
4. Click **Remove Server** to remove the server.
5. Click **Close** to close the Radius Server Information dialog.

Editing RADIUS server information

Editing information of a RADIUS server involves changing the configuration of a RADIUS server.
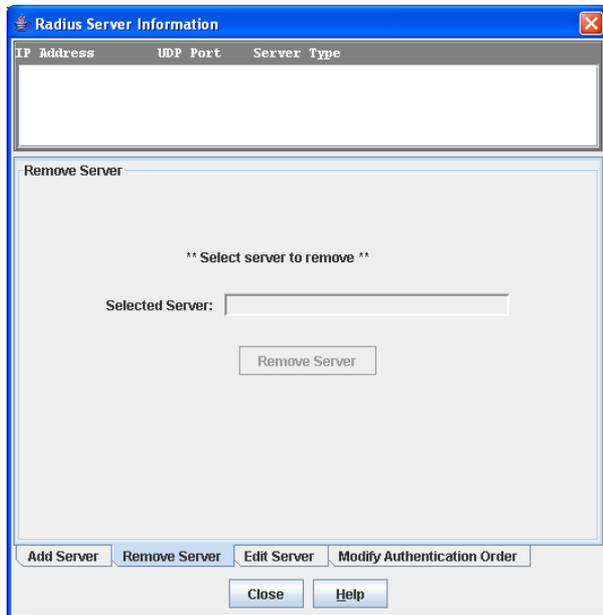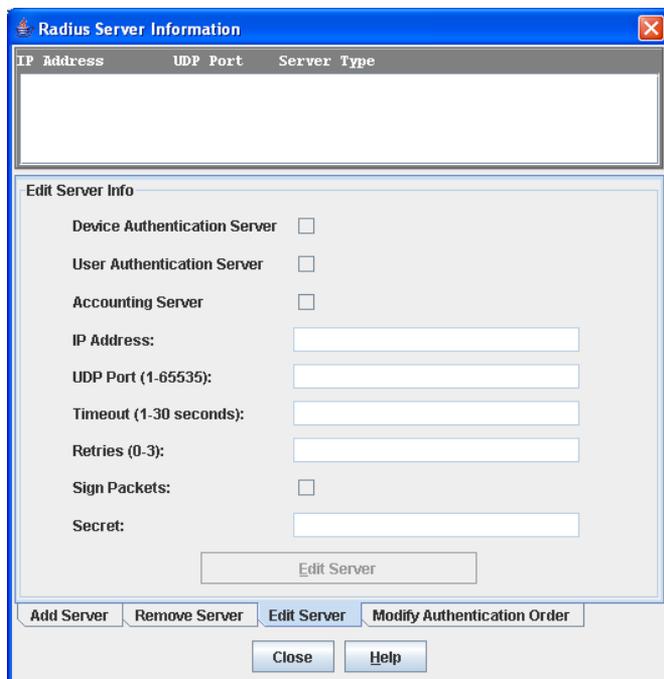

Figure 24 RADIUS Server Information dialog—Edit Server tab page

To edit information of a RADIUS server:

1. Select **Switch > Radius Servers** in the faceplate display.
2. Click the **Edit Server** tab in the Radius Server Information dialog shown in Figure 24.
3. Select the server to be edited in server list at the top of the dialog.
4. Make changes to the **IP Address**, **UDP Port**, **Timeout, Retries**, and **Secret** fields.
5. Select the server type (**Device**, **User**, **Account**) and **Sign Packet** options.
6. Click **Edit Server** to save the changes.
7. Click **Close** to close the Radius Server Information dialog.

Modifying RADIUS server authentication order

Editing information of a RADIUS server involves changing the configuration of a RADIUS server.
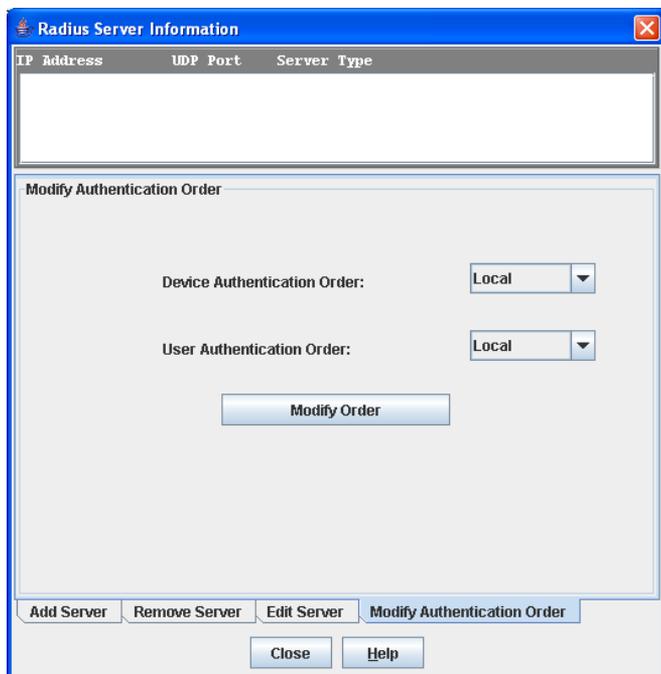
Figure 25 RADIUS Server Information dialog—Modify Authentication Order tab page

To modify the authentication order information of a RADIUS server:

1. Select **Switch > Radius Servers** in the faceplate display.
2. Click the **Modify Authentication Order** tab in the Radius Server Information dialog shown in Figure 25.
3. Select the server to be modified in server list at the top of the dialog.
4. Make changes to the **Device Authentication Order** or **User Authentication Order** drop-down lists. Select one of the following:
   a. **Local**—Only attempts to authenticate using local switch password database.
   b. **RADIUS**—Only attempts to authenticate using the RADIUS server (another computer that provides authentication).
   c. **RADIUS Local**—Attempts to authenticate using the RADIUS server. If the switch can not contact the RADIUS server due to a network or some other problem, the switch will authenticate using the local password database.
5. Click **Modify Order** to save the changes.
6. Click **Close** to close the Radius Server Information dialog.

Displaying switch information

The faceplate display and data windows provide the following switch information:

- Switch event log, page 59
- Device and Host Bus Adapter information, page 59
- Switch status and operational information, page 60
- Port performance statistics, page 64
- Port status and operational information, page 64
- McDATA Web Server Configured Zonesets data window, page 64

The fabric updates the display by forwarding changes in status to the management workstation as they occur. You can allow the fabric to update the switch status, or you can refresh the display at any time. To refresh switch status in the display, choose one of the following:

- Click **Refresh**.
- Select **View > Refresh**.
- Press the **F5** key.
- Right-click in the graphic window of the faceplate display. Select **Refresh Switch** from the popup menu.

Switch event log

You can display the switch event log using the Event Browser. To open the Event Browser from McDATA Web Server, select **Fabric > Show Event Browser**. To open the Event Browser from Element Manager, select **View > Show Event Browser**. See "Displaying the event browser" on page 31 for more information about using the Event Browser.

Device and Host Bus Adapter information

The Devices data window displays information about devices (hosts and storage targets) connected to the switch. Click the **Devices** data window tab to display name server information for all devices that are logged into the selected fabric. To narrow the display to devices that are logged into specific switches, select one or more switches in the fabric tree. See "Devices data window" on page 34 for a description of the entries in the Devices data window.

Switch status and operational information

The Switch data window, shown in Figure 26, displays the current status and operational information for the selected switch. To open the Switch data window, click the **Switch** tab below the data window.
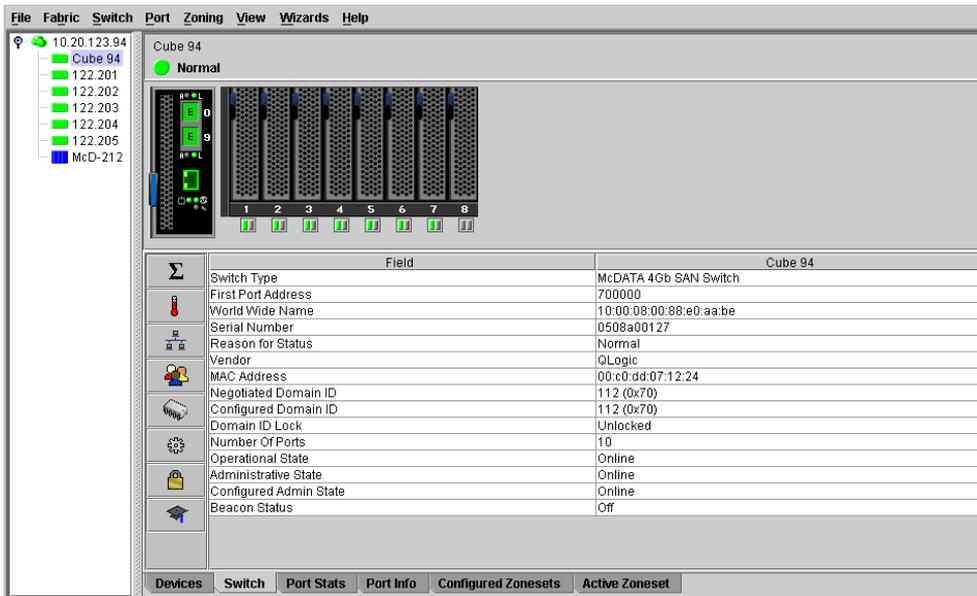
Figure 26 Switch data window

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. The Switch data window entries are listed in Table 8.

Table 8   Switch data window entries

Entry	Description
Σ Summary	
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	Additional status information
Vendor	Switch manufacturer
MAC Address	Media Access Control address
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).

Table 8 Switch data window entries (Continued)

Entry	Description
🌡 Status	
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	Additional status information
Temperature	Internal switch temperature °C
Fan 1 Status	Not applicable.
Fan 2 Status	Not applicable.
Fan 3 Status	Not applicable.
Power Supply 1 Status	Switch power status
Power Supply 2 Status	Not applicable.
Temp Failure Port Shutdown	Port shutdown status when failure temperature is exceeded.
Warning Temperature	Temperature threshold (65° Celsius) above which a warning condition alarm is generated.
Failure Temperature	Temperature threshold (70° Celsius) above which a failure condition alarm is generated.
Diag Status	Diagnostic status
Diag Fault Code	Not applicable.
Test Status	Not applicable.
Test Fault Code	Not applicable.
🖧 Network	
IP Address	Internet Protocol address
Subnet Mask	Mask that determines the IP address subnet
Gateway	Gateway address
SNMP Enabled	SNMP enabled or disabled.
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	Not applicable.

Table 8 Switch data window entries (Continued)

Entry	Description
User Login	
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	
Firmware Version	Active firmware version
Inactive Firmware Version	Not applicable.
Pending Firmware Version	Firmware version that will be activated at the next reset
PROM/Flasher Version	PROM firmware version
Services	
NTP Client Enabled	NTP client status. Controls time synchronization with an NTP 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. McDATA Web Server will report all FDMI information reported by the entry switch, if FDMI is enabled on the entry switch. See "Displaying detailed device information" on page 35 for information about displaying FDMI information.
FDMI HBA Entry Limit	Maximum number of Host Bus Adapters (HBA) that can be registered with a switch.
Embedded GUI Enabled	McDATA Web Server web applet status. Enables or disables the web applet on the switch.
Inactivity Timeout	Number of minutes the switch waits to terminating an idle command line interface session. Zero (0) disables the time out threshold.
GUI Mgmt Enabled	Web applet status.
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 CIM agent is based on the SNIA Storage Management Initiative Specification (SMI-S), which is the standard for SAN management in a heterogeneous environment.
FTP Enabled	FTP status
Management Server Enabled	Management server status.

Table 8 Switch data window entries (Continued)

Entry	Description
SNMP Enabled	SNMP enabled or disabled.
🔒 Zones/Security	
Interop Mode	Interoperability mode. Use Standard to connect to FC-SW-2 compliant switches and McDATA switches in Open Fabric Mode. Use McDATA Fabric Mode to connect to McDATA switches in McDATA Fabric Mode. The default is Standard.
Legacy Address Format	Not applicable.
Interop Auto Save	Zoning auto save status. Saves zoning updates in temporary memory and the zoning database (True) or only in temporary memory (False).
Security Auto Save	Enable to automatically save security settings to permanent memory on the switch.
Security Fabric Binding Enable	If enabled, the expected domain ID of a switch is required before attaching to the fabric.
Zoning Default Visibility	Not applicable.
Default Zone	Disables communication between ports and devices not defined in the active zone set, or when there is no active zone set.
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.
🪶 Advanced	
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	Interoperability mode. Use Standard to connect to FC-SW-2 compliant switches and McDATA switches in Open Fabric Mode. Use McDATA Fabric Mode to connect to McDATA switches in McDATA Fabric Mode. The default is Standard.
Legacy Address Format	Not applicable.
In-band Enabled	In-band management status. Permits (True) or prevents (False) a switch from being managed over an 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.
239 Domain Support	239 domain support status. When enabled on every switch in the fabric, valid domain IDs are expanded to 1–239.

Port performance statistics

The Port Statistics data window displays port performance data for the selected ports. Click the **Port Stats** data window tab in the faceplate display to open the Port Statistics data window. See "Port statistics data window" on page 88 for a description of the Port Statistics data window entries.

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. Open the drop-down list and select **Absolute** to view the total count of statistics since the last switch 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. Click **Clear Baseline** to set the current baseline.

Port status and operational information

The Port Information data window displays port detail information for the selected ports. Click the **Port Info** data window tab in the faceplate display to open the Port Statistics data window. See "Port information data window" on page 85 for a description of the Port Information data window entries.

McDATA Web Server Configured Zonesets data window

The McDATA Web Server Configured Zonesets data window displays all zone sets, zones, and zone membership in the zoning database, shown in Figure 27. Click the **Configured Zonesets** data window tab to open the Configured Zonesets data window. Click the **Active Zonesets** data window tab to view the active zone set in the Active Zonesets 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 the entry can be expanded. Click the entry 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.
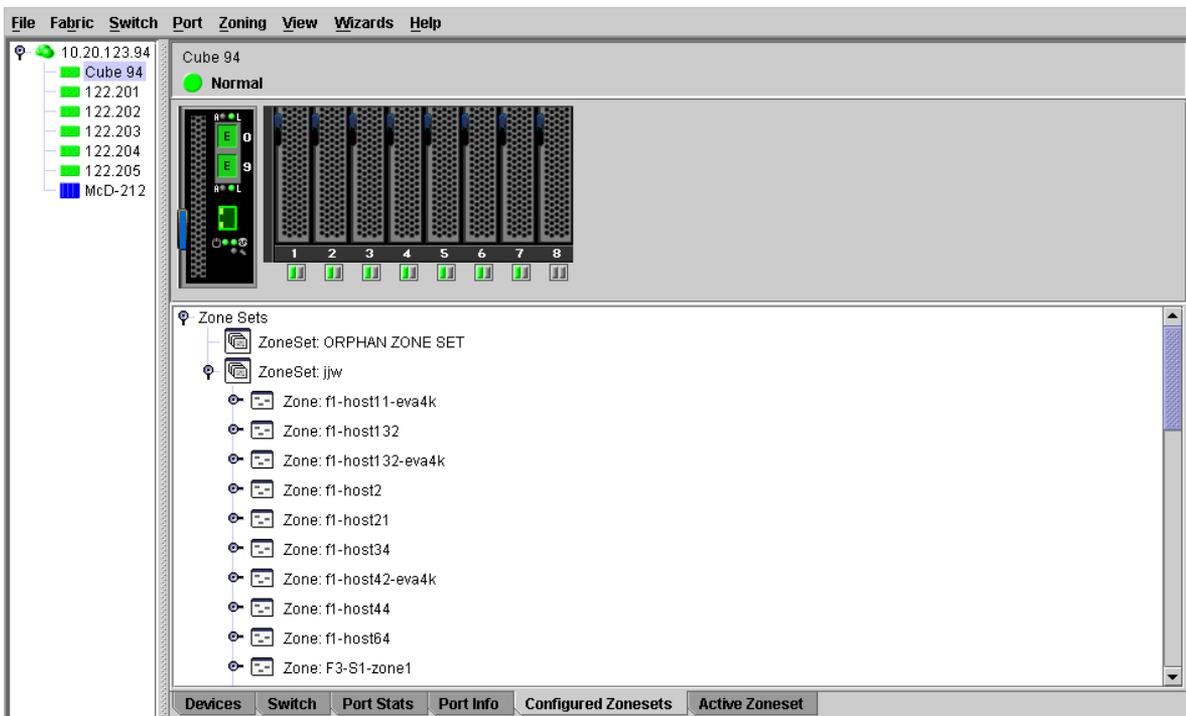
Figure 27 McDATA Web Server Configured Zonesets data window

Configuring port threshold alarms

**IMPORTANT:** Port threshold alarms can be managed only with Element Manager, which requires the Element Manager PFE key, and the CLI. See "Installing Product Feature Enablement keys" on page 82 for more information about installing a PFE key. To obtain the McDATA 4Gb SAN Switch serial number and PFE key, follow the step-by-step instructions on the *firmware feature entitlement request certificate* for the PFE key. You can obtain a PFE key from the web at: www.webkey.external.hp.com.

You can configure the switch to generate alarms for selected events. Configuring an alarm involves choosing an event type, rising and falling triggers, a sample window, and finally enabling or disabling the alarm. To configure port threshold alarms:

1. Open the faceplate display.
2. Select **Switch > Port Threshold Alarm Configuration**. The Port Threshold Alarm Configuration dialog shown in Figure 28 prompts you to enable or disable all alarms, select an event, set triggers, set a sample window and enable or disable an individual alarm.
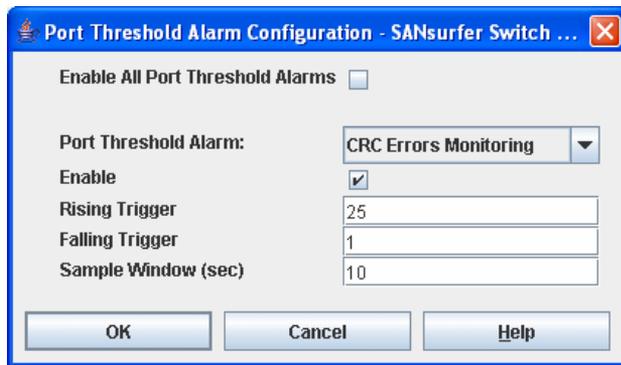
Figure 28 Port Threshold Alarm Configuration dialog

3. Select the **Enable All Port Threshold Alarms** option to enable monitoring for all the individual alarm types that are enabled. The **Enable All Port Threshold Alarms** option is the master control for the individual alarms. For example, the switch will monitor Cyclic Redundancy Check (CRC) errors only if both the **CRC Error Monitoring** option and the **Enable All Port Threshold Alarms** option are selected.
4. Select an event type from the **Port Threshold Alarm** drop-down list. Choose from the following options:
   - CRC error monitoring
   - Decode error monitoring
   - ISL monitoring
   - Login monitoring
   - Logout monitoring
   - Loss of signal monitoring
5. Select the **Enable** option to make the alarm eligible for use.
6. Enter a value for the rising trigger. A rising trigger alarm is generated when the event count per interval exceeds the rising trigger. The switch will not generate another rising trigger alarm for that event until the count descends below the falling trigger and rises again above the rising trigger. Consider the example in Figure 29.
7. Enter a value for the falling trigger. A falling trigger alarm is generated when the event count per interval descends below the falling trigger.

NOTE: The switch will down a port if a rising trigger alarm is not cleared after three consecutive sample windows.
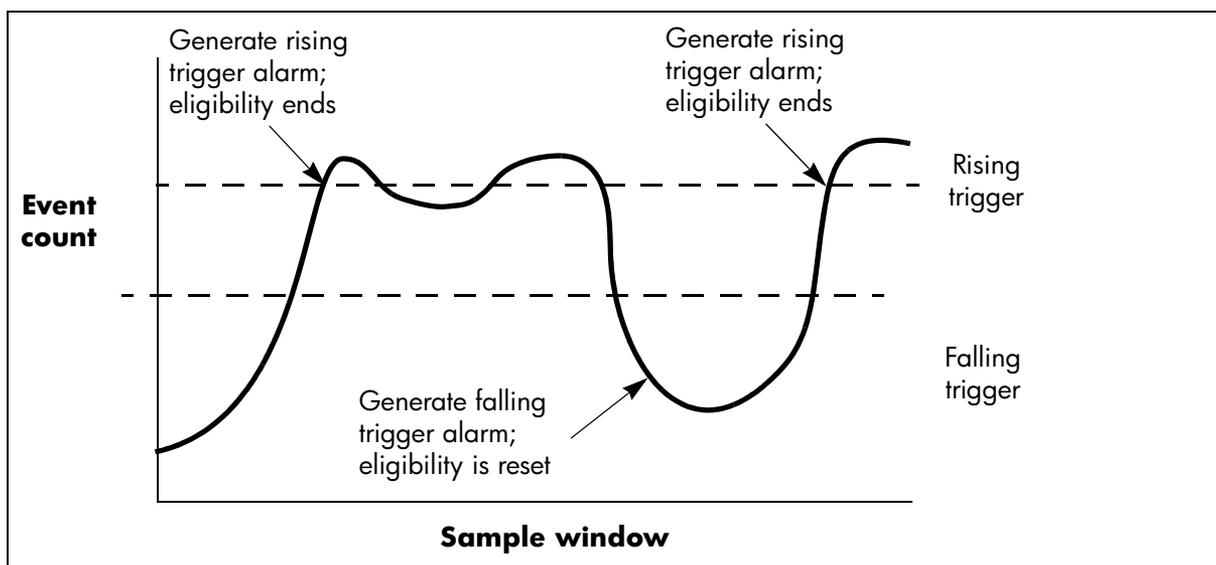
Figure 29 Port threshold alarm example

8. Enter a sample window in seconds. The sample window defines the period of time in which to count events.
9. Repeat steps 3 through 7 for each alarm you want to configure or enable.
10. Click **OK** to save all changes.

Paging a switch

You can use the beacon feature to page a switch. The beacon feature causes all Logged-In LEDs to flash, making it easier to recognize. Select **Switch > Toggle Beacon** (check mark shown) to page a switch. Select **Switch > Toggle Beacon** again (check mark removed) to cancel the beacon.

Setting the date/time and enabling NTP client

The Date/Time and Network Time Protocol (NTP) dialog enables you to manually set the date, time, and time zone on a switch, or to enable the NTP Client. The NTP client synchronizes the date, time, and time zone on the switch with an NTP server. Enabling the NTP client ensures the consistency of date and time stamps in alarms and log entries. An Ethernet connection to an NTP server is required. When date/time is set or displayed in the firmware, it is displayed based on the time zone configured. However, when displayed in the Date/Time dialog, the value is always in local time. The difference between switch and workstation times must not exceed 24 hours, or the switch management application can not connect. To set the date and time on a switch:

1. Select a switch in the fabric tree to open the faceplate display.
2. Select **Switch > Set Date/Time**.
3. Choose one of the following:
    *   Enter the year, month, day, time, and time zone in the Switch Date/Time dialog. The new date and time take effect immediately.
    *   Select a time zone option from the Select Time Zone pull-down list.
    *   Select the **NTP Client Enabled** option to enable the switch to synchronize its time with an NTP server. Enter the IP address of the NTP server. Ethernet connection to NTP server is required.
4. Click **OK** to save the settings.

Resetting a switch

Resetting a switch reboots the switch using configuration parameters in memory. Depending on the reset type, a switch reset may or may not include a Power-on Self Test (POST), or it may or may not disrupt traffic. Table 9 describes the types of switch resets.

During a hot reset operation, fabric services will be unavailable for a short period (30-75 seconds depending on switch model). Verify all administrative changes to the fabric (if any) are complete before performing an 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 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:

- McDATA Web Server or Element Manager sessions will re-connect automatically
- Telnet sessions must be restarted manually.

Applicable code versions:

- Future switch code releases will be upgraded non-disruptively unless specifically indicated in its associated release notes.
- An NDCLA operation to previous switch code releases is not supported.

Table 9   Switch resets

Type	Description
Hot Reset	Resets a switch without a POST. 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 without POST	Resets a switch without a POST. This reset activates the pending firmware and it is disruptive to switch traffic.
Hard Reset	Resets a switch with a POST. This reset activates the pending firmware and it is disruptive to switch traffic.

To reset a switch:

1. Select the switch to be reset in the fabric tree.
2. Select **Switch > 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

You can configure a switch explicitly or you can use the Configuration Wizard. The Configuration Wizard is a series of dialogs that guide you through the chassis, network, and SNMP configuration steps on new or replacement switches. Select **Wizards > Configuration Wizard** to launch the Configuration Wizard. Use the Configuration Wizard to configure a new switch in a fabric.

To configure the switch explicitly, see the following properties and services:

- Switch properties, page 68
- Advanced switch properties, page 72
- System services, page 73
- Network properties, page 75
- SNMP properties, page 76

Switch properties

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

- Domain ID and domain ID lock, page 69
- Syslog, page 70
- Symbolic name, page 70
- Switch administrative states, page 71
- Broadcast support, page 71
- In-band management, page 71
- Fabric Device Management Interface, page 72

To open the Switch Properties dialog shown in Figure 30, choose one of the following:

- Open the faceplate display for the switch you want to configure, and select **Switch > Switch Properties**.
- Right-click the switch in the graphic window, and select **Switch Properties** from the popup menu.
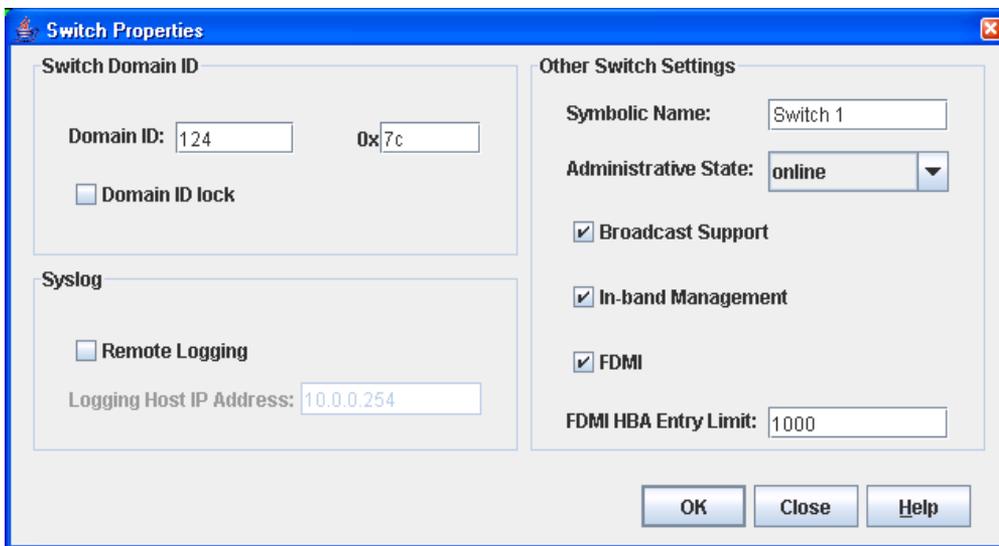
Figure 30 Switch properties dialog

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). Switches come from the factory with the Domain ID Lock setting disabled (False). This 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. See the `Set Config Switch` command to change the Domain ID Lock and Principal Priority parameters. Refer to the *McDATA 4Gb SAN Switch for HP p-Class BladeSystem command line interface guide* for information about the `Set Config Switch` command and the command line interface.

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.

NOTE: 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.

The McDATA 4Gb SAN Switch displays domain IDs differently in Standard mode than other M-series directors and edge switches. When the McDATA 4Gb SAN switch is in Standard mode (default), the domain ID will be displayed differently depending on which management utility is used. The valid Domain ID range while in standard mode (default) is 97—127. McDATA Web Server and CLI will display this as 97—127. HAFM will display this as 1—31.

Prior to changing from Standard mode to McDATA Fabric mode, it is recommended that the switch be isolated from the fabric (take switch offline) before making the configuration changes and all domain IDs in the fabric should be noted to avoid conflicts. Once isolated, using CLI or McDATA Web Server, change interop mode to McDATA Fabric mode, and change the domain ID to a unique ID within the valid range of 1—31 for McDATA Fabric mode. It is then recommended that the Domain ID be locked to prevent conflict within the fabric. When all changes have been made and the switch has been brought back online, it should then be added into the fabric.

In McDATA Fabric mode, the McDATA 4Gb SAN Switch will display the domain IDs the same as other M-series directors and edge switches no matter which management utility is used. The valid domain ID range is 1—31 for McDATA Fabric mode.

Prior to changing from McDATA Fabric mode to Standard mode, it is recommended that the switch be isolated from the fabric (take switch offline) before making the configuration changes and all domain IDs in the fabric should be noted to avoid conflicts. Once isolated, using McDATA Web Server, Element Manager, or the CLI, change interop mode to Standard and change the domain ID to a unique ID within the valid range of 97—127 for standard mode. It is then recommended that the Domain ID be locked to prevent conflict within the fabric. When all changes have been made and the switch has been brought back online, it should then be added into the fabric.

Both Standard Mode and McDATA Fabric Mode permit a maximum of 31 domain IDs. For fabrics in which all other switches support 239 domain IDs, you can extend the valid domain IDs on the McDATA 4Gb SAN Switch to 1-239 by enabling 239 Domain Support. See "Interop mode" on page 73 for more information.

Table 10 lists the corresponding domain ID values for each interop mode: Standard mode and McDATA Fabric mode.

Table 10   Corresponding domain ID values by interop mode

McDATA Fabric mode	Standard mode	McDATA Fabric mode	Standard mode	McDATA Fabric mode	Standard mode
1	97	12	108	23	119
2	98	13	109	24	120
3	99	14	110	25	121
4	100	15	111	26	122
5	101	16	112	27	123
6	102	17	113	28	124
7	103	18	114	29	125
8	104	19	115	30	126
9	105	20	116	31	127
10	106	21	117		
11	107	22	118		

Syslog

The Syslog (Remote Logging) feature enables saving of the 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 not.

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.

- The configured administrative state is the state that is saved in the switch configuration and is preserved across switch resets. McDATA Web Server or Element Manager always makes changes to the configured administrative state. The configured administrative state is displayed in the Switch Properties dialog.
- The current administrative state is 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. See the *McDATA 4Gb SAN Switch for HP p-Class BladeSystem command line interface guide* for information about the command line interface.

Table 11 describes the administrative state values.

Table 11   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 then be run on all ports of the switch. The switch must be reset after leaving the Diagnostics state.

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. When a broadcast frame is received, these zones are enforced at the N_Ports and NL_Ports. If the originator of the broadcast is in a zone, the frame is retransmitted on all online N_Ports and NL_Ports within the zone. If the originator of the broadcast frame is not in a zone, the frame is retransmitted on online N_Ports and NL_Ports that are not in a zone. The default setting is disabled.

In-band management

In-band management is the ability to manage switches across ISLs using McDATA Web Server, 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 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. McDATA Web Server or Element Manager will report any and 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 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 HBAs exceeds the maximum number, the FDMI information for those HBAs can not be registered.

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

Click the **Devices** data window tab and click **(i)** in the Details column of the Devices data window to view detailed FDMI information for a device. The Detailed Devices Display dialog displays the specific information for that device. See "Devices data window" on page 34 for more information.

Advanced switch properties

The Advanced Switch Properties dialog shown in Figure 31 enables you to set the timeout values and interop mode settings. The Advanced Switch Properties dialog is available for only the entry switch, because an in-band switch can not be taken offline. The switch will automatically be taken offline temporarily and will be restored to its original state after the changes are completed. Select **Switch > Advanced Switch Properties** to open the Advanced Switch Properties dialog. Click **OK** after making any changes to put the new values into effect. The default interop mode is Standard.
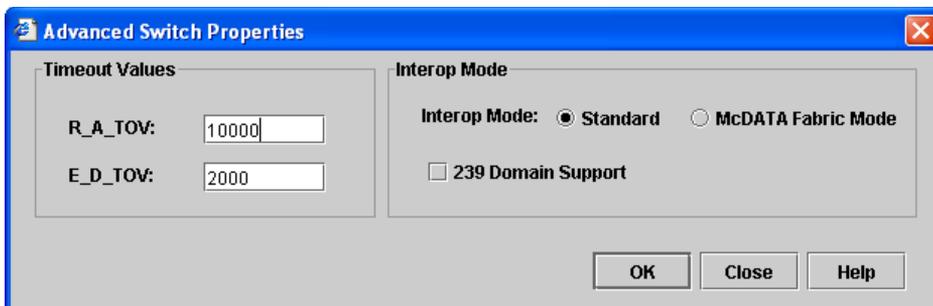
Figure 31 Advanced switch properties dialog

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

• Timeout values, page 73
• Interop mode, page 73

Timeout values

The switch timeout values determine the timeout values for all ports on the switch. Table 12 describes the switch timeout parameters. The timeout values must be the same for all switches in the fabric.

> **NOTE:** Mismatched timeout values will disrupt the fabric. These 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 12 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.

Interop mode

Interop mode permits interoperability with other switches in the following environments:

- Standard: Permits interoperability with FC-SW-2 compliant switches and McDATA switches in Open Fabric Mode. Valid domain IDs are 97–127.
- McDATA Fabric Mode: Permits interoperability with other McDATA switches in McDATA Fabric Mode. Valid domain IDs are 1–31.

Enabling the 239 Domain Support option extends the valid domain IDs to 1–239 for both Standard and McDATA Fabric Mode settings. However, all switches in the fabric must support 239 domain IDs.

System services

The System Services dialog provides a central location for you to enable or disable any of the external user services such as SNMP, Secure Sockets Layer (SSL), Secure SHell (SSH), embedded switch management application (McDATA Web Server or Element Manager), CLI, Network Time Protocol (NTP), and Common Information Model (CIM). Select **Switch > Services** to display the System Services dialog shown in Figure 32.
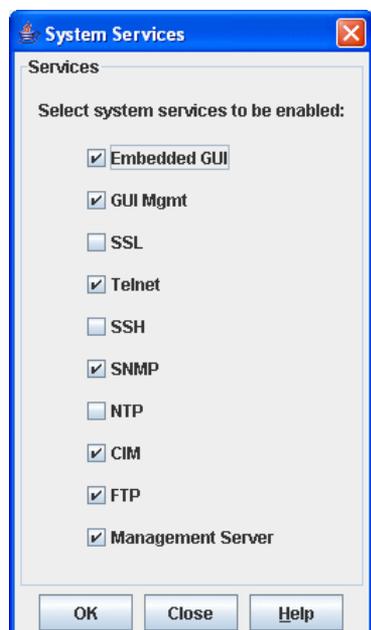
Figure 32 System services dialog

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

IMPORTANT: The SSL and SSH services can be managed only with Element Manager, which requires the Element Manager PFE key, and the CLI. See "Installing Product Feature Enablement keys" on page 82 for more information about installing a PFE key. To obtain the McDATA 4Gb SAN Switch serial number and PFE key, follow the step-by-step instructions on the *firmware feature entitlement request certificate* for the PFE key. You can obtain a PFE key from the web at: www.webkey.external.hp.com.

- **Embedded GUI**—McDATA Web Server and Element Manager. Allows users to point a browser at the switch and run the McDATA Web Server application; or run Element Manager from HAFM.
- **GUI Mgmt**—Allows out-of-band management of the switch from the switch management application (GUI). If disabled, the switch can not be specified as the entry switch for a fabric in the GUI, but can still be managed through an in-band connection.
- **SSL**—Secure Sockets Layer. Provides secure encrypted communications between the switch management application (GUI) and the switch. SSL must be enabled before you can configure device security and RADIUS servers. SSL certificates are generated on the switch with the switch date/time and validated with the workstation's date/time. If the Switch and workstation date/time are not synchronized, invalid certificates will be generated and prevent an SSL connection from being established between the switch and the management application. To disable SSL when using a user authentication RADIUS server, the RADIUS authentication order must first be set to Local.
- **Telnet**—CLI. Allows users to manage the switch through a Telnet CLI session. Disabling Telnet access to the switch is not recommended.
- **SSH**—Secure SHell. Provides secure encrypted Telnet CLI sessions with the switch. Note that you will have to have an SSH client running on your workstation in order to manage your switch with Telnet CLI when SSH is enabled.
- **SNMP**—Simple Network Management Protocol. Allows management of the switch through third-party applications that use SNMP.
- **NTP**—Network Time Protocol. Allows the switch to obtain its time and date settings from an NTP server. Configuring all of your switches and your workstations to utilize NTP will keep their date/time settings in sync and will prevent difficulties with SSL certificates and event logs.
- **CIM**—Common Information Model. Allows management of the switch through third-party applications that use CIM.
- **FTP**—File Transfer Protocol. Allows file transfers to the switch via FTP. FTP is required for out-of-band firmware uploads that will complete faster than in-band firmware uploads.
- **Management Server**—Allows management of the switch through third-party applications that use GS-3 Management Server.
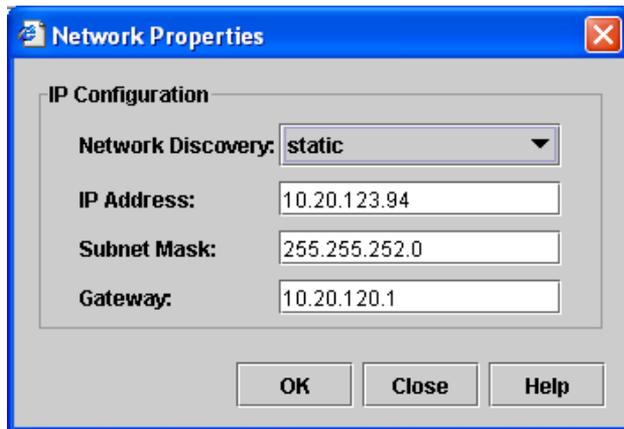
Network properties

Use the Network Properties dialog shown in Figure 33 to change IP configuration parameters.

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

- Select **Switch > Network Properties**.
- Right-click a switch graphic in the faceplate display, and select **Network Properties** from the popup menu.

Click **OK** to put any new values into effect.

Figure 33 Network properties dialog

Table 13 describes the IP configuration parameters.

Table 13 Network IP configuration parameters

Parameter	Description
Network Discovery	Choose one of the following methods by which to assign the IP address: • **Static**—Uses the IP configuration parameters entered in the Switch 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 in order 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	IP gateway address. The default value is 10.0.0.254.

SNMP properties

Use the SNMP Properties dialog shown in Figure 34 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:
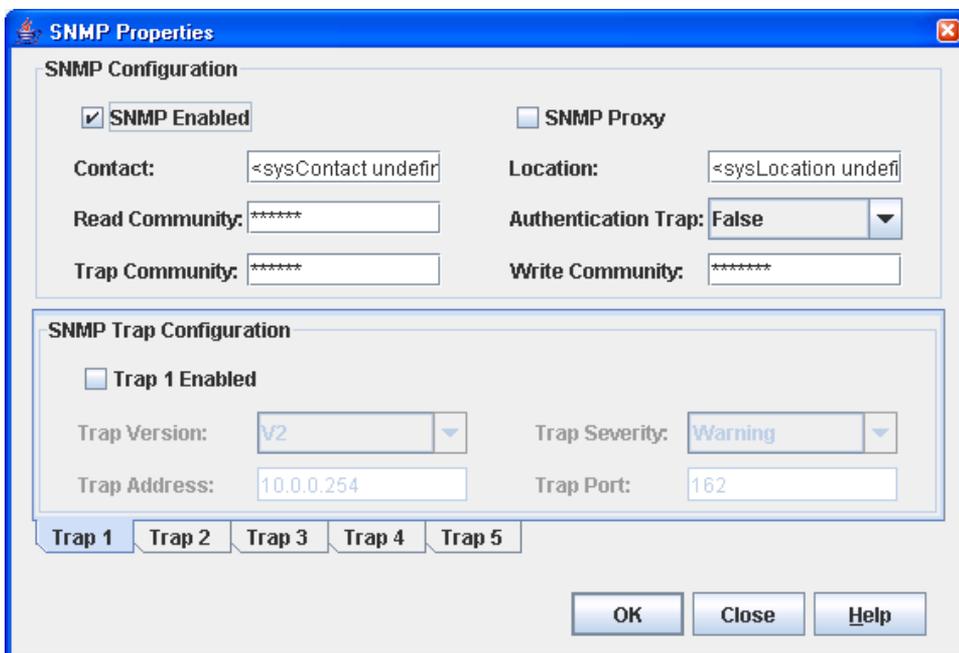
- Select **Switch > SNMP Properties**.
- Right-click a switch graphic in the faceplate display, and select **SNMP Properties** from the popup menu.

Making any changes. Click **OK** to put the new values into effect.

NOTE: 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 34 SNMP Properties dialog

SNMP properties are divided into the following components:

- SNMP configuration, page 77
- SNMP trap configuration, page 77

SNMP configuration

The SNMP configuration defines how authentication traps are managed. Table 14 describes the SNMP configuration parameters. The illegal characters for the user-defined fields are the pound sign (#), semi-colon (;), and comma (,).

Table 14   SNMP configuration parameters

Parameter	Description
SNMP Enabled	Enables or disables SNMP communication with other switches in the fabric. If disabled, the user cannot use an SNMP application at a workstation to talk to the switch that has this setting disabled.
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 is a write-only field. The value on the switch and the SNMP management server must be the same. The default is "public".
Trap Community	Trap community password (up to 32 characters) that authorizes an SNMP agent to receive traps. This is a write-only field. The value on the switch and the SNMP management server must be the same. The default is "public".
SNMP Proxy	Not applicable.
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 is a write-only field. 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 15 describes the SNMP configuration parameters.

Table 15   SNMP trap configuration parameters

Parameter	Description
Trap Version	Specifies the SNMP version (1 or 2) 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[1]	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 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

1. 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.

Archiving a switch

You can create an .XML archive file containing the configuration parameters. Basically any data received by McDATA Web Server 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.

Archived parameters include the following:

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

To archive a switch:

1. Select **Switch > Archive** in the faceplate display.
2. Enter a file name in the Save dialog.
3. Click **Save**.

Switch binding

IMPORTANT: Switch binding is available only with the McDATA SANtegrity Enhanced PFE key and can be managed only with the CLI and Element Manager. Element Manager also requires a PFE key. See "Installing Product Feature Enablement keys" on page 82 for more information about installing a PFE key. To obtain the McDATA 4Gb SAN Switch serial number and PFE key, follow the step-by-step instructions on the *firmware feature entitlement request certificate* for the PFE key. You can obtain a PFE key from the web at: www.webkey.external.hp.com.

Switch binding establishes a list of up to 256 switches or devices that are permitted to log in to a particular switch. Switches or devices that are not among the 256 are refused access to the switch. Furthermore, you can specify whether to enforce the list for all switches and devices, devices only, or switches only. To enable switch binding for a switch and specify device WWNs:

1. Select a switch and open the faceplate display
2. Select **Switch > Switch Binding** to open the Switch Binding dialog.
3. Click the **Switch Binding** checkbox to enable switch binding.
4. Select each device WWN from the WWN: pull-down menu and click **Add**. To remove a WWN, select the WWN in the WWN List and click **Remove**.
5. Specify how you want switch binding to be enforced:
   - Click **All Ports** checkbox to enforce the WWN list for all switches and devices.
   - Click the **F_Ports** checkbox to enforce the WWN list for all devices.
   - Click the **E_Ports** checkbox to enforce the WWN list for all switches.
6. Click **OK**.

Restoring a switch

Restoring a switch loads the archived switch configuration parameters to the switch. The switch configuration must be archived before it can be restored. The switch archive must be compatible with the switch to be restored; that is, you can restore a McDATA switch only with an archive from a McDATA Web Server switch. See "Archiving a switch" on page 78 for more information.

△ **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.

The Restore dialog consists of the **Full Restore** tab page and **Selective Restore** tab page. To restore a switch:

1. Log in to the fabric through the switch you want to restore. You cannot restore a switch over an ISL.
2. Select **Switch > Restore** in the faceplate display to open the Restore dialog shown in Figure 35.
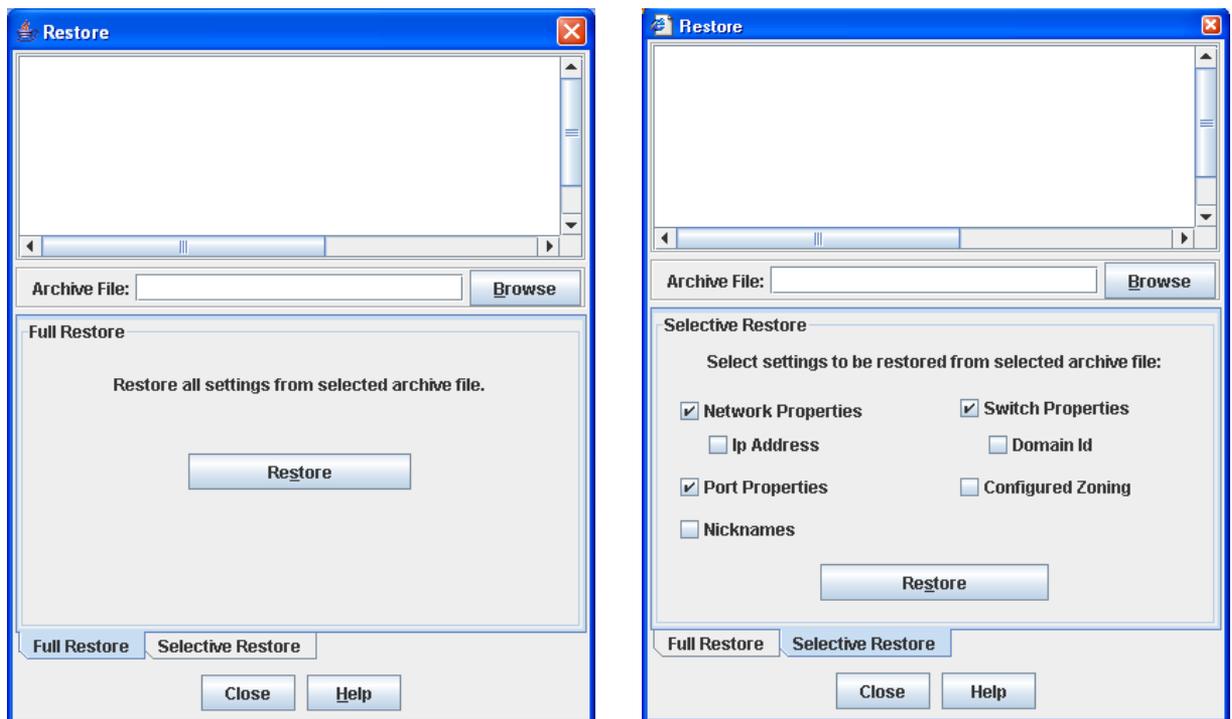
Figure 35 Restore Dialogs – Full Restore and Selective Restore tab pages

3. Enter the archive file name or browse for the file. This archive file must be one that was produced by the Archive function. Configuration backup files created with the Config Backup command are not compatible with the McDATA Web Server Restore or Element Manager Restore function.

4. To restore all configuration settings, click the **Full Restore** tab, then click **Restore**. To restore selected configuration settings, click the **Selective Restore** tab and select one or more of the following options, then click **Restore**:

   - **Network Properties**—Restores all settings presented in the Network properties dialog except the IP address. See "Network properties" on page 75.
     - **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 "Viewing and configuring ports" on page 91.
   - **Nicknames**—Restores the last saved nickname configuration.
   - **Switch Properties**—Restores all settings presented in the Switch properties dialog except the domain ID. See "Switch properties" on page 68.
     - **Domain ID**—Restores switch domain ID in addition to the other switch properties.
   - **Configured Security**—Restores all security sets in the switch database. See "Device security" on page 23. This option is available only in Element Manager.
   - **Configured Zoning**—Restores all configured zone sets, zones, and aliases in the switch's zoning database excluding the active zone set.

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 **Yes**. Select a zone set from the drop-down list in the Select Zone Set to be Activated dialog.

6. Click **OK** 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. Select **Switch > Restore Factory Defaults** to restore the factory configuration on a switch. lists the factory default switch configuration settings. Restoring the switch to the factory default configuration does not restore the account name and password settings. The most current port license will remain in effect. To restore user accounts, you must select the **Reset User Accounts to Default** option in the maintenance menu. See "Recovering a Switch" in the *McDATA 4Gb SAN Switch for HP p-Class BladeSystem installation guide* for information about maintenance mode and the maintenance menu.

Table 16 Factory default configuration settings

Setting	Value
Symbolic Name	McDATA4GbSAN
Administrative State	Online
Domain ID	97
Domain ID Lock	False
In-band Management	True
Broadcast Support	Enable
Resource Allocation Timeout (R_A_TOV)	10000 milliseconds
Interop Mode	Standard
Device Scan Enabled	True
Error Detect Timeout (E_D_TOV)	2000 milliseconds
SNMP Enabled	True
SNMP Proxy	False
IP Address	10.0.0.1
FDMI Enabled	True

Table 16 Factory default configuration settings (Continued)

Setting	Value
FDMI HBA Entry Level	1000
Subnet Mask Address	255.0.0.0
Gateway Address	10.0.0.254
Network Discovery	Static
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 for internal and external ports
Port Type	External ports are GL_Ports Internal ports are FL_Ports

Downloading a support file

The **Download Support File** 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.

To create a support file:

1. Open the faceplate display.
2. Select **Switch > Download Support File**.
3. Click **Browse** to define a location for the support file or enter the path in the text field in the Download
   Support File dialog.
4. Click **Start** to begin the process of creating and downloading the support file to your workstation.
   Observe the status in the Status area.
5. Click **Close** to close the Download Support File dialog after the support file is saved to your workstation.

Installing Product Feature Enablement keys

A PFE key is a password that you can purchase from your switch distributor or authorized reseller that enables particular features in your switch. The following PFE keys are available:

- SANtegrity Enhanced PFE key enables device security on the switch. This includes support for the following:
  - RADIUS servers. See "Configuring RADIUS servers" on page 54.
  - Device security. See "Device security" on page 23.
  - Switch binding. See "Switch binding" on page 78.
- Element Manager PFE key enables the use of the Element Manager through HAFM.

> **NOTE:** To obtain the McDATA 4Gb SAN Switch serial number and PFE key, follow the step-by-step instructions on the *firmware feature entitlement request certificate* for the PFE key. You can obtain a PFE key from the web at: www.webkey.external.hp.com.

To install a PFE key:

1. Add a fabric with the IP address of the switch on which you want to install the PFE key.
2. Open the faceplate display of the switch on which you want to install the PFE key.
3. Select **Switch > Features** to display the Feature Licenses dialog shown in Figure 36.
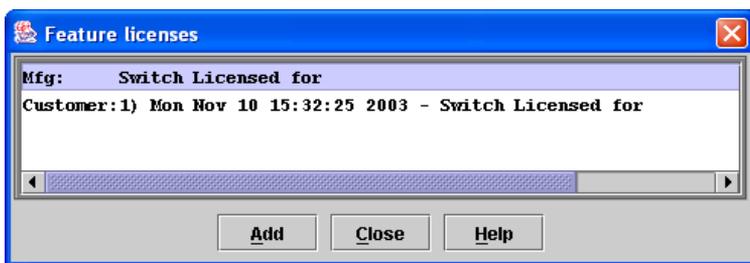
Figure 36 Features Licenses dialog

4. Click **Add** to open the Add License Key dialog shown in Figure 37.
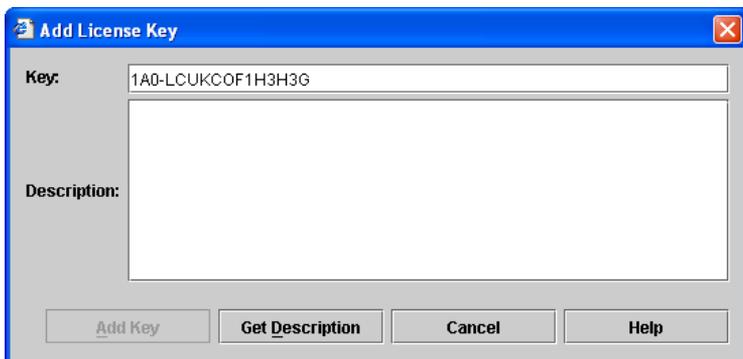
Figure 37 Add License Key dialog

5. Enter the license key in the **Key** field.
6. Click **Get Description** to display the PFE key description.
7. Click **Add Key**. Allow a minute or two to complete.

Installing firmware

Installing firmware involves loading, unpacking, and activating the firmware image on the switch. McDATA Web Server does this in one operation. To provide consistent performance throughout the fabric, ensure the following:

- All McDATA 4Gb SAN Switches are running the same version of firmware. Verify that this version of firmware is compatible with the firmware of other M-series and McDATA switch models in the fabric.
- All other M-series and McDATA switch models are running the same version of firmware.

You can load and activate firmware on an operating switch without disrupting data traffic or having to re-initialize attached devices. If you attempt to perform a non-disruptive activation without satisfying the following conditions, the switch will perform a disruptive activation:

- The current firmware version is a version that supports upgrading to the new version
- No changes are being made to switches in the fabric including powering up, powering down, disconnecting or connecting ISLs, and switch configuration changes
- No port in the fabric is in the diagnostic state
- No zoning changes are being made in the fabric
- No changes are being made to attached devices including powering up, powering down, disconnecting, connecting, and HBA configuration changes

Ports that are stable when the non-disruptive activation begins and then change states, will be reset. When the non-disruptive activation is complete, the switch automatically performs a hot reset. McDATA Web Server or Element Manager sessions reconnect automatically. However, Telnet sessions must be restarted manually.

When you need to do NDCLA/hot reset to multiple switches, only perform the NDCLA/hot reset on one switch at a time, and allow a 75 second wait before performing the NDCLA/hot reset operation on the next switch.

△ **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 includes powering up or powering down attached devices), and adding, moving or removing ISLs or other connections.

To install firmware:

1. Select **Switch > Load Firmware**.
2. Click **Browse**, and browse for and select the firmware file to be loaded in the Load Firmware dialog.
3. Click **Start** to begin the firmware load process. You will be shown a message warning you that the switch will be reset to activate the firmware.
4. Click **OK** to continue firmware installation, or click **Cancel** to cancel the firmware installation. The switch will attempt a hot reset, if possible, to activate the firmware without disrupting data traffic. During a non-disruptive activation, all Logged-In LEDs are extinguished for several seconds. If a non-disruptive activation is not possible, an error message will be shown. To activate the firmware image, the user may either resolve the error described in the message and perform a hot reset on the switch or simply reset the switch (disruptive).

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

- McDATA Web Server and Element Manager sessions will re-connect automatically
- Telnet sessions must be restarted manually

Applicable code versions:

- Future switch code releases will be upgraded non-disruptively unless specifically indicated in its associated release notes
- An NDCLA operation to previous switch code releases is not supported

Displaying hardware status

To display a summary of the hardware status information in a popup text box, rest the cursor over the chassis LED cluster in the faceplate display.

- Power LED—Indicates the voltage status of the switch.
- Heartbeat LED—Indicates the general status of the internal switch processor and the results of the POST.
- System Fault LED—Indicates an error, such as an over temperature condition, internal system error, voltage fault, or corrupt configuration.

Figure 38 Hardware status LEDs

4 Managing ports

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

> 📝 **NOTE:** External ports are numbered 0 and 9; internal ports are numbered 1–8.

Port information data window

The Port Information data window, shown in Figure 39, displays detailed port information for the selected ports. To open the Port Information data window, click the **Port Info** data window tab.

Figure 39 Port Information data window

Information in the Port Information data window is grouped and viewed by the Summary, Advanced, Extended Credits, and Media buttons. Click a button to display the corresponding information in the data window on the right.

The Port Information data window entries are listed below in Table 17.

Table 17 Port information data window entries

Entry	Description
Σ Summary	
Port Address	Port Fibre Channel address.
Administrative Port Type	The administrative port type (G, GL, F, FL). 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 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	E_Port connection status. Status can be None, Connecting, Connected or Isolated.
Isolation Reason	E_Port isolation reason
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 (1-Gbps, 2-Gbps, 4-Gbps)
Symbolic Name	Port symbolic name
Diagnostic Status	Status from the most recent Power-on self test
Diagnostic 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

Table 17 Port information data window entries (Continued)

Entry	Description
[icon] Advanced	
MFS Mode	Multiple Frame Sequence bundling status.
I/O Stream Guard	Not applicable
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	Not applicable
[icon] Extended Credits	Not applicable
[icon] Media	
Media Type	The transceiver fibre type, such as single mode, multi-mode, copper.
Media	The transceiver type.
Media Speed	The maximum transceiver speed
Media Transmitter	The transceiver transmitter type, such as longwave, 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

Port statistics data window

The Port Statistics data window, shown in Figure 40, displays statistics about port performance. Select one or more ports in the faceplate display that you want to view statistics. Click the **Port Stats** data window tab to open the Port Statistics window.
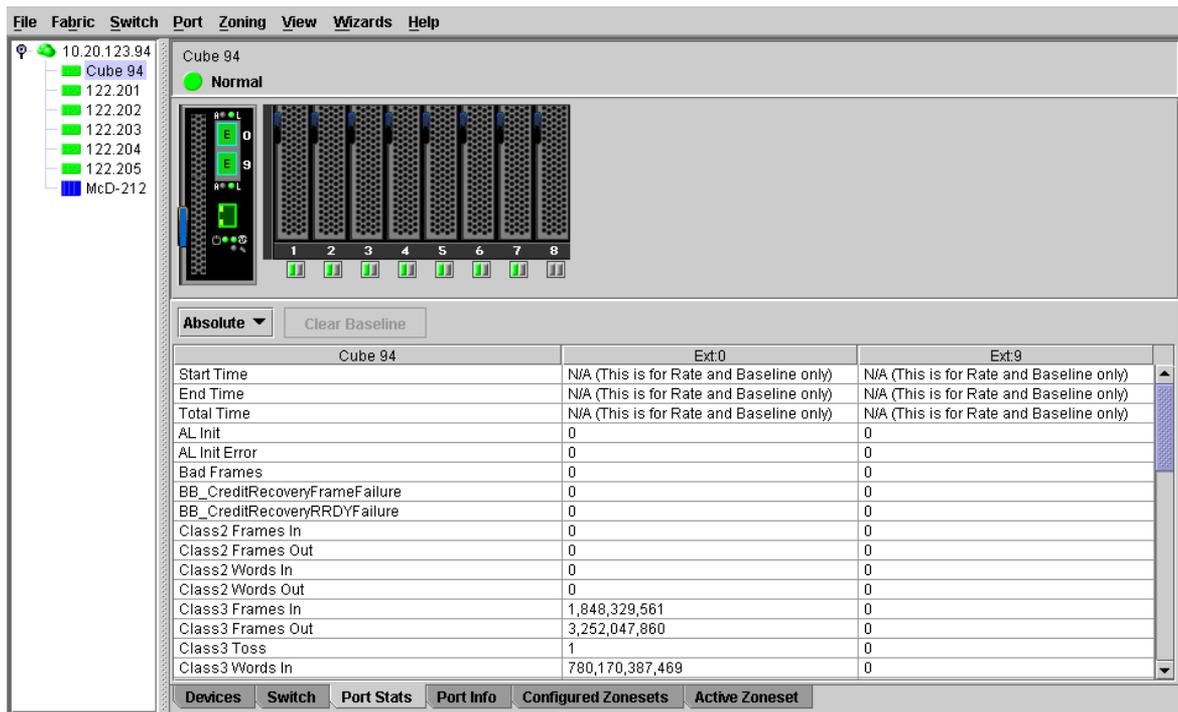
Figure 40 Port Statistics data window

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.

- 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.

Click **Clear Baseline** to set the current baseline when viewing baseline statistics. The baseline will also be set when the switch status changes from unreachable to reachable.

Table 18 describes the Port Statistics data window entries.

Table 18 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.

Table 18 Port statistics data window entries (Continued)

Entry	Description
BB_CreditRecoveryFrameFailure	Number of times more frames were lost during a credit recovery period than the recovery process could resolve. This causes a Link Reset to recover the credits.
BB_CreditRecoveryRRDYFailure	Number of times more R_RDYs were lost during a credit recovery period than the recovery process could resolve. This 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.
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 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 by 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 is used to reinitialize the loop. An L_port, identified by AL_PS, may have noticed a performance degradation and is trying to restore the loop.

Table 18 Port statistics data window entries (Continued)

Entry	Description
LIP(f7,f7)	A loop initialization primitive frame used to acquire 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.
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.
Primitive Sequence Errors	Number of bad primitives received by the port.
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.
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. Use the drop-down lists in the Port Properties dialog to change the following parameters:

- Port symbolic name, page 91
- Port states, page 92
- Port types, page 93
- Port speeds, page 94
- Port transceiver media status, page 94
- Device scan, page 94

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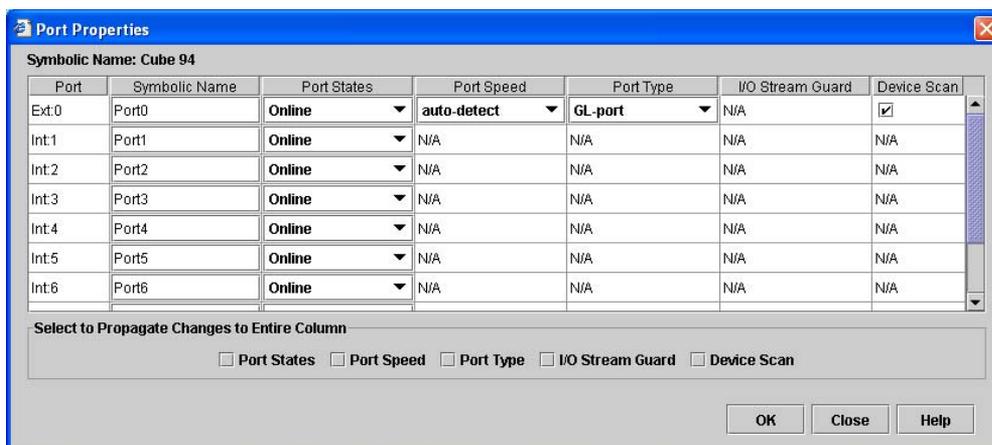
Figure 41 Port Properties dialog

NOTE: 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:

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

Port 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. Table 19 describes the port administrative and operational states.

- The configured administrative state is the state that is saved in the switch configuration and is preserved across switch resets. McDATA Web Server or Element Manager always makes changes to the configured administrative state.

- The current administrative state is the state that is applied to the port for temporary purposes and is not preserved across switch resets. The current administrative state is set using the Set Port command. Refer to the *McDATA 4Gb SAN Switch for HP p-Class BladeSystem command line interface guide* for more information.

To view the operational state select **View > View Port States.**

To change port administrative state:

1. Select one or more ports in the faceplate display.
2. Select **Port > Port Properties** to open the Port Properties dialog.
3. Select the option that corresponds to the port state you want.
4. Click **OK** to write the new port state to the switch.

Table 19   Port administrative and operational states

State	Description
Online (On)	Activates and prepares port to send data
Offline (Off)	Prevents port from receiving signal and accepting a device login
Diagnostics (Dia)	Prepares port for testing and prevents the port from accepting a device login
Down (Dn)	Disables the port
Inactive (Ia)	Port operational state is offline, but administrative state is online.
Isolated (Iso)	E_Port has lost its connection. Refer to Table 17 for information about why the E_Port has isolated.

Port types

The external ports can be configured to self-discover the proper type to match the device or switch to which it is connected. Table 20 lists the possible port types and their meanings.

> **NOTE:** Internal ports can be F_Port or FL_Port only. Port types for internal ports cannot be changed.

Select **View > View Port Types** to display port type status.

To change the port type for external ports:

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

Table 20 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 to another fibre channel switch.

Port speeds

External ports are capable of transmitting and receiving at 1-Gbps, 2-Gbps, or 4-Gbps. Internal ports are capable of transmitting and receiving at 1-Gbps or 2-Gbps. The ports can be configured for either transmission speed or to sense the transmission speed of the device to which it is connected. Table 21 lists the possible port speeds.

NOTE: The port speed of internal ports is pre-configured and cannot be changed.

Select **View > View Port Speeds** to display the speed of each port.

To change the port transmission speed for external ports:

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

Table 21 Port speeds

State	Description
Auto-Detect	Matches the transmission speed of the connected device. This is the default.
1Gbps	Sets the transmission speed to 1-Gbps.
2Gbps	Sets the transmission speed to 2-Gbps.
4Gbps	Sets the transmission speed to 4-Gbps (external ports only)

Port transceiver media status

Table 22 lists the port media states and their meanings for the two external ports. Select **View > View Port Media** to display transceiver media status.

Table 22 Port Transceiver media view

Media Icon	Description
	Optical SFP, online (green/black)
	Optical SFP, offline (gray/black)
	Copper SFP, online (green)
	Copper SFP, offline (gray)
None	Empty port; no transceiver installed (gray). This is normal for internal ports (1–8).

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.

Port binding

📝 **IMPORTANT:** Port binding is available only in Element Manager which requires the Element Manager PFE key. See "Installing Product Feature Enablement keys" on page 82 for more information about installing a PFE key. To obtain the McDATA 4Gb SAN Switch serial number and PFE key, follow the step-by-step instructions on the *firmware feature entitlement request certificate* for the PFE key. You can obtain a PFE key from the web at: www.webkey.external.hp.com.

Port binding ties one or more device WWNs to a physical port number. The port will accept logins only from the devices that are on the WWN list. To enable port binding for a port and specify device WWNs:

1. Select a single port on the faceplate display.
2. Select **Port > Port Binding to open the Port Binding dialog**.
3. Click the Port Binding checkbox to enable port binding.
4. Select each device WWN from the WWN: pull-down menu and click **Add**. To remove a WWN, select the WWN in the WWN List and click **Remove**.
5. Click **OK**.

Resetting a port

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

1. In the faceplate display, select the ports to be reset.
2. Select **Port > Reset Port**.
3. Click **OK** to reset the selected ports.

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 42 presents the following loopback tests:
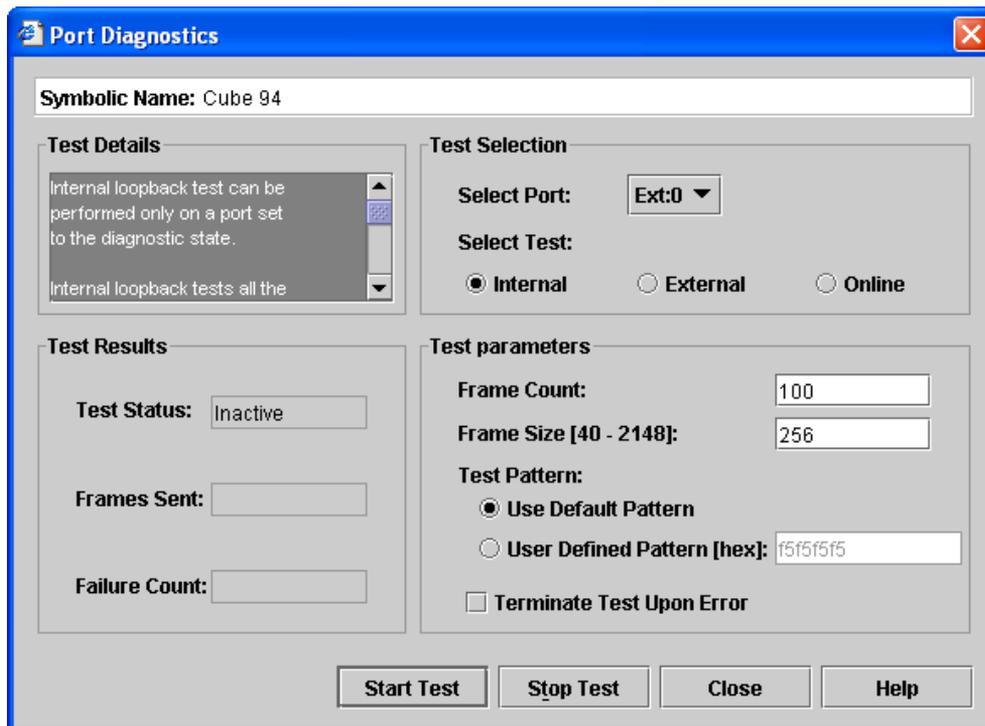
Figure 42 Port Diagnostics dialog

- **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.

To run the diagnostics tests on a port:

1. Select the port to be tested in the faceplate display.
2. Select **Port > Port Diagnostics**.
3. Select **Internal**, **External**, or **Online** in the Test Selection area.
4. Enter the frame count, frame size, and select a test pattern option. You can use the default pattern or enter an 8-digit pattern (hex). Select **Terminate Test Upon Error** for online test, if you want the test to stop should it encounter an error.
5. Click **Start Test** to begin the test. The Test Results area displays the test status, number of frames sent, and number of errors found.
6. To test another port, open the **Select Port** drop-down list and select another port (number) and test type (**Internal**, **External**, or **Online**) in the Test Selection area.
7. Click **Start Test** to begin the next test. Observe the results in the Test Results area.

Glossary

Active firmware	The firmware image on the switch that is in use
Active zone set	The zone set that defines the current zoning for the fabric
Activity LED	A port LED that indicates when frames are entering or leaving the port
Administrative state	State that determines the operating state of the port, I/O blade, or switch. The configured administrative state is stored in the switch configuration. The configured administrative state can be temporarily overridden using the CLI.
AL_PA	Arbitrated Loop Physical Address
Alarm	A message generated by the switch that specifically requests attention. Alarms are generated by several switch processes. Some alarms can be configured.
Arbitrated loop	An 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
Cascade topology	A fabric in which the switches are connected in series. If you connect the last switch back to the first switch, you create a cascade-with-a-loop topology.
CHAP	Challenge Handshake Authentication Protocol
Class 2 service	A service that multiplexes frames at frame boundaries to or from one or more N_Ports wit h 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.
DefaultZone	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 applies only when interop mode is set to McDATA Fabric Mode.
Device Security	A component of fabric security that provides for the authorization and authentication of devices that attach to a switch through the use of groups and security sets
Domain ID	User defined number that identifies the switch in the fabric
EFCM	Enterprise Fabric Connectivity Manager
Element Manager	Switch management application that is accessible through the High Availability Fabric Manager (HAFM).
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 database	The set of fabrics that have been opened during a McDATA Web Server session
Fabric management switch	The switch through which the fabric is managed (the switch connected to the Ethernet network)
Fabric name	User defined name associated with the file that contains user list data for the fabric
Fabric port	An F_Port

Fabric view file	A file containing a set of fabrics that were opened and saved during a previous McDATA Web Server session
Fan Fail LED	An LED that indicates that a cooling fan in the switch is operating below standard
Flash memory	Memory on the switch that contains the chassis control firmware
Force PROM mode	See Maintenance Mode
Frame	Data unit consisting of a start-of-frame (SOF) delimiter, header, data payload, CRC, and an end-of-frame (EOF) delimiter
FRU	Field Replaceable Unit
HAFM	High Availability Fabric Manager
Heartbeat LED	A chassis LED that indicates the status of the internal switch processor and the results of the Power-on Self Test
In-band management	The ability to manage a switch through an Fibre Channel port
Initiator	The device that initiates a data exchange with a target device
In-order-delivery	A feature that requires that frames be received in the same order in which they were sent
Interop mode	Permits interoperation with FC-SW-2 compliant (Standard/McDATA Open mode) switches and switches running in McDATA Fabric Mode (Interop_2 in CLI)
Inter-Switch Link (ISL)	The connection between two switches using E_Ports
IP	Internet Protocol
LIP	Loop Initialization Primitive sequence
Logged-in LED	A port LED that indicates device login or loop initialization status
Maintenance button	Formerly known as the Force PROM button. Momentary button on the switch used to reset the switch or place the switch in maintenance mode.
Maintenance mode	Formerly known as force PROM mode. Maintenance mode sets the IP address to 10.0.0.1 and provides access to the switch for maintenance purposes.
Management Information Base (MIB)	A set of guidelines and definitions for SNMP functions
Management workstation	PC workstation that manages the fabric through the fabric management switch
McDATA Web Server	Switch management application that resides on the switch and is accessible through an Internet browser.
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
N_Port	Node Port. An Fibre Channel device port in a point-to-point or fabric connection.
NL_Port	Node Loop Port. An Fibre Channel device port that supports arbitrated loop protocol.
Pending firmware	The firmware image that will be activated upon the next switch reset
PFE key	Product Feature Enablement key. A password that you can purchase from your switch distributor or authorized reseller to enable particular features in your switch
POST	Power-on Self Test
Power LED	A chassis LED that indicates that the switch logic circuitry is receiving proper DC voltages
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
Product Feature Enablement key	A password that you can purchase from your switch distributor or authorized reseller to enable particular features in your switch
SFP	Small Form-Factor Pluggable transceiver
Small Form-Factor Pluggable (SFP)	A transceiver device, smaller than a GigaBit Interface Converter, that plugs into the Fibre Channel port
SNMP	Simple Network Management Protocol
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	Zoning divides the fabric for purposes of controlling discovery. Members of the same zone automatically discover and communicate freely with all other members of the same zone.
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 and zones stored on a switch

Index