



Simplify

QLogic[®] 6-Port Enterprise Fibre Channel Switch Module

for IBM[®] eServer[™] BladeCenter[™]

Management Guide
Firmware Version 4.1.x



Information furnished in this manual is believed to be accurate and reliable. However, QLogic Corporation assumes no responsibility for its use, nor for any infringements of patents or other rights of third parties which may result from its use. QLogic Corporation reserves the right to change product specifications at any time without notice. Applications described in this document for any of these products are for illustrative purposes only. QLogic Corporation makes no representation nor warranty that such applications are suitable for the specified use without further testing or modification. QLogic Corporation assumes no responsibility for any errors that may appear in this document.

QLogic and SANbox are trademarks or registered trademarks of QLogic Corporation.

AIX, IBM, eServer, and BladeCenter are trademarks or registered trademarks of International Business Machines Corporation.

Linux is a registered trademark of Linus Torvalds.

Microsoft, Windows NT, Windows 2000, Windows 2003, and Internet Explorer are trademarks of Microsoft Corporation.

Netware is a registered trademark of Novell Inc.

Red Hat is a registered trademark of Red Hat Software Inc.

S.u.S.E is a registered trademark of S.u.S.E. Gesellschaft für Software-und Systementwicklung mbH CORPORATION FED REP GERMANY.

All other brand and product names are trademarks or registered trademarks of their respective owners.

Document Revision History

Revision A, Release, August, 2004

Table of Contents

Section 1	Introduction	
1.1	License Agreement for QLogic Applications	1-2
1.2	Technical Support.....	1-4
Section 2	Command Line Interface (CLI)	
2.1	Logging On to a Switch Module	2-1
2.2	Working with Switch Module Configurations	2-2
2.2.1	Modifying a Switch Module Configuration	2-2
2.2.2	Backing up and Restoring Switch Module Configurations.....	2-4
2.3	Command Syntax.....	2-6
2.4	Commands.....	2-7
	Admin Command.....	2-8
	Alias Command	2-9
	Config Command.....	2-11
	Date Command	2-13
	Fallback Command.....	2-14
	Hardreset Command	2-15
	Help Command.....	2-16
	History Command.....	2-17
	Hotreset Command	2-18
	Image Command	2-20
	Lip Command (for external ports only)	2-21
	Passwd Command	2-22
	Ping Command.....	2-23
	Ps Command.....	2-24
	Quit Command	2-25
	Reset Command.....	2-26
	Set Command.....	2-33
	Set Config Command	2-35
	Set Log Command.....	2-47
	Set Port Command	2-50
	Set Setup Command	2-52
	Show Command.....	2-58
	Show Config Command.....	2-71
	Show Log Command	2-75
	Show Perf Command	2-78

Show Setup Command.....	2-81
Shutdown Command	2-84
Test Command	2-85
Uptime Command.....	2-88
User Command	2-89
Whoami Command.....	2-92
Zone Command.....	2-93
Zoneset Command	2-97
Zoning Command.....	2-99

Section 3 Using SAN Utility

3.1	Fabric Management Workstation	3-1
3.2	SAN Browser.....	3-2
3.3	SAN Utility User Interface.....	3-2
3.3.1	Menu Bars	3-5
3.3.1.1	Topology Window Menu	3-5
3.3.1.2	Faceplate Window Menu	3-6
3.3.1.3	Topology Window Shortcut Keys	3-7
3.3.1.4	Faceplate Window Shortcut Keys.....	3-8
3.3.2	Tool Bar	3-9
3.3.3	Fabric Tree	3-10
3.3.4	Graphic Window	3-11
3.3.5	Data Window and Tabs.....	3-11
3.3.6	Working Status Indicator.....	3-11
3.3.7	Using the Topology Window	3-12
3.3.7.1	Fibre Channel Switch Module and Link Status	3-13
3.3.7.2	Working with Switch Modules and Links.....	3-13
3.3.8	Using the Faceplate Window.....	3-15
3.3.8.1	Port Views and Status.....	3-16
3.3.8.2	Working with Ports.....	3-17
3.3.8.3	Faceplate Data Window Tabs.....	3-17
3.4	Configuring the SAN Utility Environment.....	3-18
3.4.1	Working with Fabric View Files.....	3-18
3.4.1.1	Saving a Fabric View File	3-18
3.4.1.2	Opening a Fabric View File.....	3-18
3.4.1.3	Changing the Encryption Key for the Default Fabric View File	3-19
3.4.2	Setting SAN Utility Preferences.....	3-19
3.5	Managing Fabrics.....	3-21
3.5.1	Securing a Fabric	3-21
3.5.1.1	User Account Security	3-21

3.5.1.2	Fabric Services	3-22
3.5.2	Tracking Fabric Version Information	3-23
3.5.2.1	Saving a Version Snapshot.....	3-23
3.5.2.2	Viewing and Comparing Version Snapshots.....	3-24
3.5.2.3	Exporting Version Snapshots to a File.....	3-24
3.5.3	Managing the Fabric Database	3-25
3.5.3.1	Adding a Fabric	3-25
3.5.3.2	Removing a Fabric	3-26
3.5.3.3	Rediscovering a Fabric.....	3-26
3.5.3.4	Adding a New Switch Module to a Fabric.....	3-27
3.5.3.5	Replacing a Failed Switch Module in a Fabric.....	3-28
3.5.3.6	Deleting Switches and Links from the Topology Window	3-28
3.5.4	Displaying Fabric Information	3-29
3.5.4.1	Fabric Status.....	3-29
3.5.4.2	Displaying the Event Browser.....	3-31
3.5.4.3	Devices Data Window.....	3-35
3.5.4.4	Active Zone Set Data Window	3-36
3.5.5	Working with Device Information and Nicknames	3-37
3.5.5.1	Displaying Detailed Device Information	3-37
3.5.5.2	Exporting Device Information to a File.....	3-38
3.5.5.3	Managing Device Port Nicknames	3-38
3.5.6	Zoning a Fabric.....	3-40
3.5.6.1	Zoning Concepts.....	3-41
3.5.6.2	Using the Zoning Wizard	3-44
3.5.6.3	Managing the Zoning Database.....	3-45
3.5.6.4	Managing Zone Sets.....	3-50
3.5.6.5	Managing Zones	3-53
3.5.6.6	Managing Aliases	3-56
3.5.6.7	Merging Fabrics and Zoning.....	3-58
3.6	Managing Switch Modules	3-60
3.6.1	Managing User Accounts	3-61
3.6.1.1	Creating User Accounts.....	3-62
3.6.1.2	Removing a User Account.....	3-63
3.6.1.3	Changing a User Account Password.....	3-64
3.6.1.4	Modifying a User Account.....	3-65
3.6.2	Displaying Switch Module Information.....	3-66
3.6.2.1	Hardware Status	3-67
3.6.2.2	Devices Data Window.....	3-68
3.6.2.3	Switch Data Window.....	3-68

3.6.2.4	Link Data Window.....	3-71
3.6.2.5	Port Statistics Data Window.....	3-71
3.6.2.6	Port Information Data Window.....	3-72
3.6.2.7	Configured Zonesets Data Window.....	3-72
3.6.3	Configuring Port Threshold Alarms.....	3-73
3.6.4	Paging a Switch Module.....	3-74
3.6.5	Setting the Date/Time and Enabling NTP Client.....	3-75
3.6.6	Setting Temperature Thresholds.....	3-75
3.6.7	Resetting a Switch Module.....	3-76
3.6.8	Configuring a Switch Module.....	3-77
3.6.8.1	Using the Configuration Wizard.....	3-78
3.6.8.2	Switch Properties.....	3-78
3.6.8.3	Network Properties.....	3-84
3.6.9	Archiving a Switch Module Configuration.....	3-86
3.6.10	Restoring a Switch Module Configuration.....	3-87
3.6.11	Restoring the Factory Default Configuration.....	3-89
3.6.12	Managing Firmware.....	3-91
3.6.12.1	Installing Firmware.....	3-91
3.6.12.2	Activating the Pending Firmware.....	3-92
3.6.12.3	Changing the Pending Firmware.....	3-92
3.7	Managing Ports.....	3-93
3.7.1	Displaying Port Information.....	3-93
3.7.1.1	Monitoring Port Status.....	3-94
3.7.1.2	Displaying Port Types.....	3-95
3.7.1.3	Displaying Port Operational States.....	3-96
3.7.1.4	Displaying Port Speeds.....	3-96
3.7.1.5	Displaying Transceiver Media Status.....	3-97
3.7.1.6	Port Graphing and SAN Utility Performance View Application.....	3-97
3.7.1.7	Port Statistics Data Window.....	3-97
3.7.1.8	Port Information Data Window.....	3-101
3.7.2	Configuring Ports.....	3-103
3.7.2.1	Changing Port Administrative States.....	3-104
3.7.2.2	Changing Port Speeds (External Ports Only).....	3-105
3.7.2.3	Changing Port Types (External Ports Only).....	3-106
3.7.2.4	Changing I/O Stream Guard (External Ports Only).....	3-106
3.7.2.5	Changing Device Scan (External Ports Only).....	3-107
3.7.2.6	Changing Port Symbolic Name (External Ports Only).....	3-107
3.7.3	Resetting a Port.....	3-107

Section 4 Switch Module Utility Functions

4.1	LED Diagnostics.....	4-1
4.2	Testing Ports.....	4-3
4.3	Switch Module Monitoring Using SNMP.....	4-5
4.3.1	SNMP Configuration.....	4-6
4.3.2	SNMP Trap Configuration	4-7
4.4	Using the SAN Utility Performance View Application	4-8
4.4.1	Starting SAN Utility Performance View	4-9
4.4.2	Exiting SAN Utility Performance View	4-9
4.4.3	Saving and Opening Performance View Files	4-10
4.4.4	Changing the Default Performance View File Encryption Key	4-11
4.4.5	Setting SAN Utility Performance View Preferences	4-11
4.4.5.1	Setting the Polling Frequency.....	4-12
4.4.5.2	Displaying Graphs	4-12
4.4.6	Printing Graphs.....	4-15
4.4.7	Saving Graph Statistics to a File.....	4-15

Appendix A Mapping Port Locations and Software Numbering

A.1	Port Mapping.....	A-1
-----	-------------------	-----

Index

Figures

Figure		Page
3-1	Topology Window.....	3-3
3-2	BladeCenter Faceplate Window.....	3-4
3-3	BladeCenter T Faceplate Window	3-4
3-4	Topology Window Menu.....	3-5
3-5	Faceplate Window Menu.....	3-6
3-6	Fabric Tree.....	3-10
3-7	Topology Window.....	3-12
3-8	Faceplate Window.....	3-16
3-9	Preferences Window – SAN Utility.....	3-20
3-10	Fabric Version Snapshot Analysis Window.....	3-23
3-11	Add a New Fabric Window.....	3-25
3-12	Events Browser.....	3-32
3-13	Filter Events Window	3-34
3-14	Active Zone Set Data Window	3-36
3-15	Detailed Devices Display Window.....	3-37
3-16	Edit Zoning Window	3-45
3-17	Zoning Config Window.....	3-48
3-18	User Account Administration Window – Add Account.....	3-62



3-19	User Account Administration Window – Remove Account.....	3-63
3-20	User Account Administration Window – Change Password.....	3-64
3-21	User Account Administration Window - Modify Account	3-65
3-22	Faceplate Window - Switch Information.....	3-66
3-23	Hardware Status LEDs.....	3-67
3-24	Configured Zonesets Data Window	3-72
3-25	Port Threshold Alarm Configuration Window	3-73
3-26	Port Threshold Alarm Example	3-74
3-27	Temperature Thresholds Window	3-75
3-28	Switch Properties Window	3-78
3-29	Network Properties Window.....	3-84
3-30	Restore Windows – Full and Selective.....	3-87
3-31	BladeCenter Faceplate Window – Port Information	3-93
3-32	BladeCenter T Faceplate Window – Port Information.....	3-94
3-33	External Port Properties Window	3-103
3-34	Internal Properties Window	3-104
4-1	Switch Module LEDs.....	4-2
4-2	Port Loopback Test Window	4-4
4-3	SNMP Properties Window.....	4-5
4-4	Fabric View Graphs.....	4-8
4-5	Save Default Performance View File Dialog	4-9
4-6	Load Default View File Dialog	4-10
4-7	Preferences – SAN Utility Performance View	4-11
4-8	Default Graph Options Dialog	4-13

Tables

Table	Page	
2-1	Command-Line Completion	2-6
2-2	Commands Listed by Authority Level.....	2-7
2-3	Switch Module Configuration Defaults	2-27
2-4	Port Configuration Defaults	2-27
2-5	Port Threshold Alarm Configuration Defaults.....	2-29
2-6	Zoning Configuration Defaults.....	2-29
2-7	SNMP Configuration Defaults	2-30
2-8	System Configuration Defaults.....	2-31
2-9	Set Config Port Parameters	2-36
2-10	Set Config Switch Parameters	2-38
2-11	Set Config Threshold Parameters.....	2-41
2-12	Set Config Zoning Parameters.....	2-42
2-13	SNMP Configuration Settings	2-52
2-14	System Configuration Settings.....	2-53
2-15	Show Port Parameters	2-60
2-16	Switch Module Operational Parameters.....	2-64
2-17	Zoning Database Limits	2-100
3-1	Management Workstation Requirements.....	3-1

3-2	Topology Window Menu Shortcut Keys	3-7
3-3	Faceplate Window Shortcut Keys	3-8
3-4	Tool Bar Buttons	3-9
3-5	Fibre Channel Switch Module and Link Status Indicators.....	3-13
3-6	Topology Window Switch and Status Icons	3-30
3-7	Severity Levels.....	3-32
3-8	Devices Data Window Entries.....	3-35
3-9	Edit Zoning Window Tool Bar Buttons and Icons.....	3-47
3-10	Factory User Accounts.....	3-61
3-11	Switch Data Window Entries	3-68
3-12	Switch Module Resets.....	3-77
3-13	Switch Module Administrative States	3-80
3-14	Timeout Values	3-83
3-15	IP Configuration Parameters.....	3-85
3-16	Factory Default Configuration Settings	3-89
3-17	Port Types.....	3-95
3-18	Port Operational States.....	3-96
3-19	Port Speeds	3-96
3-20	Port Transceiver Media View	3-97
3-21	Port Statistics Data Window Entries.....	3-98
3-22	Port Information Data Window Entries	3-101
3-23	Port Administrative States.....	3-105
3-24	Port Speeds	3-105
3-25	Port Types.....	3-106
4-1	SNMP Configuration Parameters.....	4-6
4-2	SNMP Trap Configuration Parameters	4-7
A-1	Port Mapping For Server Units.....	A-1



Notes

Section 1

Introduction

You can manage and configure your QLogic 6-Port Enterprise Fibre Channel Switch Module through a Telnet connection to the embedded command line interface (CLI) or by using the SAN Utility application. The SAN Utility application provides an intuitive graphical user interface (GUI) that you can use to configure multiple Fibre Channel Switch modules through other connected SAN devices from a single interface. The SAN Utility application is referred to throughout this document as SAN Utility. The QLogic 6-Port Enterprise Fibre Channel Switch Module is also referred to throughout this document as the 6-port Switch Module. The IBM eserver BladeCenter and IBM eserver BladeCenter T units are also referred to throughout this document as the BladeCenter unit.

This Management Guide provides instructions to:

- Configure your 6-port Switch Module
- Manage fabrics, ports, and 6-port Switch Modules
- Use Telnet and the CLI to configure 6-port Switch Module parameters

You can manage the fabric through an Ethernet network using the SAN Utility or the CLI. The SAN Utility is installed on a Microsoft® Windows® 2000, Microsoft Windows 2003, Red Hat® Linux®, or S.u.S.E® Linux, Netware, or AIX® network management workstation.

The 6-port Switch Module has an embedded Telnet server through which a Telnet client can connect and manage the 6-port Switch Module using the CLI. See [Section 2 Command Line Interface \(CLI\)](#) for more information about Telnet and CLI commands.

SNMP provides monitoring and trap functions for the fabric. The 6-port Switch Module firmware supports SNMP Versions 1 and 2; the Fibre Alliance Management Information Base (FA-MIB) version 4.0; and the Fabric Element Management Information Base (FE-MIB) RFC 2837. Traps are formatted using SNMP version 2.

If you are an experienced user, you can use the Telnet CLI to perform the following tasks:

- Manage the 6-port Switch Module from your server management module interface to the Telnet client
- Perform single 6-port Switch Module management
- Use advanced control commands

If you are a new user or if you need to manage multiple 6-port Switch Modules from a single interface, you can use the SAN Utility to perform the following tasks:

- Manage your 6-port Switch Module from a remote client or network management workstation
- Manage your multiswitch fabric

For information about installing the 6-port Switch Module, see the *QLogic 6-Port Enterprise Fibre Channel Switch Module for IBM Eserver BladeCenter Installation Guide*.

1.1 License Agreement for QLogic Applications

All QLogic software in object code format that is available from QLogic Corporation is the property of QLogic and is intended to be used ONLY with manufactured by or for QLogic and OEM implementation approved by QLogic and associated QLogic driver software.

ANY OTHER USE OF THIS SOFTWARE MAY CAUSE UNFORSEEABLE PROBLEMS INCLUDING DATA ERRORS. QLOGIC DISCLAIMS ANY AND ALL LIABILITY, RESPONSIBILITY OR OBLIGATION FOR ANY LOSS OR DAMAGE RESULTING FROM SUCH USE.

If your product implementation was not manufactured by QLogic or does not meet the above requirements, please contact the manufacturer for software, drivers, utilities and ongoing support.

1. INTRODUCTION This agreement is for software in object or bit code format that is available from QLogic Corporation ("QLogic"). After you agree to the terms and conditions of this Agreement, you will be allowed to install and use the SAN Utility with the applicable QLogic products. This agreement is not a transfer of rights, title or interest between QLogic and you. Instead, this Agreement is a license that grants to you certain rights below.
2. REPRESENTATION If you are an employee or agent, you represent and warrant that you have adequate legal capacity to enter into this Agreement on behalf of your employer or principal such that, your employer or principal is bound by the terms and conditions of this agreement.

3. **LICENSE** You may copy the software modules in object or bit form. Your may use each software module only with the associated QLogic hardware. Besides the copy of the software module necessary to operate that associated QLogic hardware, you may make only one additional copy for archive purposes. You may not modify, adapt, translate, reverse engineer, decompile, disassemble otherwise attempt to discern the source code if the software modules. You may not sublicense or transfer the software module to any third party. You must reproduce each software module in its entirety and without modification, including any and all copyright notices, serial number and any other QLogic legend or notice on any copy. Each software module contains or embodies proprietary intellectual property of QLogic or its licensors. The structure, organization or code are valuable trade secrets of Logic or its licensors. QLogic and/or its licensors do not grant, convey or license to you any rights under any patents, copyrights or any other intellectual property except as specifically granted herein.
4. **WARRANTY** EACH SOFTWARE MODULE IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BY NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT OF THIRD PARTY RIGHTS AND FITNESS FOR A PARTICULAR PURPOSE. QLOGIC MAKES NO REPRESENTATIONS THAT ANY SOFTWARE MODULE COMPLIES WITH THE APPLICABLE STATUS, LAWS OR REGULATIONS. The entire risk as to the quality and performance of the software module is with you. Should the software module prove defective, you (and not QLogic's distributors or any licensor of QLogic) assume the entire cost of all necessary servicing, repair or correction. There is no warranty by QLogic to any other party or person that the functions contained in the software module will be uninterrupted or error free. You assume all responsibility for the selection of the software module to achieve your intended results, and for the installation, use and results obtained from the software module.
5. **LIMITATION OF LIABILITY** IN NO EVENT WILL QLOGIC BE LIABLE TO YOU OR ANY OTHER PARTY FOR ANY DIRECT OR INDIRECT DAMAGES, INCLUDING LOST PROFITS, LOST SAVINGS OR OTHER INCIDENTS OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE DRIVER/UTILITY EVEN IF QLOGIC OR THE OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
6. **APPLICABLE LAW** This Agreement will be governed by the laws of the State of California. You agree not to export or re-export the software modules in violation of the export control laws of the United States and other foreign countries.

7. **GENERAL PROVISIONS** If any term or condition of this Agreement is held void or unenforceable by a competent court, all the other terms and conditions shall survive. This Agreement shall terminate immediately if you breach any of its terms and conditions. You agree and are solely responsible to ensure that your use of the software modules will not violate any law or treaties of any state or country.
8. **ENTIRE AGREEMENT** This Agreement sets forth the entire agreement and understanding between you and QLogic with respect to the subject matter hereof and supersedes and cancels all previous negotiations, agreements, commitments, and writings in respect to the subject matter hereof. Modifications to this Agreement can be made only in writing that is executed by both QLogic and you.

1.2

Technical Support

Customers should contact their authorized maintenance provider for technical support of their QLogic switch products. QLogic-direct customers may contact QLogic Technical Support; others will be redirected to their authorized maintenance provider.

Section 2

Command Line Interface (CLI)

Your QLogic 6-Port Enterprise Fibre Channel Switch Module contains an embedded Telnet server. This server enables a Telnet client to establish a Telnet session with the 6-port Switch Module to retrieve information or to configure parameters using the CLI. You can use the CLI to perform a variety of fabric and switch management tasks through an Ethernet connection to your server unit.

You can access the Telnet interface in two ways:

- Using your server management interface
- From a command-line window on a connected network management workstation

Note: Before you configure your 6-port Switch Module, be sure that the management modules in your server unit are properly configured. In addition, to access and manage your 6-port Switch Module from an external environment, you might need to enable certain features, such as the external ports and external management over all ports. For more detailed information about configuring your management module, see your server Installation Guide.

2.1

Logging On to a Switch Module

To log on to a 6-port Switch Module using Telnet, complete the following steps:

Note: The IP addresses in the following step are the default IP address of the 6-port Switch Modules; if new IP addresses have been assigned to the I/O modules, use these instead.

1. Open a command-line window on the network management workstation, type one of the following commands, and press Enter.

For I/O-module bay 3:

```
telnet 192.168.70.129
```

For I/O-module bay 4:

```
telnet 192.168.70.130
```

A command prompt window opens.

2. At the Login prompt, type the initial default user account, `USERID`. At the Password prompt, type the initial default password, `PASSWORD` (the sixth character is a zero, not the letter O). The user account and password are case sensitive.

This user account provides full access to the switch module and its configuration. After planning your fabric management needs and creating your own user accounts, consider changing the password for this account. Refer to ["Command Syntax" on page 2-6](#) for more information about authority levels. See the ["User Command" on page 2-89](#) for information about creating user accounts.

Note: The 6-port Switch Module supports a combined maximum of 19 logins or sessions reserved as follows:

- 4 logins or sessions for internal applications such as management server and SNMP
- 9 high priority Telnet sessions
- 6 logins or sessions for SAN Utility inband and out-of-band logins, Application Programming Interface (API) inband and out-of-band logins, and Telnet logins.

2.2

Working with Switch Module Configurations

Successful management of switch modules and fabrics with the command line interface depends on the effective use of switch module configurations. Modifying configurations, backing up configurations, and restoring configurations are key switch management tasks.

2.2.1

Modifying a Switch Module Configuration

A 6-port Switch Module supports up to 10 configurations including the default configuration. Each configuration contains switch module, port, port threshold alarm, and zoning configuration components.

The Show Switch command displays the name of the active configuration. A configuration name can have up to 31 characters excluding the pound symbol (#), semicolon (;), and comma (,). By editing the latest configuration and saving the results under a new name, you can create a history of configuration changes. Use

the Config List command to display the names of the configurations stored on the switch

```
FCSM6: user1> config list
Current list of configurations
-----
default
config_10132003
```

To modify a switch module configuration you must open an Admin session with the Admin Start command. An Admin session prevents other accounts from making changes at the same time either through Telnet or SAN Utility. You must also open a Config Edit session with the Config Edit command and indicate which configuration you want to modify. If you do not specify a configuration name the active configuration is assumed. The Config Edit session provides access to the Set Config commands with which you make modifications to the port, switch module, port threshold alarm, or zoning configuration components as shown:

```
FCSM6: user1> admin start
FCSM6 (admin): user1> config edit default
The config named default is being edited.
FCSM6 (admin-config): user1> set config port . . .
FCSM6 (admin-config): user1> set config switch . . .
FCSM6 (admin-config): user1> set config threshold . . .
FCSM6 (admin-config): user1> set config zoning . . .
```

The Config Save command saves the changes you made during the Config Edit session. In this case, changes to the configuration named *Default* are being saved to a new configuration named *config_10132003*. However, the new configuration does not take effect until you activate it with the Config Activate command as shown:

```
FCSM6 (admin-config): user1> config save config_10132003
FCSM6 (admin-config): user1> config activate config_10132003
FCSM6 (admin-config): user1> admin end
FCSM6: user1>
```

The Admin End command releases the Admin session for other administrators when you are done making changes to the switch module.

2.2.2

Backing up and Restoring Switch Module Configurations

Backing up and restoring a switch module configuration is useful to protect your work or for use as a template in configuring other switch modules. The Config Backup command creates a temporary file on the switch module named *configdata*. This file can be used to restore a switch module only with the command line interface; it cannot be used to restore a 6-port Switch Module using SAN Utility.

```
FCSM6: user1> admin start
FCSM6 (admin): user1> config backup
```

The *configdata* file contains all of the switch module configuration information including the following:

- All named switch module configurations including the default configuration. This includes port, switch, port threshold alarm, and zoning configuration components.
- All SNMP and network information defined with the Set Setup command.
- The zoning database included all zone sets, zones, and aliases

You use FTP to download the *configdata* file to your workstation for safe keeping and to upload the file back to the switch module for the restore function. To download the *configdata* file, open an FTP session on the switch and log in with the account name *images* and password *images*. Transfer the file in binary mode with the Get command as shown:

```
>ftp ip_address
user:images
password: images

ftp>bin
ftp>get configdata
xxxxx bytes sent in xx secs.
ftp>quit
```

You should rename the *configdata* file on your workstation with the switch module name and date, *config_switch_169_10112003*, for example.

The restore operation begins with FTP to upload the configuration file from the workstation to the switch module, then finishes with a Telnet session and the Config Restore command. To upload the configuration file, *config_switch_169_10112003* in this case, open an FTP session with account name *images* and password *images*. Transfer the file in binary mode with the Put command as shown:

```
ftp ip_address
user:images
password: images
ftp> bin
ftp> put config_switch_169_10112003 configdata
ftp>quit
```

The restore process replaces all configuration information on the switch module and afterwards the switch module is automatically reset. If the restore process changes the IP address, all management sessions are terminated. Use the Set Setup System command to return the IP configuration to the values you want. Refer to the ["Set Setup Command" on page 2-52](#). To restore the switch module, open a Telnet session, then enter the Config Restore command from within an Admin session as shown:

```
FCSM6: user1> admin start
FCSM6 (admin): user1> config restore
The switch will be reset after restoring the configuration.
Please confirm (y/n): [n] y
```

2.3 Command Syntax

The command syntax is as follows:

```
command  
  keyword  
  keyword [value]  
  keyword [value1] [value2]
```

The command is followed by one or more keywords. Consider the following rules and conventions:

- Commands and keywords are case insensitive.
- Required keyword values appear in standard font: [value]. Optional values are shown in italics: *[value]*.
- The underlined portion of each keyword indicates the abbreviated form that can be used. For example the Delete keyword can be abbreviated Del.

The command-line completion feature makes entering and repeating commands easier. [Table 2-1](#) describes the command-line completion keystrokes.

Table 2-1. Command-Line Completion

Keystroke	Effect
Tab	Completes the command line. Enter at least one character and press the tab key to complete the command line. If more than one possibility exists, press the Tab key again to display all possibilities.
Up Arrow	Scrolls backward through the list of previously entered commands.
Down Arrow	Scrolls forward through the list of previously entered commands.
Control-A	Moves the cursor to the beginning of the command line
Control-E	Moves the cursor to the end of the command line.

2.4 Commands

The command set performs monitoring and configuration tasks. Commands related to monitoring tasks are available to all account names. Commands related to configuration tasks are available only within an admin session. An account must have Admin authority to enter the Admin Start command, which opens an admin session. Refer to the "[Admin Command](#)" on page 2-8.

The commands and their page numbers are listed in [Table 2-2](#).

Table 2-2. Commands Listed by Authority Level

Monitoring Commands	Configuration Command	
Help (2-16)	Admin (2-8)	
History (2-17)	Admin Session Commands	
Ping (2-23)		
Ps (2-24)		
Quit (2-25)		
Show (2-58)		
Show Config (2-71)		
Show Log (2-75)		
Show Perf (2-78)		
Show Setup (2-81)		
Uptime (2-88)		
Whoami (2-92)		
		Alias ¹ (2-9)
		Config ¹ (2-11)
	Date ¹ (2-13)	
	Fallback (2-14)	
	Hardreset (2-15)	
	Hotreset (2-18)	
	Image (2-20)	
	Lip (2-21)	
	Passwd (2-22)	
	Reset (2-26)	
	Set ¹ (2-33)	
	Set Config (2-35)	
	Set Log (2-47)	
	Set Port ¹ (2-50)	
	Set Setup (2-52)	
	Shutdown (2-84)	
	Test (2-85)	
	User ¹ ² (2-89)	
	Zone ¹ (2-93)	
	Zoneset ¹ (2-97)	
	Zoning ¹ (2-99)	

¹Some keywords do not require an Admin session.

² Some keywords can be executed only by the USERID account name.

Admin Command

Opens and closes an Admin session. The Admin session provides commands that change the fabric and switch module configurations. Only one Admin session can be open on the switch module at any time. An inactive Admin session will time out after a period of time which can be changed using the Set Setup System command. Refer to the ["Set Setup Command" on page 2-52](#).

Authority Admin

Syntax **admin**
start (or begin)
end (or stop)
cancel

Keywords **start (or begin)**
Opens the admin session.

end (or stop)
Closes the admin session. The Hardreset, Hotreset, Logout, Shutdown, and Reset Switch commands will also end an admin session.

cancel
Terminates an Admin session opened by another user. Use this keyword with care because it terminates the Admin session without warning the other user and without saving pending changes.

Notes Closing a Telnet window during an admin session does not release the session. In this case, you must either wait for the admin session to time out, or use the Admin Cancel command.

Examples The following example shows how to open and close an Admin session:

```
FCSM6: user1> admin start
```

```
FCSM6 (admin):user1>
```

```
FCSM6 (admin): user1> admin end
```

```
FCSM6: user1>
```

Alias Command

Creates a named set of ports/devices. Aliases make it easier to assign a set of ports/devices to many zones. An alias can not have a zone or another alias as a member.

Authority Admin session and a Zoning Edit session. Refer to the ["Zoning Command" on page 2-99](#) for information about starting a Zoning Edit session. The List and Members keywords do not require an Admin nor a Zoning Edit session.

Syntax **alias**

- add [alias] [member_list]
- copy [alias_source] [alias_destination]
- create [alias]
- delete [alias]
- list
- members [alias]
- remove [alias] [member_list]
- rename [alias_old] [alias_new]

Keywords **add [alias] [member_list]**

Specifies one or more ports/devices given by [member_list] to add to the alias named [alias]. Use a <space> to delimit ports/devices in [member_list]. An alias can have a maximum of 2000 members. A port/device in [member_list] can have any of the following formats:

- Domain ID and port number pair (Domain ID, Port Number). Domain IDs can be 1–239; port numbers can be 0–255.
- 6-character hexadecimal device Fibre Channel address (hex)
- 16-character hexadecimal worldwide port name (WWPN) with the format xx:xx:xx:xx:xx:xx:xx:xx.

The application verifies that the [alias] format is correct, but does not validate that such a port/device exists.

copy [alias_source] [alias_destination]

Creates a new alias named [alias_destination] and copies the membership into it from the alias given by [alias_source].

create [alias]

Creates an alias with the name given by [alias]. An alias name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, \$, ^, and -. The zoning database supports a maximum of 256 aliases.

delete [alias]

Deletes the specified alias given by [alias] from the zoning database. If the alias is a member of the active zone set, the alias will not be removed from the active zone set until the active zone set is deactivated.

list

Displays a list of all aliases. This keyword does not require an Admin session nor a Zoning Edit session.

members [alias]

Displays all members of the alias given by [alias]. This keyword does not require an Admin session nor a Zoning Edit session.

remove [alias] [member_list]

Removes the ports/devices given by [member_list] from the alias given by [alias]. Use a <space> to delimit ports/devices in [member_list]. A port/device in [member_list] can have any of the following formats:

- Domain ID and port number pair (Domain ID, Port Number). Domain IDs can be 1–239; port numbers can be 0–255.
- 6-character hexadecimal device Fibre Channel address (hex)
- 16-character hexadecimal worldwide port name (WWPN) for the device with the format xx:xx:xx:xx:xx:xx:xx:xx.

rename [alias_old] [alias_new]

Renames the alias given by [alias_old] to the alias given by [alias_new].

Examples

The following is an example of the Alias Create command:

```
FCSM6: user1> admin start
FCSM6 (admin): user1> zoning edit
FCSM6 (admin-zoning): user1> alias create reserve
```

The following is an example of an Alias Members command:

```
FCSM6: user1> alias members reserve
Current list of members for Zone Alias: reserve
-----
10:00:00:00:00:10:12:79
10:00:00:00:00:10:12:80
10:00:00:00:00:10:12:81
10:00:00:00:00:10:12:82
```


Config Command

Manages the 6-port Switch Module configurations. For information about setting the port and 6-port Switch Module configurations, refer to the ["Set Config Command" on page 2-35](#).

Authority Admin session for all keywords except List. The Cancel keyword requires an Admin session and a Config Edit session.

Syntax

```
config  
  activate [config_name]  
  backup  
  cancel  
  copy [config_source] [config_destination]  
  delete [config_name]  
  edit [config_name]  
  list  
  restore  
  save [config_name]
```

Keywords **activate [config_name]**
Activates the configuration given by [config_name]. If you omit [config_name], the currently active configuration is used. Only one configuration can be active at a time.

backup
Creates a file named *configdata*, which contains the system configuration information. To download this file, open an FTP session, log in with account name/password of "images" for both, and type "get configdata". Refer to ["Backing up and Restoring Switch Module Configurations" on page 2-4](#).

cancel
Terminates the current configuration edit session without saving changes that were made. This keyword requires an Admin session and a Config Edit session.

copy [config_source] [config_destination]
Copies the configuration given by [config_source] to the configuration given by [config_destination]. The 6-port Switch Module supports up to 10 configurations including the default configuration.

delete [config_name]
Deletes the configuration given by [config_name] from the 6-port Switch Module.

edit [config_name]
Opens an edit session for the configuration given by [config_name]. If you omit [config_name], the currently active configuration is used.

list
Displays a list of all available configurations on the 6-port Switch Module. This keyword does not require an admin session.

restore

Restores configuration settings to an out-of-band 6-port Switch Module from a backup file named *configdata*, which must be first uploaded on the 6-port Switch Module using FTP. You create the backup file using the Config Backup command. Use FTP to load the backup file on a 6-port Switch Module, then enter the Config Restore command. After the restore is complete, the 6-port Switch Module automatically resets. Refer to ["Backing up and Restoring Switch Module Configurations"](#) on page 2-4.

- Note:**
- If the restore process changes the IP address, all management sessions are terminated. Use the Set Setup System command to return the IP configuration to the values you want. Refer to the ["Set Setup Command"](#) on page 2-52.
 - Configuration archive files created with the SAN Utility Archive function are not compatible with the Config Restore command.

save [*config_name*]

Saves changes made during a configuration edit session in the configuration given by [*config_name*]. If you omit [*config_name*], the value for [*config_name*] you chose for the most recent Config Edit command is used. [*config_name*] can be up to 31 characters excluding #, semicolon (;), and comma (,). The 6-port Switch Module supports up to 10 configurations including the default configuration.

Notes If you edit the active configuration, changes will be held in suspense until you reactivate the configuration or activate another configuration.

Examples The following shows an example of how to open and close a Config Edit session:

```
FCSM6: user1> admin start
FCSM6 (admin): user1> config edit
    The config named default is being edited.
.
.
FCSM6 (admin-config): user1> config cancel
    Configuration mode will be canceled. Please confirm (y/n): [n] y
FCSM6 (admin):user1> admin end
```

Date Command

This command displays or sets the system date and time. To set the date and time the information string must be provided in this format: MMDDhhmmCCYY. The new date and time takes effect immediately.

Authority Admin session except to display the date.

Syntax **date**
[MMDDhhmmCCYY]

Keywords **[MMDDhhmmCCYY]**
Specifies the date – this requires an admin session. If you omit [MMDDhhmmCCYY], the current date is displayed which does not require an admin session.

Examples The following is an example of the Date command:

```
FCSM6: user1> date  
Mon Sep 06 07:51:24 2004
```

Fallback Command

Assigns the pending firmware status back and forth between the active and inactive firmware images stored in switch module memory.

Authority Admin session

Syntax `fallback`

- Notes**
- The Show Switch command displays the active, inactive, and pending firmware versions.
 - After executing the Fallback command, reset the 6-port Switch Module to activate the pending firmware.

Examples The following is an example of the Fallback command:

```
FCSM6: user1> admin start
```

```
FCSM6 (admin): user1> fallback
```

```
Reverting to previous software image. Please confirm (y/n): [n] y
```

Hardreset Command

Resets the 6-port Switch Module and performs a power-on self test. This reset disrupts traffic, activates the pending firmware, and clears the alarm log. To save the alarm log before resetting, refer to the ["Set Log Command" on page 2-47](#).

Authority Admin session

Syntax **hardreset**

Notes To reset the 6-port Switch Module without a power-on self test, refer to the ["Reset Command" on page 2-26](#).

To reset the 6-port Switch Module without disrupting traffic, refer to the ["Hotreset Command" on page 2-18](#).

Examples The following is an example of the Hardreset command:

```
FCSM6: user1> admin start
FCSM6 (admin) user1> hardreset
The switch will be reset. Please confirm (y/n): [n] y
Alarm Msg: [Thu Mar 30 08:02:49.160 2000][A1000.000B][SM][The switch will be
reset and POST will run in several seconds]
Hardreset in progress...
Alarm Msg: [Thu Mar 30 08:02:55.588 2000][A1000.0005][SM][The switch is being
reset - this may take several seconds]
```

Help Command

Displays a brief description of the specified command, its keywords, and usage.

Authority None

Syntax **help [command] [keyword]**

Keywords **[command]**

Displays a summary of the command given by [command] and its keywords. If you omit [command], the system displays all available commands.

[keyword]

Displays a summary of the keyword given by [keyword] belonging to the command given by [command]. If you omit [keyword], the system displays the available keywords for the specified command.

all

Displays a list of all available commands (including command variations).

Examples The following is an example of the Help Config command:

```
FCSM6: user1> help config
config CONFIG_OPTIONS
The config command operates on configurations.
```

```
Usage: config { activate | backup | cancel | copy | delete |
              edit | list | restore | save }
```

The following is an example of the Help Config Edit command:

```
FCSM6: user1> help config edit
config edit [CONFIG_NAME]
This command initiates a configuration session and places the current session
into config edit mode.
If CONFIG_NAME is given and it exists, it gets edited; otherwise, it gets
created. If it is not given, the currently active configuration is edited.
Admin mode is required for this command.
```

```
Usage: config edit [CONFIG_NAME]
```

History Command

Displays a numbered list of the previously entered commands from which you can re-execute selected commands.

Authority None

Syntax `history`

Notes Use the History command to provide context for the `!` command:

- Enter `![command]` to re-enter the most recent execution of that command.
- Enter `![line number]` to re-execute the corresponding command from the History display
- Enter `![partial command string]` to re-execute a command that matches the command string.
- Enter `!!` to re-execute the most recent command.

Examples The following is an example of the History command:

```
FCSM6: user1> history
```

```
 1 show switch
 2 date
 3 help set
 4 history
```

```
FCSM6: user1> !3
```

```
help set
```

```
set SET_OPTIONS
```

```
There are many attributes that can be set.
```

```
Type help with one of the following to get more information:
```

```
Usage: set { alarm | beacon | config | log | pagebreak |
           port | setup | switch }
```

Hotreset Command

Resets the 6-port Switch Module for the purpose of activating the pending firmware without disrupting traffic. This command terminates all management sessions, saves all configuration information, and clears the alarm log. After the pending firmware is activated, the configuration is recovered. This process takes less than 80 seconds. To save the alarm log to a file before resetting, refer to the ["Set Log Command" on page 2-47](#).

Authority Admin session

Syntax `hotreset`

Notes You can load and activate version 4.1.x.x firmware on an operating 6-port Switch Module without disrupting data traffic or having to re-initialize attached devices under the following conditions:

- The current firmware version is a 4.1.x.x version that precedes the upgrade version.
- No changes are being made to switches in the fabric including powering up, powering down, disconnecting or connecting ISLs, and 6-port Switch Module 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, then change states, will be reset. When the non-disruptive activation is complete, SAN Utility sessions reconnect automatically. However, Telnet sessions must be restarted manually. This command clears the event log and all counters.

Examples The following is an example of the Hotreset command:

```
FCSM6: user1> admin start
```

```
FCSM6 (admin): user1> hotreset
```

A stable fabric is required to successfully activate the firmware on a switch without disrupting traffic. Therefore, before continuing with this action, ensure there are no administrative changes in progress anywhere in the fabric.

Continuing with this action will terminate all management sessions, including any Telnet sessions. When the firmware activation is complete, you may log in to the switch again. SANbox Manager will refresh automatically.

```
Please confirm (y/n): [n] y
```

```
Alarm Msg: [Thu Mar 30 08:01:17.732 2000][A1000.000D][SM][The switch will NDCLA  
in several seconds]
```

```
Alarm Msg: [Thu Mar 30 08:01:23.998 2000][A1000.0009][SM][The switch is  
proceeding with NDCLA]
```

```
Alarm Msg: [Thu Mar 30 08:01:38.629 2000][A1005.0002][cmon: NDCLA V4.1.0.17 ->  
V4.1.0.17]
```

Image Command

Manages and installs 6-port Switch Module firmware.

Authority Admin session

Syntax **image**
cleanup
fetch [account_name] [ip_address] [file_source] [file_destination]
list
unpack [file]

Keywords **cleanup**
Removes all firmware image files from the switch. All firmware image files are removed automatically each time the 6-port Switch Module is reset.

fetch [account_name] [ip_address] [file_source] [file_destination]
Retrieves image file given by [file_source] and stores it on the 6-port switch module with the file name given by [file_destination]. The image file is retrieved from the FTP server with the IP address given by [ip_address] and an account name given by [account_name]. If an account name needs a password to access the FTP server, the system will prompt you for it.

list
Displays the list of image files that reside on the switch.

unpack [file]
Installs the firmware file given by [file]. After unpacking the file, a message appears confirming successful unpacking. The switch must be reset for the new firmware to take effect.

Notes To provide consistent performance throughout the fabric, ensure that all switches are running the same version of firmware.

Use the Hotreset command to perform a non-disruptive activation.

Examples The following is an example of the Image Fetch command:

```
FCSM6: user1> admin start
FCSM6 (admin): user1> image fetch user1 10.0.0.254 file_source file_destination
Connected to 10.0.0.254.
331 Password required for user1.
Password:*****
230 User user1 logged in.
bin
200 Type set to I.
verbose
Verbose mode off.
```

Lip Command (for external ports only)

Reinitializes the specified loop port.

Authority Admin session

Syntax lip [port_number]

Keywords [port_number]
The number of the port to be reinitialized.

Examples The following is an example of the Lip command:

```
FCSM6 (admin): user1> lip 2
```

Passwd Command

Changes a user account's password.

Authority USERID account name and an Admin session to change another account's password; You can change you own password without an Admin session.

Syntax `passwd [account_name]`

Keywords `[account_name]`

The user account name. To change the password for an account name other than your own, you must open an admin session with the account name USERID. If you omit `[account_name]`, you will be prompted to change the password for the current account name.

Examples The following is an example of the Passwd command:

```
FCSM6 (admin): userid> passwd user2
```

```
Press 'q' and the ENTER key to abort this command.
```

```
account OLD password           : *****
```

```
account NEW password (4-20 chars) : *****
```

```
please confirm account NEW password: *****
```

```
password has been changed.
```

Ping Command

Initiates an attempt to communicate with another switch over an Ethernet network and reports the result.

Authority None

Syntax **ping**
ip_address

Keywords **ip_address**
The IP address of the switch to query.

Examples The following is an example of a successful Ping command:

```
FCSM6: user1> ping 10.20.11.57
Ping command issued. Waiting for response...
FCSM6: user1>
Response successfully received from 10.20.11.57.
```

This following is an example of an unsuccessful Ping command:

```
FCSM6: user1> ping 10.20.10.100
Ping command issued. Waiting for response...
No response from 10.20.10.100. Unreachable.
```

Ps Command

Displays current system process information.

Authority None

Syntax ps

Examples The following is an example of the Ps command:

```
FCSM6: user1> ps
```

PID	PPID	%CPU	TIME	ELAPSED	COMMAND
338	327	0.0	00:00:00	3-01:18:35	cns
339	327	0.0	00:00:01	3-01:18:35	ens
340	327	0.0	00:00:21	3-01:18:35	dlog
341	327	0.1	00:05:35	3-01:18:35	ds
342	327	0.2	00:11:29	3-01:18:35	mgmtApp
343	327	0.0	00:00:04	3-01:18:35	fc2
344	327	0.0	00:02:16	3-01:18:35	nserver
345	327	0.0	00:02:44	3-01:18:35	mserver
346	327	0.8	00:35:12	3-01:18:35	util
347	327	0.0	00:00:29	3-01:18:35	snmpservicepath
348	327	0.0	00:02:46	3-01:18:34	eport
349	327	0.0	00:00:21	3-01:18:34	PortApp
350	327	5.6	04:08:24	3-01:18:34	port_mon
351	327	0.0	00:01:38	3-01:18:34	zoning
352	327	0.0	00:00:01	3-01:18:34	diagApp
404	327	0.0	00:00:04	3-01:18:27	snmpd
405	327	0.0	00:00:02	3-01:18:27	snmpmain
406	405	0.0	00:00:00	3-01:18:26	snmpmain

Quit Command

Closes the Telnet session.

Authority None

Syntax **quit, exit, or logout**

Notes You can also enter Control-D to close the Telnet session.

Examples The following is an example of the Quit command:

```
FCSM6: user1> quit
```

```
Connection to host lost.
```

Reset Command

Resets the 6-port Switch Module configuration parameters. If you omit the keyword, the default is Reset Switch.

Authority Admin session

Syntax **reset**
 config [*config_name*]
 factory
 port [port_number]
 snmp
 switch (default)
 system
 zoning

Keywords **config [*config_name*]**
Resets the configuration given by [*config_name*] to the factory default values for 6-port Switch Module, port, port threshold alarm, and zoning configuration. If [*config_name*] does not exist on the switch, a configuration with that name will be created. If you omit [*config_name*], the active configuration is reset. You must activate the configuration for the changes to take effect. Refer to [Table 2-3](#) through [Table 2-6](#) for switch, port, and port threshold alarm configuration default values.

factory
Resets 6-port Switch Module configuration, port configuration, port threshold alarm configuration, zoning configuration, SNMP configuration, system configuration, and zoning to the factory default values. The 6-port Switch Module configuration is activated automatically. Refer to [Table 2-3](#) through [Table 2-8](#).

port [port_number]
Reinitializes the port given by [port_number]. Ports are numbered beginning with 0.

snmp
Resets the SNMP configuration settings to the factory default values. Refer to [Table 2-7](#) for SNMP configuration default values.

switch
Resets the 6-port Switch Module without a power-on self test. This is the default. This reset disrupts traffic and does the following:

- Activates the pending firmware.
- Closes all management sessions.
- Clears the alarm log. To save the alarm log before resetting, refer to the "[Set Log Command](#)" on [page 2-47](#).

To reset the 6-port Switch Module with a power-on self test, refer to the "[Hardreset Command](#)" on [page 2-15](#). To reset the 6-port Switch Module without disrupting traffic, refer to the "[Hotreset Command](#)" on [page 2-18](#).

system

Resets the system configuration settings to the factory default values. Refer to [Table 2-8](#) for system configuration default values.

zoning

Clears the zoning database and deactivates the active zone set. The zoning configuration values (autosave, default visibility) remain unchanged.

Notes

The following tables specify the various factory default settings:

Table 2-3. Switch Module Configuration Defaults

Parameter	Default
Admin State	Online
Broadcast Enabled	True
InbandEnabled	True
FDMIEEnabled	True
FDMIEEntries	1000
Domain ID	1 (0x Hex)
Domain ID Lock	False
Symbolic Name	FCSM6
R_A_TOV	10000
E_D_TOV	2000
Principal Priority	254
Configuration Description	QLogic 6-Port Enterprise Fibre Channel Switch Module for IBM eServer BladeCenter (TM)

Table 2-4. Port Configuration Defaults

Parameter	External Port Defaults (Ports 0, 15, 16, 17, 18, 19)	Internal Port Defaults (Ports 1–14) ¹
Admin State	Online	Online
Link Speed	Auto	2-Gbps
Port Type	GL	F
Symbolic Name	Portn, where n is the port number	Portn, where n is the port number

Table 2-4. Port Configuration Defaults (Continued)

Parameter	External Port Defaults (Ports 0, 15, 16, 17, 18, 19)	Internal Port Defaults (Ports 1–14) ¹
ALFairness	False	False
DeviceScanEnabled	True	True
ForceOfflineRSCN	False	False
ARB_FF	False	False
InteropCredit	0	0
ExtCredit	0	0
FANEnable	True	True
AutoPerfTuning	True	True
LCFEnable	False	False
MFSEnable	False	False
VIEnable	False	False
MSEnable	True	False
NoClose	False	False
IOStreamGuard	Disabled	Disabled
PDISCPingEnable	True	True

¹ Ports 1–14 apply to BladeCenter unit Type 8677. Ports 1–8 apply to BladeCenter T unit Types 8720 and 8730; ports 9–14 are not used.

Table 2-5. Port Threshold Alarm Configuration Defaults

Parameter	Default
ThresholdMonitoringEnabled	False
CRCErrorsMonitoringEnabled	True
RisingTrigger	25
FallingTrigger	1
SampleWindow	10
DecodeErrorsMonitoringEnabled	True
RisingTrigger	200
FallingTrigger	0
SampleWindow	10
ISLMonitoringEnabled	True
RisingTrigger	2
FallingTrigger	0
SampleWindow	10
LoginMonitoringEnabled	True
RisingTrigger	5
FallingTrigger	1
SampleWindow	10
LogoutMonitoringEnabled	True
RisingTrigger	5
FallingTrigger	1
SampleWindow	10
LOSMonitoringEnabled	True
RisingTrigger	100
FallingTrigger	5
SampleWindow	10

Table 2-6. Zoning Configuration Defaults

Parameter	Default
FC-SW-2 AutoSave	True
Default Visibility	All

Table 2-7. SNMP Configuration Defaults

Parameter	Default
SNMPEnabled	True
Contact	<syscontact undefined>
Location	<sysLocation undefined>
Description	QLogic 6-Port Enterprise Fibre Channel Switch Module for IBM eServer BladeCenter
Trap [1-5] Address	Trap 1: 10.0.0.254; Traps 2–5: 0.0.0.0
Trap [1-5] Port	162
Trap [1-5] Severity	Warning
Trap [1-5] Version	2
Trap [1-5] Enabled	False
ObjectID	1.3.6.14.1.1663.1.1.1.1.22
AuthFailureTrap	False
ProxyEnabled	True

Table 2-8. System Configuration Defaults

Parameter	Default
Ethernet Network Discovery	Static
Ethernet Network IP Address	Bay 3: 192.168.70.129 Bay 4: 192.168.70.130
Ethernet Network IP Mask	255.255.255.0
Ethernet Gateway Address	0.0.0.0
Admin Timeout	30 minutes
InactivityTimeout	0
Temp Monitoring Warning	75 (°C)
Temp Monitoring Failure	80 (°C)
Temp Failure Port Shutdown	False
UserAuthentication	False
LocalLogEnabled	True
RemotelogEnabled	False
RemoteLogHostAddress	10.0.0.254
NTPClientEnabled	False
NTPServerAddress	10.0.0.254
EmbeddedGUIEnabled	True

Examples The following is an example of the Reset Switch command:

```
FCSM6: user1>admin start
FCSM6 (admin): user1> reset switch
  The switch will be reset. Please confirm (y/n): [n] y
  Alarm Msg: [Thu Mar 30 08:04:50.655 2000][A1000.000B][SM][The switch will be
reset in several seconds]
  Reset switch in progress...
  Alarm Msg: [Thu Mar 30 08:04:57.005 2000][A1000.0005][SM][The switch is being
reset - this may take several seconds]
```

The following is an example of the Reset Config command

```
FCSM6: user1>admin start
FCSM6 (admin): user1> reset config production_config
  The active configuration will be reset.  Please confirm (y/n): [n] y

  Reset config in progress...

  Must execute 'config activate default' command before new settings can take
effect.
```

Set Command

Sets a variety of 6-port Switch Module parameters.

Authority Admin session for all keywords except Alarm, Beacon, and Pagebreak which are available without an Admin session.

Syntax **set**
alarm [option]
beacon [state]
config [option]
log [option]
pagebreak [state]
port [option]
setup [option]
switch [state]

Keywords **alarm [option]**
Controls the display of alarms in the session output stream or clears the alarm log. [option] can be one of the following:

- clear
Clears the alarm log history. This value requires an Admin session.
- on
Enables the display of alarms in the session output stream.
- off
Disables the display of alarms in the session output stream.

beacon [state]
Enables or disables the flashing of the Logged-In LEDs according to [state]. This keyword does not require an Admin session. [state] can be one of the following:

- on
Enables the flashing beacon.
- off
Disables the flashing beacon.

config [option]
Sets 6-port Switch Module, port, port threshold alarm, and zoning configuration parameters. Refer to the "[Set Config Command](#)" on page 2-35.

log [option]
Specifies the type of entries to be entered in the event log. Refer to the "[Set Log Command](#)" on page 2-47.

pagebreak [state]

Specifies how much information is displayed on the screen at a time according to the value given by [state]. This keyword does not require an Admin session.

[state] can be one of the following:

on

Limits the display of information to 20 lines at a time. The page break functions affects the following commands: Alias (List, Members), Show (Alarm, Log), Zone (List, Members), Zoneset (List, Zones), Zoning (Active, List).

off

Allows continuous display of information without a break.

port [option]

Sets port state and speed for the specified port. The previous Set Config Port settings are restored after a 6-port Switch Module reset or a reactivation of a 6-port Switch Module configuration. Refer to the ["Set Port Command" on page 2-50](#).

setup [option]

Changes SNMP and system configuration settings. Refer to the ["Set Setup Command" on page 2-52](#).

switch [state]

Changes the administrative state for all ports on the 6-port Switch Module to the state given by [state]. The previous Set Config Switch settings are restored after a 6-port Switch Module reset or a reactivation of a 6-port Switch Module configuration. [state] can be one of the following:

online

Places all ports online

offline

Places all ports offline.

diagnostics

Prepares all ports for testing.

Examples The following examples enables and disables the beacon:

```
FCSM6: user1> set beacon on
```

```
Command succeeded.
```

```
FCSM6 $> set beacon off
```

```
Command succeeded.
```


Set Config Command

Sets 6-port Switch Module, port, port threshold alarm, and zoning configuration parameters. The changes you make with this command are not retained when you reset or power cycle the 6-port Switch Module unless you save them using the Config Save command. Refer to the ["Config Command" on page 2-11](#).

Authority Admin session and a Config Edit session

Syntax **set config**
port [*port_number*]
ports [*port_set*]
switch
threshold
zoning

Keywords **port [*port_number*]**
Initiates an edit session in which to change configuration parameters for the port number given by [*port_number*]. If you omit [*port_number*], the system begins with port 0 and proceeds in order through the last port. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets. Enter "q" to end the configuration for one port, or "qq" to end the configuration for all ports. [Table 2-9](#) describes the port configuration parameters.

Note: For external ports (0, 15, 16, 17, 18, 19), all port parameters apply. For internal ports (1–14), only the port state setting is configurable. Ports 1–14 apply to BladeCenter unit Type 8677. Ports 1–8 apply to BladeCenter T unit Types 8720 and 8730; ports 9–14 are not used. For information about port numbering and mapping, see [Table A-1](#).

ports [*port_set*]
Initiates an editing session in which to change configuration parameters (except symbolic port name) for the set of all external ports based on external port 0, or the set off all internal ports based on internal port 1, depending on the value given by [*port_set*]. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets. Enter "q" to end the configuration. [Table 2-9](#) describes the port configuration parameters. [*port_set*] can have the following values:

external

The configurations for all external ports (0, 15, 16, 17, 18, 19) are made based on the configuration of external port 0.

internal

The configuration for all internal ports (1–14) are made based on the configuration of internal port 1.

Note: Ports 1–14 apply to BladeCenter unit Type 8677. Ports 1–8 apply to BladeCenter T unit Types 8720 and 8730; ports 9–14 are not used. For information about port numbering and mapping, see [Table A-1](#).

Table 2-9. Set Config Port Parameters

Parameter	Description
AdminState	Port administrative state: <ul style="list-style-type: none"> ■ Online – Activates and prepares the port to send data. This is the default. ■ Offline – Prevents the port from receiving signal and accepting a device login. ■ Diagnostics – Prepares the port for testing and prevents the port from accepting a device login. ■ Down – Disables the port by removing power from the port lasers.
LinkSpeed	1-Gbps, 2-Gbps, or Auto. The default is Auto.
PortType	GL, G, F, FL, Donor. The default is GL.
SymbolicPortName	Descriptive name for the port. The name can be up to 32 characters excluding #, semicolon (;), and comma (,). The default is Port n where n is the port number. This parameter can be changed only with the Set Config Port command.
ALFairness	Arbitration loop fairness. Enables (True) or disables (False) the switch's priority to arbitrate on the loop. The default is False.
DeviceScanEnabled	Enables (True) or disables (False) the scanning of the connected device for FC-4 descriptor information during login. The default is True.
ForceOfflineRSCN	Enables (False) or disables (True) the immediate transmission of RSCN messages when communication between a port and a device is interrupted. If enabled, the RSCN message is delayed for 200 ms for locally attached devices and 400 ms for devices connected through other switches. The default is False. This parameter is ignored if IOStreamGuard is enabled.
ARB_FF	Send ARB_FF (True) instead of IDLEs (False) on the loop. The default is False.

Table 2-9. Set Config Port Parameters (Continued)

Parameter	Description
InteropCredit	Interoperability credit. The number of buffer-to-buffer credits per port. 0 means the default (16) is unchanged. Changing interoperability credits is necessary only for E_Ports that are connected to non-FC-SW-2-compliant switches. Contact your authorized maintenance provider for assistance in using this feature.
ExtCredit	Extended credits. The number of port buffer credits that this port can acquire from donor ports. The default is 0.
FANEnable	Fabric address notification. Enables (True) or disables (False) the communication of the FL_Port address, port name, and node name to the logged-in NL_Port. The default is True.
AutoPerfTuning	Automatic performance tuning for FL_Ports only. The default is True. <ul style="list-style-type: none"> ■ If AutoPerfTuning is enabled (True) and the port is an FL_Port, MFSEnable is automatically enabled. LCFEnable and VIEnable are overridden to False. ■ If AutoPerfTuning is disabled (False), MFSEnable, LCFEnable, and VIEnable retain their original values.
LCFEnable	Link control frame preference routing. This parameter appears only if AutoPerfTuning is False. Enables (True) or disables (False) preferred routing of frames with R_CTL = 1100 (Class 2 responses). The default is False. Enabling LCFEnable will disable MFSEnable.
MFSEnable	Multi-Frame Sequence bundling. This parameter appears only if AutoPerfTuning is False. Prevents (True) or allows (False) the interleaving of frames in a sequence. The default is False. Enabling MFSEnable disables LCFEnable and VIEnable.
VIEnable	Virtual Interface (VI) preference routing. This parameter appears only if AutoPerfTuning is False. Enables (True) or disables (False) VI preference routing. The default is False. Enabling VIEnable will disable MFSEnable.
MSEnable	Management server enable. Enables (True) or disables (False) management server on this port. The default is True.

Table 2-9. Set Config Port Parameters (Continued)

Parameter	Description
NoClose	Loop circuit closure prevention. Enables (True) or disables (False) the loop's ability to remain in the open state indefinitely. True reduces the amount of arbitration on a loop when there is only one device on the loop. The default is False.
IStreamGuard	I/O Stream Guard. Enable (Enable) or disables (Disable) the suppression of RSCN messages. I/O Stream Guard should be enabled only for ports connected to initiator devices. The default is Disable.
PDISCPingEnable	Enables (True) or disables (False) the transmission of ping messages from the 6-port Switch Module to all devices on a loop port. The default is True.

switch

Initiates an editing session in which to change 6-port Switch Module configuration settings. The system displays each parameter one line at a time and prompts you for a value. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets. [Table 2-10](#) describes the Set Config Switch parameters.

Table 2-10. Set Config Switch Parameters

Parameter	Description
AdminState	Switch module administrative state: online, offline, or diagnostics. The default is Online.
BroadcastEnabled	Broadcast. Enables (True) or disables (False) forwarding of broadcast frames. The default is True.
InbandEnabled	Inband management. Enables (True) or disables (False) the ability to manage the 6-port Switch Module over an ISL. The default is True.
FDMIEnabled	Fabric Device Monitoring Interface. Enables (True) or disables (False) the monitoring of target and initiator device information.

Table 2-10. Set Config Switch Parameters (Continued)

Parameter	Description
FDMIEntries	The number of device entries to maintain in the FDMI database. Enter a number from 0–1000. The default is 1000.
DefaultDomainID	Default domain ID. The default is 1.
DomainIDLock	Prevents (True) or allows (False) dynamic reassignment of the domain ID. The default is False.
SymbolicName	Descriptive name for the 6-port Switch Module. The name can be up to 32 characters excluding #, semicolon (;), and comma (.). The default is FCSM6.
R_A_TOV	Resource Allocation Timeout Value. The number of milliseconds the 6-port Switch Module waits to allow two ports to allocate enough resources to establish a link. The default is 10000.
E_D_TOV	Error Detect Timeout Value. The number of milliseconds a port is to wait for errors to clear. The default is 2000.
PrincipalPriority	The priority used in the FC-SW-2 principal switch selection algorithm. 1 is high, 255 is low. The default is 254.
ConfigDescription	Switch module configuration description. The configuration description can be up to 32 characters excluding #, semicolon (;), and comma (.). The default is Default Config.

Table 2-10. Set Config Switch Parameters (Continued)

Parameter	Description
FC-SW-2 Compliant	Propagates just the active zone set throughout the fabric (True, compliant) or the entire zoning database (False, non-compliant). The default is True. Contact your authorized maintenance provider for assistance in using this feature.
LegacyAddressFormat	Available only when the FC-SW-2 Compliant parameter is False, this parameter enables (True) or disables (False) the use of legacy address formatting for interoperating with non-FC-SW-2 switches. Refer to the FC-SW-2 Compliant parameter. The default is False. Contact your authorized maintenance provider for assistance in using this feature.

threshold

Initiates a configuration session by which to generate and log alarms for selected events. The system displays each event, its triggers, and sampling window one line at a time and prompts you for a value. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets. These parameters must be saved in a configuration and activated before they will take effect. Refer to the "Config Command" on page 2-11 for information about saving and activating a configuration. Table 2-11 describes the Set Config Threshold parameters. The 6-port Switch Module will down a port if an alarm condition is not cleared within three consecutive sampling windows (by default 30 seconds). Reset the port to bring it back online. An alarm is cleared when the threshold monitoring detects that the error rate has fallen below the falling trigger.

Table 2-11. Set Config Threshold Parameters

Parameter	Description
Threshold Monitoring Enabled CRCErrorsMonitoringEnabled DecodeErrorsMonitoringEnabled ISLMonitoringEnabled LoginMonitoringEnabled LogoutMonitoringEnabled LOSMonitoringEnabled	Master enable/disable parameter for all events. Enables (True) or disables (False) the generation of all enabled event alarms. The default is False. The event type enable/disable parameter. Enables (True) or disables (False) the generation of alarms for each of the following events: <ul style="list-style-type: none"> ■ CRC errors ■ Decode errors ■ ISL connection count ■ Device login errors ■ Device logout errors ■ Loss-of-signal errors
Rising Trigger	The event count above which a rising trigger alarm is logged. The 6-port Switch Module will not generate another rising trigger alarm for that event until the count descends below the falling trigger and again exceeds the rising trigger.
Falling Trigger	The event count below which a falling trigger alarm is logged. The 6-port Switch Module will not generate another falling trigger alarm for that event until the count exceeds the rising trigger and descends again below the falling trigger.
Sample Window	The period of time in seconds in which to count events.

zoning

Initiates an editing session in which to change 6-port Switch Module zoning attributes. The system displays each parameter one line at a time and prompts you for a value. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets.

Table 2-12. Set Config Zoning Parameters

Parameter	Description
FC-SW-2 AutoSave	Available only when the FC-SW-2 Compliant parameter is True, this parameter enables (True) or disables (False) the saving of changes to active zone set in the switch's permanent memory. Refer to " FC-SW-2 Compliant " on page 2-40. The default is True. Disabling the Autosave parameter can be useful to prevent the propagation of zoning information when experimenting with different zoning schemes. However, leaving the Autosave parameter disabled can disrupt device configurations should a 6-port Switch Module have to be reset. For this reason, the Autosave parameter should be enabled in a production environment. Contact your authorized maintenance provider for assistance in using this feature.
Default Visibility	Enables (All) or disables (None) communication among the 6-port Switch Module ports/devices and the fabric in the absence of an active zone set. The default is All.

Examples The following is an example of the Set Config Port command:

```
FCSM6: user1> admin start
FCSM6 (admin): user1> config edit
FCSM6 (admin-config): user1> set config port 0
```

A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current value.
If you wish to terminate this process before reaching the end of the list
press 'q' or 'Q' and the ENTER key to do so.

```
Configuring Port Number: 0
```

```
-----
```

AdminState	(1=Online, 2=Offline, 3=Diagnostics, 4=Down)	[Online]
LinkSpeed	(1=1Gb/s, 2=2Gb/s, 3=Auto)	[Auto]
PortType	(GL / G / F / FL / Donor)	[GL]
SymPortName	(string, max=32 chars)	[Port0]
ALFairness	(True / False)	[False]
DeviceScanEnable	(True / False)	[True]
ForceOfflineRSCN	(True / False)	[False]
ARB_FF	(True / False)	[False]
InteropCredit	(decimal value, 0-255)	[0]
ExtCredit	(dec value, increments of 15, non-loop only)	[0]
FANEnable	(True / False)	[True]
AutoPerfTuning	(True / False)	[True]
MSEnable	(True / False)	[True]
NoClose	(True / False)	[False]
IOStreamGuard	(Enable / Disable)	[Disabled]
PDISCPingEnable	(True / False)	[True]

Finished configuring attributes.

This configuration must be saved (see config save command) and
activated (see config activate command) before it can take effect.

To discard this configuration use the config cancel command.

```
FCSM6 (admin-config): user1>
```

The following is an example of the Set Config Switch command:

```
FCSM6: user1> admin start
FCSM6 (admin): user1> config edit
FCSM6 (admin-config): user1> set config switch
```

A list of attributes with formatting and default values will follow.
Enter a new value or simply press the ENTER key to accept the current value.
If you wish to terminate this process before reaching the end of the list
press 'q' or 'Q' and the ENTER key to do so.

```
AdminState          (1=Online, 2=Offline, 3=Diagnostics) [Online      ]
BroadcastEnable     (True / False)                       [False       ]
InbandEnabled       (True / False)                       [False       ]
FDMIEnabled         (True / False)                       [True        ]
FDMIEntries         (decimal value, 0-1000)               [1000        ]
DefaultDomainID     (decimal value, 1-239)                [11          ]
DomainIDLock        (True / False)                       [True        ]
SymbolicName        (string, max=32 chars)               [FCSM6       ]
R_A_TOV             (decimal value, 100-100000 msec)      [10000       ]
E_D_TOV             (decimal value, 10-20000 msec)      [2000        ]
PrincipalPriority    (decimal value, 1-255)                [254         ]
ConfigDescription   (string, max=32 chars) [Fibre Channel Switch Module]
FC-SW-2 Compliant   (True / False)                       [True        ]
```

The following is an example of the Set Config Threshold command:

```
FCSM6: user1> admin start
FCSM6 (admin): user1> config edit
FCSM6 (admin-config): user1> set config threshold
```

A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current value.
If you wish to terminate this process before reaching the end of the list
press 'q' or 'Q' and the ENTER key to do so.

```
ThresholdMonitoringEnabled (True / False) [False ]
CRCErrorsMonitoringEnabled (True / False) [True  ]
  RisingTrigger            (decimal value, 1-1000) [25   ]
  FallingTrigger           (decimal value, 0-1000) [1    ]
  SampleWindow             (decimal value, 1-1000 sec) [10   ]
DecodeErrorsMonitoringEnabled (True / False) [True  ]
```

RisingTrigger	(decimal value, 1-1000)	[200]
FallingTrigger	(decimal value, 0-1000)	[0]
SampleWindow	(decimal value, 1-1000 sec)	[10]
ISLMonitoringEnabled	(True / False)	[True]
RisingTrigger	(decimal value, 1-1000)	[2]
FallingTrigger	(decimal value, 0-1000)	[0]
SampleWindow	(decimal value, 1-1000 sec)	[10]
LoginMonitoringEnabled	(True / False)	[True]
RisingTrigger	(decimal value, 1-1000)	[5]
FallingTrigger	(decimal value, 0-1000)	[1]
SampleWindow	(decimal value, 1-1000 sec)	[10]
LogoutMonitoringEnabled	(True / False)	[True]
RisingTrigger	(decimal value, 1-1000)	[5]
FallingTrigger	(decimal value, 0-1000)	[1]
SampleWindow	(decimal value, 1-1000 sec)	[10]
LOSMonitoringEnabled	(True / False)	[True]
RisingTrigger	(decimal value, 1-1000)	[100]
FallingTrigger	(decimal value, 0-1000)	[5]
SampleWindow	(decimal value, 1-1000 sec)	[10]

Finished configuring attributes.

This configuration must be saved (see config save command) and activated (see config activate command) before it can take effect. To discard this configuration use the config cancel command.

The following is an example of the Set Config Zoning command.

```
FCSM6: user1> admin start
FCSM6 (admin): user1> config edit
FCSM6 (admin-config): user1> set config zoning
```

A list of attributes with formatting and current values will follow.

Enter a new value or simply press the ENTER key to accept the current value.

If you wish to terminate this process before reaching the end of the list press 'q' or 'Q' and the ENTER key to do so.

```
FC-SW-2 AutoSave      (True / False) [True]
Default Visibility    (All / None)  [All ]
```

Finished configuring attributes.

This configuration must be saved (see config save command) and activated (see config activate command) before it can take effect.

To discard this configuration use the config cancel command.

Set Log Command

Specifies the type of entries to be entered in the event log. Log entries are created for ports, components, and event severity levels.

Authority Admin session

Syntax **set log**
archive
clear
component [list]
level [level]
port [port_list]
restore
save
start (default)
stop

Keywords **archive**
Collects the most recent 200 entries plus the previous 1000 entries and stores the result in new file named *logfile* that is maintained in switch memory where it can be downloaded using FTP. To download *logfile*, open an FTP session, log in with account name/password of “images” for both, and type “get logfile”.

clear
Clears all log entries.

component [list]
Specifies one or more components to monitor for events. Use <space> to delimit values in the list. Choose one or more of the following values:

- All
Monitors all components. To maintain optimal 6-port Switch Module performance, do not use this setting with the Level keyword set to Info.
- Chassis
Monitors chassis hardware components such as fans and power supplies.
- Eport
Monitors all E_Ports.
- Mgmtserver
Monitors management server status.
- Nameserver
Monitors name server status.
- None
Monitor none of the component events.
- Other
Monitors other miscellaneous events.

Port
Monitors all port events

Switch
Monitors switch management events.

Zoning
Monitors zoning conflict events.

level [level]

Specifies the severity level given by [level] to use in monitoring events for the specified components or ports. [level] can be one of the following values:

Critical
Monitors critical events.

Warn
Monitors warning events.

Info
Monitors informational events. To maintain optimal 6-port Switch Module performance, do not use this setting with the Component keyword set to All.

None
Monitors none of the severity levels.

port [port_list]

Specifies one or more ports to monitor for events. Choose one of the following values:

[port_list]
Specifies port or ports to monitor. Use a <space> to delimit values in the list. Ports are numbered beginning with 0.

All
Specifies all ports.

None
Disables monitoring on all ports.

restore

Restores and saves the port, component, and level settings to the default values.

save

Saves the log settings for the component, level, and port. These settings remain in effect after a 6-port Switch Module reset. The log settings can be viewed using the Show Log Settings command. To export log entries to a file, use the Set Log Archive command.

start

Starts the logging of events based on the Port, Component, and Level keywords assigned to the current configuration. The logging continues until you enter the Set Log Stop command.

stop
Stops logging of events.

Notes To maintain optimal 6-port Switch Module performance, do not set the Component keyword to All and the Level keyword to Info at the same time.

Examples The following is an example of the Set Log Archive command:

```
FCSM6: user1> admin start
FCSM6 (admin): user1> set log archive
```

The following is an example of the Set Log Restore command:

```
FCSM6: user1> admin start
FCSM6 (admin): user1> set log restore
```

Set Port Command

Sets port state and speed for the specified port temporarily until the next switch module reset or new configuration activation. This command also clears port counters. For information about port numbering and mapping, see [Table A-1](#).

Note: For external ports (0, 15, 16, 17, 18, 19), all port parameters apply. For internal ports (1–14), only the port state setting is configurable.

Authority Admin session except for the Clear keyword.

Syntax **set port [port_number]**
bypass [alpa] (for external ports only)
clear
enable (for external ports only)
speed [transmission_speed]
state [state]

Keywords **[port_number]**
Specifies the port. Ports are numbered beginning with 0. For information about port numbering and mapping, see [Table A-1](#).

bypass [alpa]
Sends a Loop Port Bypass (LPB) to a specific Arbitrated Loop Physical Address (ALPA) or to all ALPAs on the arbitrated loop. [alpa] can be a specific ALPA or the keyword ALL to choose all ALPAs.

clear
Clears the counters on the port. This keyword does not require an admin session.

enable
Sends a Loop Port Enable (LPE) to all ALPAs on the arbitrated loop.

speed [transmission_speed]
Specifies the transmission speed for the specified port. Choose one of the following port speed values:

1Gb/s
One gigabit per second.

2Gb/s
Two gigabits per second.

Auto
The port speed is automatically detected.

state [state]
Specifies one of the following administrative states for the specified port:

Online
Places the port online. This activates and prepares the port to send data.

Offline

Places the port offline. This prevents the port from receiving signal and accepting a device login.

Diagnostics

Prepares the port for testing. This prepares the port for testing and prevents the port from accepting a device login.

Down

Disables the port by removing power from the port lasers.

Examples The following is an example of the Set Port State command:

```
FCSM6: user1> admin start
FCSM6 (admin): user1> set port state down
```

Set Setup Command

Changes SNMP and system configuration settings. The 6-port Switch Module maintains one SNMP configuration and one system configuration.

Authority Admin session

Syntax **set setup**
snmp
system

Keywords **snmp**
Prompts you in a line-by-line fashion to change SNMP configuration settings. [Table 2-13](#) describes the SNMP fields. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets.

Table 2-13. SNMP Configuration Settings

Entry	Description
SNMPEnabled	Enables (True) or disables (False) SNMP on the 6-port Switch Module. The default is True.
Contact	Specifies the name of the person to be contacted to respond to trap events. The name can be up to 64 characters excluding #, semicolon (;), and comma (.). The default is undefined.
Location	Specifies the name of the 6-port Switch Module location. The name can be up to 64 characters excluding #, semicolon (;), and comma (.). The default is undefined.
Trap [1-5] Address	Specifies the workstation IP address to which SNMP traps are sent. The default address for trap 1 is 10.0.0.254. The default address for traps 2–5 is 0.0.0.0. Addresses, other than 0.0.0.0, for all traps must be unique.
Trap [1-5] Port	Specifies the workstation port to which SNMP traps are sent. Valid workstation port numbers are 1–65535. The default is 162.
Trap [1-5] Severity	Specifies the severity level to use when monitoring trap events. The default is Warning
Trap [1-5] Version	Specifies the SNMP version (1 or 2) to use in formatting traps. The default is 2.
Trap [1-5] Enabled	Specifies whether traps (event information) are enabled or disabled (default).

Table 2-13. SNMP Configuration Settings (Continued)

Entry	Description
ReadCommunity	Read community password that authorizes an SNMP agent to read information from the 6-port Switch Module. This is a write-only field. The value on the 6-port Switch Module and the SNMP management server must be the same. The read community password can be up to 32 characters excluding #, semicolon (;), and comma (.). The default is "public".
WriteCommunity	Write community password that authorizes an SNMP agent to write information to the 6-port Switch Module. This is a write-only field. The value on the 6-port Switch Module and the SNMP management server must be the same. The write community password can be up to 32 characters excluding #, semicolon (;), and comma (.). The default is "private".
TrapCommunity	Trap community password that authorizes an SNMP agent to receive traps. This is a write-only field. The value on the 6-port Switch Module and the SNMP management server must be the same. The trap community password can be up to 32 characters excluding #, semicolon (;), and comma (.). The default is "public".
AuthFailureTrap	Enables (True) or disables (False) the generation of traps in response to trap authentication failures. The default is False.
ProxyEnabled	Enables (True) or disables (False) SNMP communication with other switches in the fabric. The default is True.

system

Prompts you in a line-by-line fashion to change system configuration settings. [Table 2-14](#) describes the system configuration fields. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets.

Note: Changing the IP address will terminate all Ethernet management sessions.

Table 2-14. System Configuration Settings

Entry	Description
Eth0NetworkDiscovery	Ethernet boot method: (1 - Static). Bootp, DHCP, and RARP do not apply.
Eth0NetworkAddress	Ethernet Internet Protocol (IP) address.

Table 2-14. System Configuration Settings (Continued)

Entry	Description
Eth0NetworkMask	Ethernet subnet mask address.
Eth0GatewayAddress	Ethernet IP address gateway.
AdminTimeout	Amount of time in minutes the 6-port Switch Module waits before terminating an idle Admin session. Zero (0) disables the time out threshold. The default is 30, the maximum is 1440.
InactivityTimeout	Amount of time in minutes the 6-port Switch Module waits before terminating an idle CLI session. Zero (0) disables the time out threshold. The default is 0, the maximum is 1440.
UserAuthentication	Enables (True) or disables (False) the enforcement of account names and passwords for SAN Utility. Enabling this parameter does not affect a logged in account until that account logs in again. The default is False.
LocalLogEnabled	Enables (True) or disables (False) the saving of log information on the switch. The default is True.
RemoteLogEnabled	Enables (True) or disables (False) the recording of the 6-port Switch Module event log on a remote host that supports the syslog protocol. The default is False.
RemoteLogHostAddress	The IP address of the host that will receive the 6-port Switch Module event log information if remote logging is enabled. The default is 10.0.0.254.
NTPClientEnabled	Enables (True) or disables (False) the Network Time Protocol (NTP) client on the switch. This client enables the 6-port Switch Module to synchronize its time with an NTP server. This feature supports NTP version 4 and is compatible with version 3. An Ethernet connection to the server is required and you must first set an initial time and date on the switch. The synchronized time becomes effective immediately.

Table 2-14. System Configuration Settings (Continued)

Entry	Description
NTPServerAddress	The IP address of the NTP server from which the NTP client acquires the time and date.
EmbeddedGUIEnabled	Enables (True) or disables (False) the SAN Browser. Changing this parameter to False while the SAN Browser is running will terminate SAN Browser. The default is True.

Examples The following is an example of the Set Setup SNMP command:

```
FCSM6: user1> admin start
```

```
FCSM6 (admin): user1> set setup snmp
```

A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current value.
If you wish to terminate this process before reaching the end of the list
press 'q' or 'Q' and the ENTER key to do so.

```
Trap Severity Options
```

```
-----
```

```
unknown, emergency, alert, critical, error, warning, notify, info, debug, mark
```

SNMPEnabled	(True / False)	[True]
Contact	(string, max=64 chars)	[<sysContact undefined]
Location	(string, max=64 chars)	[sysLocation undefined]
Trap1Address	(dot-notated IP Address)	[10.20.71.15]
Trap1Port	(decimal value)	[162]
Trap1Severity	(see allowed options above)	[warning]
Trap1Version	(1 / 2)	[2]
Trap1Enabled	(True / False)	[False]
Trap2Address	(dot-notated IP Address)	[0.0.0.0]
Trap2Port	(decimal value)	[162]
Trap2Severity	(see allowed options above)	[warning]
Trap2Version	(1 / 2)	[2]
Trap2Enabled	(True / False)	[False]
Trap3Address	(dot-notated IP Address)	[0.0.0.0]
Trap3Port	(decimal value)	[162]
Trap3Severity	(see allowed options above)	[warning]
Trap3Version	(1 / 2)	[2]
Trap3Enabled	(True / False)	[False]
Trap4Address	(dot-notated IP Address)	[0.0.0.0]
Trap4Port	(decimal value)	[162]
Trap4Severity	(see allowed options above)	[warning]
Trap4Version	(1 / 2)	[2]
Trap4Enabled	(True / False)	[False]
Trap5Address	(dot-notated IP Address)	[0.0.0.0]
Trap5Port	(decimal value)	[162]
Trap5Severity	(see allowed options above)	[warning]
Trap5Version	(1 / 2)	[2]
Trap5Enabled	(True / False)	[False]
ReadCommunity	(string, max=32 chars)	[public]
WriteCommunity	(string, max=32 chars)	[private]

TrapCommunity	(string, max=32 chars)	[public]
AuthFailureTrap	(True / False)	[False]
ProxyEnabled	(True / False)	[True]

The following is an example of the Set Setup System command:

```
FCSM6 (admin): user1> set setup system
```

A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current value.
If you wish to terminate this process before reaching the end of the list
press 'q' or 'Q' and the ENTER key to do so.

Eth0NetworkDiscovery	(1=Static, 2=Bootp, 3=Dhcp, 4=Rarp)	[Static]
Eth0NetworkAddress	(dot-notated IP Address)	[192.168.70.129]	
Eth0NetworkMask	(dot-notated IP Address)	[255.255.255.0]	
Eth0GatewayAddress	(dot-notated IP Address)	[0.0.0.0]	
AdminTimeout	(dec value 0-1440 minutes, 0=never)	[30]
InactivityTimeout	(dec value 0-1440 minutes, 0=never)	[10]
UserAuthentication	(True / False)	[False]
LocalLogEnabled	(True / False)	[True]
RemoteLogEnabled	(True / False)	[False]
RemoteLogHostAddress	(dot-notated IP Address)	[10.0.0.254]	
NTPClientEnabled	(True / False)	[False]
NTPServerAddress	(dot-notated IP Address)	[10.0.0.254]	
EmbeddedGUIEnabled	(True / False)	[True]

Show Command

Displays fabric, 6-port Switch Module, and port operational information.

Authority None

Syntax **show**
 about
 alarm *[option]*
 broadcast
 chassis
 config *[option]*
 domains
 donor
 fabric
 fdmi *[port_wwn]*
 interface
 log *[option]*
 lsdb
 mem *[count]*
 ns *[option]*
 pagebreak
 perf *[option]*
 port *[port_number]*
 post log
 setup *[option]*
 steering *[domain_id]*
 support
 switch
 topology
 users
 version

Keywords **about**

Displays an introductory set of information about operational attributes of the 6-port Switch Module. This keyword is equivalent to the Version keyword.

alarm *[option]*

Displays the alarm log and session display setting. If you omit *[option]*, the command displays the last 200 alarm entries. The alarm log is cleared when the 6-port Switch Module is reset or power cycled. *[option]* has the following value:

setting

Displays the status of the parameter that controls the display of alarms in the session output stream. This parameter is set using the Set Alarm command.

broadcast

Displays the broadcast tree information and all ports that are currently transmitting and receiving broadcast frames.

chassis

Displays chassis component status and temperature.

config [option]

Displays 6-port Switch Module, port, and zoning configuration attributes. Refer to the ["Show Config Command" on page 2-71](#).

domains

Displays list of each domain and its worldwide name in the fabric.

donor

Displays list of current donor configuration for all ports.

fabric

Displays list of each domain, symbolic name, worldwide name, node IP address, and port IP address.

fdmi [port_wwn]

Displays detailed information about the device host bus adapter given by [port_wwn]. If you omit [port_wwn], the command displays a summary of host bus adapter information for all attached devices in the fabric. Illegal characters in the display appear as question marks (?).

interface

Displays the status of the active network interfaces.

log [option]

Displays log entries. Refer to the ["Show Log Command" on page 2-75](#). The log is cleared when the 6-port Switch Module is reset or power cycled.

lsdb

Displays Link State database information

mem [count]

Displays information about memory activity for the number of seconds given by [count]. If you omit [count], the value 1 is used. Displayed memory values are in 1K block units.

Note: This keyword will display memory activity updates until [count] is reached – it cannot be interrupted. Therefore, avoid using large values for [count].

ns [option]

Displays name server information for the specified [option]. If you omit [option], name server information for the local domain ID is displayed. [option] can have the following values:

all

Displays name server information for all switches and ports.

[domain_id]

Displays name server information for the switch given by [domain_id].

[domain_id] is a switch domain ID.

[port_id]

Displays name server information for the port given by [port_id]. [port_id] is a port Fibre Channel address.

pagebreak

Displays the current pagebreak setting. The pagebreak setting limits the display of information to 20 lines (On) or allows the continuous display of information without a break (Off).

perf [option]

Displays performance information for all ports. Refer to the ["Show Perf Command" on page 2-78](#).

port [port_number]

Displays operational information for the port given by [port_number]. Ports are numbered beginning with 0. If [port number] is omitted, information is displayed for all ports. [Table 2-15](#) describes the port parameters.

Note: For external ports (0, 15, 16, 17, 18, 19), all parameters apply. For internal ports (1 through 14) only AdminState applies. For information about port numbering and mapping, see [Table A-1](#).

Table 2-15. Show Port Parameters

Entry	Description
AdminState	Port administrative state: Online, Offline, Diagnostics, Down
AsicNumber	ASIC identifier
AsicPort	ASIC port number
ConfigType	Configured port type
DiagStatus	Power on self test results
EpConnState	E_Port connection state
EplsoReason	E_Port isolation reason

Table 2-15. Show Port Parameters (Continued)

Entry	Description
LinkSpeed	Port transmission speed
LinkState	Port administrative state
LoginStatus	Port login status
MaxCredit	Port buffer credit capacity
OperationalState	Port operational state
PortID	Port Fibre Channel address
PortWWN	Port World Wide Name
RunningType	Operational port type
MediaPartNumber	Transceiver part number
MediaRevision	Transceiver hardware version
MediaType	Transceiver type
MediaVendor	Transceiver manufacturer
MediaVendorID	Transceiver manufacturer identifier
SymbolicName	Port symbolic name
SyncStatus	Synchronization status
XmitterEnabled	Port laser status
PerfTuningMode	Performance tuning mode status
Alinit	Incremented each time the port begins AL initialization.
AlinitError	Number of times the port entered initialization and the initialization failed.
Bad Frames	Number of frames that have framing errors.
ClassXFramesIn	Number of class x frames received by this port.
ClassXFramesOut	Number of class x frames sent by this port.
ClassXWordsIn	Number of class x words received by this port.
ClassXWordsOut	Number of class x words sent by this port.
ClassXToss	Number of times an SOFi3 or SOFn3 frame is tossed from TBUF.
DecodeError	Number of decode errors detected

Table 2-15. Show Port Parameters (Continued)

Entry	Description
EpConnects	Number of times an E_Port connected through ISL negotiation.
FBusy	Number of times the 6-port Switch Module sent a F_BSY because Class 2 frame could not be delivered within ED_TOV time. 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.
Flowerrors	Received a frame when there were no available credits.
FReject	Number of frames from devices that were rejected.
InvalidCRC	Invalid CRC detected.
InvalidDestAddr	Invalid destination address detected.
LIP_AL_PD_ALPS	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.
LIP_F8_AL_PS	This LIP denotes a loop failure detected by the L_Port identified by AL_PS.
LIP_F7_F7	A loop initialization primitive frame used to acquire a valid AL_PA.
LIP_F8_F7	A loop initialization primitive frame used to indicate that a loop failure has been detected at the receiver.
Link Failures	Number of optical link failures detected by this port. A link failure is a loss of synchronization or a loss of signal while not in the offline state. A loss of signal causes the 6-port Switch Module 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.
Login	Number of device logins
Logout	Number of device logouts
LoopTimeouts	A two (2) second timeout as specified by FC-AL-2.
LossOfSync	Number of synchronization losses (>100 ms) detected by this port. A loss of synchronization is detected by receipt of an invalid transmission word.

Table 2-15. Show Port Parameters (Continued)

Entry	Description
PrimSeqErrors	Primitive sequence errors detected.
RxLinkResets	Number of link reset primitives received from an attached device.
RxOfflineSeq	Number of offline sequences received. An OLS is issued for link initialization, a Receive & Recognize Not_Operational (NOS) state, or to enter the offline state.
TotalErrors	Total number of errors detected.
TotalLIPsRecvd	Number of loop initialization primitive frames received by this port.
TotalLIPsXmitd	Number of loop initialization primitive frames transmitted by this port.
TotalLinkResets	Total number of link reset primitives.
TotalOfflineSeq	Total number of Offline Sequences issued and received by this port.
TotalRxFrames	Total number of frames received by this port.
TotalRxWords	Total number of words received by this port.
TotalTxFrames	Total number of frames issued by this port.
TotalTxWords	Total number of words issued by this port.
TxLinkResets	Number of Link Resets issued by this port.
TxOfflineSeq	Total number of Offline Sequences issued by this port.

post log

Displays the Power On Self Test (POST) log which contains results from the POST.

setup [option]

Displays setup attributes for the system, SNMP, and the 6-port Switch Module manufacturer. Refer to the ["Show Setup Command" on page 2-81](#).

steering [domain_id]

Displays the routes that data takes to the 6-port Switch Module given by [domain_id]. If you omit [domain_id], the system displays routes for all switches in the fabric.

support

Executes a series of commands that display a complete description of the 6-port Switch Module, its configuration, and operation. The display can be captured from the screen and used for diagnosing problems. This keyword is intended for use at the request of your authorized maintenance provider. The commands that are executed include the following:

- Alias List
- Config List
- Date
- History
- Ps
- Show (About, Alarm, Backtrace, Chassis, Config Port, Config Switch, Config Threshold, Dev, Dev Settings, Domains, Donor, Fabric, Log, Log Settings, Lsdb, Mem, Ns, Perf, Port, Setup Mfg, Setup Snmp, Setup System, Steering, Switch, Topology, Users)
- Uptime
- User Accounts
- Whoami
- Zoneset (Active, List)
- Zoning (History, Limits, List)

switch

Displays 6-port Switch Module operational information. [Table 2-16](#) describes the 6-port Switch Module operational parameters.

Table 2-16. Switch Module Operational Parameters

Parameter	Description
SymbolicName	Descriptive name for the switch module
SwitchWWN	Switch module world wide name
SwitchType	Switch module model
BootVersion	PROM boot version
CreditPool	Number of port buffer credits available to recipient ports
DomainID	Switch module domain ID
FirstPortAddress	FC address of port 0
FlashSize - MBytes	Size of the flash memory in megabytes

Table 2-16. Switch Module Operational Parameters (Continued)

Parameter	Description
LogLevel	Event severity level used to record events in the event log
MaxPorts	Number of ports available on the switch module
NumberOfResets	Number of times the 6-port Switch Module has been reset over its service life
ReasonForLastReset	Action that caused the last reset
SWImageVersion (1) - build date	Firmware image 1 version and build date. This image occupies position 1 in the flash memory.
SWImageVersion (2) - build date	Firmware image 2 version and build date. This image occupies position 2 in the flash memory.
ActiveImageVersion - build date	Firmware image and build date that is active. This is the firmware image that is currently running on the 6-port Switch Module.
PendingImageVersion - build date	Firmware image version and build date that is pending. This image will become active at the next reset or power cycle. The pending firmware points to either SWImageVersion (1) or (2).
ActiveConfiguration	Name of the 6-port Switch Module configuration that is in use.
AdminState	Switch module administrative state
AdminModeActive	Admin session status
BeaconOnStatus	Beacon status as set by the Set Beacon command.
OperationalState	Switch module operational state
PrincipalSwitchRole	Principal switch status. True indicates that this switch is the principal switch.
BoardTemp (1) - Degrees Celsius	Internal switch module temperature at circuit board sensor 1
BoardTemp (2) - Degrees Celsius	Internal switch module temperature at circuit board sensor 2

Table 2-16. Switch Module Operational Parameters (Continued)

Parameter	Description
SwitchDiagnosticsStatus	Results of the power-on self test
SwitchTemperatureStatus	Switch module temperature status: normal, warning, failure

topology

Displays all connected devices.

users

Displays a list of logged-in users. This is equivalent to the User List command.

version

Displays an introductory set of information about operational attributes of the switch. This keyword is equivalent to the About keyword.

Examples The following is an example of the Show Chassis command:

```
Chassis Information
-----
BoardTemp (1) - Degrees Celsius    45
PowerSupplyStatus (1)              Good
HeartBeatCode                       1
HeartBeatStatus                     Normal
```

The following is an example of the Show NS (local domain) command:

```
FCSM6: user1> show ns
Seq Domain   Port   Port
No  ID       ID     Type  COS  PortWWN                NodeWWN
---  -
1   1 (0x1)   010100 N     3    21:00:00:09:6b:00:05:01 20:00:00:09:6b:00:05:00
2   1 (0x1)   010300 N     3    21:00:00:09:6b:20:4f:00 20:00:00:09:6b:00:4f:00
3   1 (0x1)   010f00 N     3    20:05:00:a0:b8:13:03:04 20:04:00:a0:b8:13:03:03
4   1 (0x1)   011300 N     3    21:00:00:e0:8b:0f:99:93 20:00:00:e0:8b:0f:99:93
```


The following is an example of the Show NS [port_ID] command:

```
FCSM6: user1> show ns 010100
  Port ID: 010100
  -----
PortType           N
PortWWN            21:00:00:09:6b:00:05:01
SymbolicPortName   (NULL)
NodeWWN            20:00:00:09:6b:00:05:00
SymbolicNodeName   FW:v3.02.24 DVR:v8.2.3.93 (w32 VI)
NodeIPAddress      0.0.0.0
ClassOfService     3
PortIPAddress      0.0.0.0
FabricPortName     20:01:00:c0:dd:02:13:a0
FC4Type            FCP
FC4Desc            (NULL)
```

The following is an example of the Show Interface command:

```
FCSM6: user1> show interface
eth0      Link encap:Ethernet  HWaddr 00:C0:DD:02:13:9F
          inet addr:10.20.90.103 Bcast:10.20.90.255 Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:239356 errors:0 dropped:0 overruns:0 frame:0
          TX packets:235048 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:28328175 (27.0 Mb)  TX bytes:30490633 (29.0 Mb)
          Interrupt:16

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:226999 errors:0 dropped:0 overruns:0 frame:0
          TX packets:226999 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:16197524 (15.4 Mb)  TX bytes:16197524 (15.4 Mb)
```

The following is an example of the Show Port command:

```
FCSM6: user1> show port 0
  Port Number: 0
  -----
AdminState      Online          PortID          010000
AsicNumber      0              PortWWN         20:00:00:c0:dd:02:13:a0
AsicPort        4              RunningType     Unknown
ConfigType      GL             MediaPartNumber PL-XPL-VC-S23-11
DiagStatus      Passed         MediaRevision
EpConnState     None           MediaType       200-M5-SN-I
EpIsoReason     NotApplicable  MediaVendor     PICOLIGHT
LinkSpeed       Auto           MediaVendorID   00000485
LinkState       Inactive       SymbolicName    Port0
LoginStatus     NotLoggedInIn  SyncStatus      SyncLost
MaxCredit       16            XmitterEnabled  True
OperationalState Offline         PerfTuningMode  Normal

ALInit          9              LIP_F8_AL_PS   0
ALInitError     0              LIP_F8_F7      0
BadFrames       0              LinkFailures    0
Class2FramesIn  0              Login           0
Class2FramesOut 0              Logout          0
Class2WordsIn   0              LoopTimeouts    0
Class2WordsOut  0              LossOfSync      0
Class3FramesIn  0              PrimSeqErrors   0
Class3FramesOut 0              RxLinkResets    0
Class3Toss      0              RxOfflineSeq    0
Class3WordsIn   0              TotalErrors     0
Class3WordsOut  0              TotalLinkResets 0
DecodeErrors    0              TotalLIPsRecvd  0
EpConnects     0              TotalLIPsXmitd  9
FBusy          0              TotalOfflineSeq 27
FlowErrors      0              TotalRxFrames   0
FReject        0              TotalRxWords    0
InvalidCRC      0              TotalTxFrames   0
InvalidDestAddr 0              TotalTxWords    0
LIP_AL_PD_AL_PS 0              TxLinkResets    0
LIP_F7_AL_PS   0              TxOfflineSeq    27
LIP_F7_F7      0
```

The following is an example of the Show Switch command:

```

FCSM6: user1> show switch
Switch Information
-----
SymbolicName                FCSM6
SwitchWWN                   10:00:00:c0:dd:02:13:a0
SwitchType                   SwitchBlade20
BootVersion                  V1.1.0.5-0 (Mon Mar 22 13:12:01 2004)
CreditPool                   0
DomainID                    1 (0x1)
FirstPortAddress             010000
FlashSize - MBytes          128
LogLevel                     Critical
MaxPorts                     20
NumberOfResets               8
ReasonForLastReset           NormalReset
SWImageVersion (1) - build date V4.1.0.19-0 (Thu Jun 10 15:51:31 2004)
SWImageVersion (2) - build date V4.1.0.19-0 (Mon May 3 16:29:04 2004)
ActiveImageVersion - build date V4.1.0.19-0 (Thu Jun 10 15:51:31 2004)
PendingImageVersion - build date V4.1.0.19-0 (Thu Jun 10 15:51:31 2004)
ActiveConfiguration          default
AdminState                   Online
AdminModeActive              False
BeaconOnStatus               False
OperationalState             Online
PrincipalSwitchRole          True
BoardTemp (1) - Degrees Celsius 45
SwitchDiagnosticsStatus      Passed
SwitchTemperatureStatus       Normal

```

The following is an example of the Show Topology command:

```

FCSM6: user1> show topology
Unique ID Key
-----
A = ALPA, D = Domain ID, P = Port ID

```

Port	Loc Type	Local PortWWN	Rem Type	Remote NodeWWN	Unique ID	
Ext2:15	F	20:0f:00:c0:dd:02:13:a0	N	20:04:00:a0:b8:13:03:03	010f00	P
Ext6:19	F	20:13:00:c0:dd:02:13:a0	N	20:00:00:e0:8b:0f:99:93	011300	P
Bay1	F	20:01:00:c0:dd:02:13:a0	N	20:00:00:09:6b:00:05:00	010100	P
Bay3	F	20:03:00:c0:dd:02:13:a0	N	20:00:00:09:6b:00:4f:00	010300	P

The following is an example of the Show Topology command for port 15:

```
FCSM6: user1> show topology 15
  Local Link Information
  -----
Port      Ext2:15
PortID    010f00
PortWWN   20:0f:00:c0:dd:02:13:a0
PortType  F
```

```
Remote Link Information
-----
```

```
Device 0

PortID      010f00
PortWWN     20:05:00:a0:b8:13:03:04
NodeWWN     20:04:00:a0:b8:13:03:03
PortType    N
Description LSI      INF-01-00      (Rev. 0540)
IPAddress   0.0.0.0
```

The following is an example of the Show Version command:

```
FCSM6: user1> show version
*****
*
*      Command Line Interface SHell  (CLISH)
*
*****

SystemDescription  QLogic 6-Port Enterprise Fibre Channel Switch Module for
                  IBM eServer BladeCenter (TM)
Eth0NetworkAddress 192.168.70.129 (use 'set setup system' to update)
MACAddress         00:c0:dd:02:13:9f
WorldWideName      10:00:00:c0:dd:02:13:a0
ChassisSerialNumber 11S442010
SymbolicName       FCSM6
ActiveSWVersion     V4.1.0.19-0
ActiveTimestamp     Thu Jun 10 15:51:31 2004
DiagnosticsStatus   Passed
UserAuthentication  False
```

Show Config Command

Displays 6-port Switch Module, port, alarm threshold, and zoning for the current configuration.

Authority None

Syntax **show config**
 port *[port_number]*
 switch
 threshold
 zoning

Keywords **port *[port_number]***
 Displays configuration parameters for the port number given by *[port_number]*. Ports are numbered beginning with 0. If *[port_number]* is omitted, all ports are specified.

Note: For external ports (0, 15, 16, 17, 18, 19), all parameters apply. For internal ports (1 through 14) only AdminState applies. Ports 1–14 apply to BladeCenter unit Type 8677. Ports 1–8 apply to BladeCenter T unit Types 8720 and 8730; ports 9–14 are not used. For information about port numbering and mapping, see [Table A-1](#).

switch
 Displays configuration parameters for the switch.

threshold
 Displays alarm threshold parameters for the switch.

zoning
 Displays zoning configuration parameters for the switch.

Examples The following is an example of the Show Config Port command:

```
FCSM6: user1> show config port 15
  Port Number: 15
  -----
  AdminState           Offline
  LinkSpeed            Auto
  PortType             GL
  SymbolicName         Port15
  ALFairness           False
  DeviceScanEnabled    True
  ForceOfflineRSCN     False
  ARB_FF               False
  InteropCredit        0
  ExtCredit            0
  FANEnabled           True
```

```
AutoPerfTuning      False
LCFEnabled          False
MFSEnabled          True
MSEnabled           True
NoClose             False
IOStreamGuard       Disabled
VIEEnabled          False
PDISCPingEnable     True
```

The following is an example of the Show Config Switch command:

```
FCSM6: user1> show config switch
Configuration Name: default
-----
Switch Configuration Information
-----
AdminState           Online
BroadcastEnabled     False
InbandEnabled        True
FDMIEnabled          False
FDMIEntries          10
DomainID             19 (0x13)
DomainIDLck          True
SymbolicName         FCSM6
R_A_TOV              10000
E_D_TOV              2000
PrincipalPriority     254
ConfigDescription    QLogic 6-Port Enterprise Fibre Channel Switch Module
ConfigLastSavedBy    USERID@OB-session5
ConfigLastSavedOn    day month date time year
FC-SW-2 Compliant    True
Legacy Address Format False1
```

¹ Appears only if FC-SW-2 Compliant is False.

The following is an example of the Show Config Threshold command:

```
FCSM6: user1> show config threshold
Configuration Name: default
-----

Threshold Configuration Information
-----
ThresholdMonitoringEnabled      False
CRCErrorsMonitoringEnabled     True
RisingTrigger                  25
FallingTrigger                 1
SampleWindow                   10
DecodeErrorsMonitoringEnabled  True
RisingTrigger                  25
FallingTrigger                 0
SampleWindow                   10
ISLMonitoringEnabled           True
RisingTrigger                  2
FallingTrigger                 0
SampleWindow                   10
LoginMonitoringEnabled         True
RisingTrigger                  5
FallingTrigger                 1
SampleWindow                   10
LogoutMonitoringEnabled       True
RisingTrigger                  5
FallingTrigger                 1
SampleWindow                   10
LOSMonitoringEnabled           True
RisingTrigger                  100
FallingTrigger                 5
SampleWindow                   10
```

The following is an example of the Show Config Zoning command:

```
FCSM6: user1> show config zoning
```

```
Configuration Name: default
```

```
-----
```

```
Zoning Configuration Information
```

```
-----
```

```
FC-SW-2 AutoSave      True
```

```
Default Visibility    All
```


Show Log Command

Displays the contents of the log or the parameters used to create entries in the log. The log contains a maximum of 200 entries. When the log reaches its entry capacity, subsequent entries overwrite the existing entries, beginning with the oldest.

Authority None

Syntax **show log**
 component
 level
 options
 port
 settings

Keywords **component**
Displays the components currently being monitored for events. The components are as follows:

All

Monitors all components.

Chassis

Monitors chassis hardware components such as fans and power supplies.

Eport

Monitors all E_Ports.

Mgmtserver

Monitors management server status.

Nameserver

Monitors name server status.

None

Monitor none of the component events.

Other

Monitors other miscellaneous events.

Port

Monitors all port events

Switch

Monitors switch management events.

Zoning

Monitors zoning conflict events.

level

Displays the event severity level needed to create an entry in the log. If the severity level occurs on a port or on a component which is not defined, no entry is made in the log. The severity levels are as follows:

- Critical
Monitors critical events.
- Warn
Monitors warning events.
- Info
Monitors informational events.
- None
Monitors none of the severity levels.

options

Displays the options used to set the component and severity level attributes.

port

Displays the ports being monitored for events. If an event occurs which is of the defined level and on a defined component, but not on a defined port, no entry is made in the log.

settings

Displays the current settings for component, level and port. This command is equivalent to executing the following commands separately: Show Log Component, Show Log Level, and Show Log Port.

Examples

The following is an example of the Show Log Component command:

```
FCSM6: user1> show log component

Current setting(s) for log component: NameServer
```

The following is an example of the Show Log Level command:

```
FCSM6: user1> show log level

Current settings for log
-----
level      Critical
```

The following is an example of the Show Log Options command:

```
FCSM6: user1> show log options

Allowed options for log
-----

component  All, None, NameServer, MgmtServer, Zoning, Switch, Chassis, Blade,
           Port, Eport, Snmp, Other

level      Critical,Warn,Info,None
```

The following is an example of the Show Log command:

```
FCSM6: user1> show log
[327][day month date time year][I][Eport Port:0/8][Eport State=
E_A0_GET_DOMAIN_ID]
[328][day month date time year][I][Eport Port: 0/8][FSPF PortUp state=0]
[329][day month date time year][I][Eport Port: 0/8][Sending init hello]
[330][day month date time year][I][Eport Port: 0/8][Processing EFP, oxid= 0x8]
[331][day month date time year][I][Eport Port: 0/8][Eport State = E_A2_IDLE]
[332][day month date time year][I][Eport Port: 0/8][EFP,WWN= 0x100000c0dd00b845,
len= 0x30]
[333][day month date time year][I][Eport Port: 0/8][Sending LSU oxid=0xc:type=1]
[334][day month date time year][I][Eport Port: 0/8][Send Zone Merge Request]
[335][day month date time year][I][Eport Port: 0/8][LSDB Xchg timer set]
[336][day month date time year][I][Eport Port: 0/8][Setting attribute
Oper.UserPort.0.8.EpConnState Connected]
```

Show Perf Command

Displays port performance in frames/second and bytes/second. If you omit the keyword, the command displays data transmitted (out), data received (in), and total data transmitted and received in frames/second and bytes per second.

Authority None

Syntax **show perf**
byte
inbyte
outbyte
frame
inframe
outframe
errors

Keywords **byte**

Displays continuous performance data in total bytes/second transmitted and received for all ports. Type any character to stop the display.

inbyte

Displays continuous performance data in bytes/second received for all ports. Type any character to stop the display.

outbyte

Displays continuous performance data in bytes/second transmitted for all ports. Type any character to stop the display.

frame

Displays continuous performance data in total frames/second transmitted and received for all ports. Type any character to stop the display.

inframe

Displays continuous performance data in frames/second received for all ports. Type any character to stop the display.

outframe

Displays continuous performance data in frames/second transmitted for all ports. Type any character to stop the display.

errors

Displays continuous error counts for all ports. Type any character to stop the display.

Keywords The following is an example of the Show Perf command:

```
FCSM6: user1> show perf
```

Port	Bytes/s (in)	Bytes/s (out)	Bytes/s (total)	Frames/s (in)	Frames/s (out)	Frames/s (total)
Ext1:0	0	0	0	0	0	0
Ext2:15	49M	3M	52M	32K	2K	34K
Ext3:16	0	0	0	0	0	0
Ext4:17	0	0	0	0	0	0
Ext5:18	0	0	0	0	0	0
Ext6:19	0	0	0	0	0	0
Bay1	2M	23M	26M	1K	15K	17K
Bay2	0	0	0	0	0	0
Bay3	1M	25M	26M	972	16K	17K
Bay4	0	0	0	0	0	0
Bay5	0	0	0	0	0	0
Bay6	0	0	0	0	0	0
Bay7	0	0	0	0	0	0
Bay8	0	0	0	0	0	0
Bay9	0	0	0	0	0	0
Bay10	0	0	0	0	0	0
Bay11	0	0	0	0	0	0
Bay12	0	0	0	0	0	0
Bay13	0	0	0	0	0	0
Bay14	0	0	0	0	0	0

The following is an example of the Show Perf Byte command:

```
FCSM6: user1> show perf byte
```

```
  Displaying bytes/sec (total)...  (Press any key to stop display)
```

0	15	16	17	18	19	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	63M	0	0	0	0	31M	0	31M	0	0	0	0	0	0	0	0	0	0	0
0	65M	0	0	0	0	31M	0	34M	0	0	0	0	0	0	0	0	0	0	0
0	60M	0	0	0	0	29M	0	30M	0	0	0	0	0	0	0	0	0	0	0
0	62M	0	0	0	0	28M	0	33M	0	0	0	0	0	0	0	0	0	0	0
0	58M	0	0	0	0	26M	0	31M	0	0	0	0	0	0	0	0	0	0	0
0	52M	0	0	0	0	26M	0	26M	0	0	0	0	0	0	0	0	0	0	0
0	61M	0	0	0	0	34M	0	26M	0	0	0	0	0	0	0	0	0	0	0
0	58M	0	0	0	0	29M	0	28M	0	0	0	0	0	0	0	0	0	0	0
0	54M	0	0	0	0	28M	0	26M	0	0	0	0	0	0	0	0	0	0	0
0	66M	0	0	0	0	32M	0	34M	0	0	0	0	0	0	0	0	0	0	0
0	64M	0	0	0	0	35M	0	29M	0	0	0	0	0	0	0	0	0	0	0
0	59M	0	0	0	0	30M	0	29M	0	0	0	0	0	0	0	0	0	0	0
0	56M	0	0	0	0	26M	0	29M	0	0	0	0	0	0	0	0	0	0	0
0	54M	0	0	0	0	26M	0	27M	0	0	0	0	0	0	0	0	0	0	0
0	50M	0	0	0	0	24M	0	25M	0	0	0	0	0	0	0	0	0	0	0
0	61M	0	0	0	0	31M	0	30M	0	0	0	0	0	0	0	0	0	0	0

Show Setup Command

Displays the current SNMP and system settings.

Authority None

Syntax **show setup**
mfg
snmp
system

Keywords **mfg**
Displays manufacturing information about the 6-port Switch Module.

snmp
Displays the current SNMP settings.

system
Displays the current system settings.

Examples The following is an example of the Show Setup Mfg command:

```
FCSM6: user1> show setup mfg
Manufacturing Information
-----
BrandName           QLogic
BuildDate           Unknown
ChassisPartNumber   SB20-SDV
ChassisSerialNumber 000015889
CPUBoardSerialNumber 000015889
MACAddress          00:c0:dd:01:6e:54
PlanarPartNumber    31106-02 A
SwitchSymbolicName  FCSM6
SwitchWWN           10:00:00:c0:dd:01:6e:55
SystemDescription   QLogic 6-Port Enterprise Fibre Channel Switch Module for
                    IBM eServer BladeCenter (TM)
SystemObjectID      1.3.6.1.4.1.1663.1.1.1.1.22
```

The following is an example of the Show Setup Snmp command:

```
FCSM6: user1> show setup snmp
SNMP Information
-----
SnmpEnabled           True
Contact               <sysContact undefined>
Location              <sysLocation undefined>
Description            QLogic 6-Port Enterprise Fibre Channel Switch Module for
                      IBM eServer BladeCenter (TM)
Trap1Address          10.20.32.110
Trap1Port              162
Trap1Severity         warning
Trap1Version           1
Trap1Enabled           True
Trap2Address           0.0.0.0
Trap2Port              162
Trap2Severity         warning
Trap2Version           2
Trap2Enabled           False
Trap3Address           0.0.0.0
Trap3Port              162
Trap3Severity         warning
Trap3Version           2
Trap3Enabled           False
Trap4Address           0.0.0.0
Trap4Port              162
Trap4Severity         warning
Trap4Version           2
Trap4Enabled           False
Trap5Address           0.0.0.0
Trap5Port              162
Trap5Severity         warning
Trap5Version           2
Trap5Enabled           False
ObjectID              1.3.6.1.4.1.1663.1.1.1.1.22
AuthFailureTrap       False
ProxyEnabled          True
```


The following is an example of the Show Setup System command:

```
FCSM6: user1> show setup system
  System Information
  -----
Eth0NetworkDiscovery      Static
Eth0NetworkAddress       192.168.70.129
Eth0NetworkMask          255.255.255.0
Eth0GatewayAddress       0.0.0.0
AdminTimeout              30
InactivityTimeout        10
TempMonitoringWarning     75
TempMonitoringFailure    80
TempFailurePortShutdown  False
UserAuthentication       False
LocalLogEnabled           True
RemoteLogEnabled          False
RemoteLogHostAddress     10.0.0.254
NTPClientEnabled         False
NTPServerAddress         10.0.0.254
EmbeddedGUIEnabled       True
```

Shutdown Command

Terminates all data transfers on the 6-port Switch Module at convenient points and closes the Telnet session. Always power cycle the 6-port Switch Module after entering this command.

Authority Admin session

Syntax **shutdown**

Notes Always use this command to perform an orderly shut down before removing power from the 6-port Switch Module.

Test Command

Tests ports using internal (SerDes level), external (transceiver), and online loopback tests. Internal and external tests require that the port be placed in diagnostic mode. Refer to the ["Set Command" on page 2-33](#) for information about changing the port administrative state. While the test is running, the remaining ports on the 6-port Switch Module remain fully operational.

Authority Admin session

Syntax **test**
port [port_number] [test_type]
cancel
status

Keywords **port [port_number] [test_type]**
Tests the port given by [port_number] using the test given by [test_type]. If you omit [test_type], Internal is used. [test_type] can have the following values:

- internal
Tests the SerDes. This is the default. The port must be in diagnostics mode to perform this test.
- external
Tests both the SerDes and transceiver. The port must be in diagnostics mode to perform this test, and a loopback plug must be installed in the transceiver.
- online
Tests 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 if the test frame that was sent by the ASIC matches the frame that is received. This test does not disrupt communication on the port.

cancel
Cancels the online test in progress.

status
Displays the status of a test in progress, or if there is no test in progress, the status of the test that was executed last.

Examples To run an internal or external port test, do the following:

1. To start an admin session, enter the following command and press the Enter key.

```
admin start
```

2. Place the port in Diagnostics mode, enter the following command (x = port number) and press the Enter key.

```
set port x state diagnostics
```

3. Choose the type of port loopback test to run:

- To run an internal loopback test, enter the following:

```
test port x internal
```

- To run an external loopback test, enter the following command. A loopback plug must be installed for this test to pass.

```
test port x external
```

4. A series of test parameters are displayed on the screen. Press the Enter key to accept each default parameter value, or type a new value for each parameter and press the Enter key. The TestLength parameter is the number of frames sent, the FrameSize (256 byte maximum in some cases) parameter is the number of bytes in each frame, and the DataPattern parameter is the pattern in the payload.
5. After the test type has been chosen and the command executed, a message on the screen will appear detailing the test results.
6. After the test is run, put the port back into online state by entering the following command (x = port number) and pressing the Enter key.

```
set port x state online
```

7. To verify port is back online, enter the following command and press the Enter key. The contents of the AdminState field should display be "Online".

```
show port x
```

The online loopback (node-to-node) test requires that port be online and connected to a remote device. To run the online loopback test, do the following:

1. To start an admin session, enter the following command and press the Enter key.

```
admin start
```

2. To run the online loopback test, enter the following command and press the Enter key.

```
test port x online
```

3. A series of test parameters are displayed on the screen. Press the Enter key to accept each default parameter value, or type a new value for each parameter and press the Enter key. The TestLength parameter is the number of frames sent, the FrameSize (256 byte maximum in some cases) parameter is the number of bytes in each frame, and the DataPattern parameter is the pattern in the payload. Before running the test, make sure that the device attached to the port can handle the test parameters.

```
FCSM6 (admin): user1> test port x online
```

```
A list of attributes with formatting and current values will follow. Enter a new value or simply press the ENTER key to accept the default value. If you wish to terminate this process before reaching the end of the list press 'q' or 'Q' and the ENTER key to do so.
```

```
TestLength      (decimal value, 1-4294967295)  [100    ]
FrameSize       (decimal value, 36-2148)           [256    ]
DataPattern     (32-bit hex value or 'Default') [Default]
StopOnError     (True/False)                          [False  ]
Do you want to start the test? (y/n) [n]
```

4. After all parameter values are defined, press the Y key to start the test. After the command executes, a message on the screen will appear detailing the test results.

Uptime Command

Displays the elapsed up time since the 6-port Switch Module was last reset and reset method. A hot reset or non-disruptive firmware activation does not reset the elapsed up time reported by this command.

Authority None

Syntax `uptime`

Examples The following is an example of the Uptime command:

```
FCSM6: user1> uptime
```

```
Elapsed up time : 0 day(s), 2 hour(s), 28 min(s), 44 sec(s)
Reason last reset: NormalReset
```

User Command

Administers and displays user accounts.

Authority USERID account name and an Admin session. The Accounts and List keywords are available to all account names without an Admin session.

Syntax **user**
accounts
add
delete [account_name]
edit
list

Keywords **accounts**
Displays all user accounts that exist on the switch. This keyword is available to all account names without an Admin session.

add

Add a user account to the 6-port Switch Module. You will be prompted for an account name, a password, authority, and an expiration date.

- A 6-port Switch Module can have a maximum of 15 user accounts.
- Account names are limited to 15 characters; passwords must be 4–20 characters.
- Admin authority grants permission to use the Admin command to open an admin session, from which all commands can be entered. Without Admin authority, you are limited to view-only commands.
- The expiration date is expressed in the number of days until the account expires (2000 maximum). The 6-port Switch Module will issue an expiration alarm every day for seven days prior to expiration. 0 (zero) specifies that the account has no expiration date.

delete [account_name]

Deletes the account name given by [account_name] from the switch.

edit

Initiates an edit session that prompts you for the account name for which to change the expiration date and authority.

list

Displays the list of users currently logged in and their session numbers. Provides the same function as the Show Users command. This keyword is available to all account names without an Admin session.

Notes

- User accounts are enforced in SAN Utility only if the UserAuthentication parameter is set to True. The UserAuthentication default value is False. Refer to System keyword of the ["Set Setup Command"](#) on page 2-52 for information about setting the UserAuthentication parameter.
- Authority level or password changes that you make to an account that is currently logged in do not take effect until that account logs in again.

Examples

The following is an example of the User Accounts command:

```
FCSM6 (admin): user1> user accounts
```

```

Current list of user accounts
-----
images      (admin authority = False, never expires)
USERID      (admin authority = True , never expires)
user1       (admin authority = True , never expires)
user2       (admin authority = False, expires in < 50 days)
user3       (admin authority = True , expires in < 100 days)
```

The following is an example of the User Add command:

```
FCSM6 (admin): userid> user add
Press 'q' and the ENTER key to abort this command.
account name (1-15 chars)      : user1
account password (4-20 chars)  : *****

please confirm account password: *****

set account expiration in days (0-2000, 0=never): [0] 100

should this account have admin authority? (y/n): [n] y

OK to add user account 'user1' with admin authority
and to expire in 100 days?

Please confirm (y/n): [n] y
```


The following is an example of the User Edit command:

```
FCSM6 (admin): userid> user edit
```

```
Press 'q' and the ENTER key to abort this command.
```

```
account name (1-15 chars)      : user1
set account expiration in days (0-2000, 0=never): [0]
should this account have admin authority? (y/n): [n]
```

```
OK to modify user account 'user1' with no admin authority
and to expire in 0 days?
```

```
Please confirm (y/n): [n]
```

The following is an example of the User Delete command:

```
FCSM6 (admin): userid> user del user3
```

```
The user account will be deleted. Please confirm (y/n): [n] y
```

The following is an example of the User List command:

```
FCSM6 (admin): user1> user list
```

User	Ethernet Addr-Port	Logged in Since
----	-----	-----
USERID@OB-session1	10.20.68.108-1031	day month date time year
USERID@OB-session2	10.20.68.108-1034	day month date time year
snmp@OB-session3	Unknown	day month date time year
snmp@IB-session4	Unknown	day month date time year
user1@OB-session5	Unknown	day month date time year

Whoami Command

Displays the account name, session number, and 6-port Switch Module domain ID for the Telnet session.

Authority None

Syntax **whoami**

Examples The following is an example of the Whoami command:

```
FCSM6: admin> whoami
```

```
User name            : USERID@session2
```

```
Switch name         : FCSM6
```

```
Switch domain ID: 21 (0x15)
```

Zone Command

Manages zones and zone membership on a switch.

Authority Admin session and a Zoning Edit session. Refer to the ["Zoning Command" on page 2-99](#) for information about starting a Zoning Edit session. The List, Members, and Zonesets keywords are available without an Admin session.

Syntax

zone

- add [zone] [member_list]
- copy [zone_source] [zone_destination]
- create [zone]
- delete [zone]
- list
- members [zone]
- remove [zone] [member_list]
- rename [zone_old] [zone_new]
- type [zone] [zone_type]
- zonesets [zone]

Keywords **add [zone] [member_list]**
Specifies one or more ports/devices given by [members] to add to the zone named [zone]. Use a <space> to delimit aliases and ports/devices in [member_list]. A zone can have a maximum of 2000 members. [member_list] can have any of the following formats:

- Domain ID and port number pair (Domain ID, Port Number). Domain IDs can be 1–239; port numbers can be 0–255.
- 6-character hexadecimal device Fibre Channel address (hex)
- 16-character hexadecimal worldwide port name (WWPN) with the format xx:xx:xx:xx:xx:xx:xx:xx.
- Alias name

The application verifies that the [members] format is correct, but does not validate that such a member exists.

copy [zone_source] [zone_destination]

Creates a new zone named [zone_destination] and copies the membership into it from the zone given by [zone_source].

create [zone]

Creates a zone with the name given by [zone]. An zone name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, \$, ^, and -. The zoning database supports a maximum of 1000 zones.

delete [zone]

Deletes the specified zone given by [zone] from the zoning database. If the zone is a component of the active zone set, the zone will not be removed from the active zone set until the active zone set is deactivated.

list

Displays a list of all zones and the zone sets of which they are components. This keyword does not require an Admin session.

members [zone]

Displays all members of the zone given by [zone]. This keyword does not require an Admin session.

remove [zone] [member_list]

Removes the ports/devices given by [member_list] from the zone given by [zone]. Use a <space> to delimit aliases and ports/devices in [member_list].

[member_list] can have any of the following formats:

- Domain ID and port number pair (Domain ID, Port Number). Domain IDs can be 1–239; port numbers can be 0–255.
- 6-character hexadecimal device Fibre Channel address (hex)
- 16-character hexadecimal worldwide port name (WWPN) with the format xx:xx:xx:xx:xx:xx:xx:xx.
- Alias name

rename [zone_old] [zone_new]

Renames the zone given by [zone_old] to the zone given by [zone_new].

type [zone] [zone_type]

Specifies the zone type given by [zone_type] to be assigned to the zone name given by [zone]. If you omit the [zone_type], the system displays the zone type for the zone given by [zone]. [zone_type] can be one of the following:

soft – name server zone

hardACL – Access control list hard zone. This keyword is case sensitive.

zonesets [zone]

Displays all zone sets of which the zone given by [zone] is a component. This keyword does not require an Admin session.

Examples The following is an example of the Zone List command:

```
FCSM6: user1> zone list
```

```
Zone          ZoneSet
-----
wnn_b0241f
                zone_set_1

wnn_23bd31
                zone_set_1

wnn_221416
                zone_set_1

wnn_2215c3
                zone_set_1

wnn_0160ed
                zone_set_1

wnn_c001b0
                zone_set_1

wnn_401248
                zone_set_1

wnn_02402f
                zone_set_1

wnn_22412f
                zone_set_1
```

The following is an example of the Zone Members command:

```
FCSM6: user1> zone members wnn_b0241f
```

```
Current List of Members for Zone: wnn_b0241f
-----
50:06:04:82:bf:d2:18:c2
50:06:04:82:bf:d2:18:d2
21:00:00:e0:8b:02:41:2f
```

The following is an example of the Zone Zonesets command:

```
FCSM6: user1> zone zonesets zone1
```

```
Current List of ZoneSets for Zone: zone1
```

```
-----  
zone_set_1
```

Zoneset Command

Manages zone sets and component zones across the fabric.

Authority Admin session and a Zoning Edit session. Refer to the ["Zoning Command" on page 2-99](#) for information about starting a Zoning Edit session. The Active, List, and Zones keywords are available without an Admin session. You must close the Zoning Edit session before using the Activate and Deactivate keywords.

Syntax

```
zoneset  
  activate [zone_set]  
  active  
  add [zone_set] [zone_list]  
  copy [zone_set_source] [zone_set_destination]  
  create [zone_set]  
  deactivate  
  delete [zone_set]  
  list  
  remove [zone_set] [zone_list]  
  rename [zone_set_old] [zone_set_new]  
  zones [zone_set]
```

Keywords

activate [zone_set]
Activates the zone set given by [zone_set]. This keyword deactivates the active zone set. Close the Zoning Edit session before using this keyword.

active
Displays the name of the active zone set. This keyword does not require Admin session.

add [zone_set] [zone_list]
Adds a list of zones and aliases given by [zone_list] to the zone set given by [zone_set]. Use a <space> to delimit zone and alias names in [zone_list].

copy [zone_set_source] [zone_set_destination]
Creates a new zone set named [zone_set_destination] and copies into it the zones from the zone set given by [zone_set_source].

create [zone_set]
Creates the zone set with the name given by [zone_set]. 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 -. The zoning database supports a maximum of 256 zone sets.

deactivate
Deactivates the active zone set. Close the Zoning Edit session before using this keyword.

delete [zone_set]
Deletes the zone set given by [zone_set]. If the specified zone set is active, the command is suspended until the zone set is deactivated.

list

Displays a list of all zone sets. This keyword does not require an Admin session.

remove [zone_set] [zone_list]

Removes a list of zones given by [zone_list] from the zone set given by [zone_set]. Use a <space> to delimit zone names in [zone_list]. If [zone_set] is the active zone set, the zone will not be removed until the zone set has been deactivated.

rename [zone_set_old] [zone_set_new]

Renames the zone set given by [zone_set_old] to the name given by [zone_set_new]. You can rename the active zone set.

zones [zone_set]

Displays all zones that are components of the zone set given by [zone_set]. This keyword does not require an Admin session.

Notes

- A zone set must be active for its definitions to be applied to the fabric.
- Only one zone set can be active at one time.
- A zone can be a component of more than one zone set.

Examples

The following is an example of the Zoneset Active command:

```
FCSM6: user1> zoneset active

ActiveZoneSet      Bets
LastActivatedBy    USERID@OB-session6
LastActivatedOn    day month date time year
```

The following is an example of the Zoneset List command:

```
FCSM6: user1> zoneset list

Current List of ZoneSets
-----
alpha
beta
```

The following is an example of the Zoneset Zones command:

```
FCSM6: user1> zoneset zones ssss

Current List of Zones for ZoneSet: ssss
-----
zone1
zone2
zone3
```


Zoning Command

Opens a Zoning Edit session in which to create and manage zone sets and zones. Refer to the ["Zone Command" on page 2-93](#) and the ["Zoneset Command" on page 2-97](#).

Authority Admin session except for the Active, History, Limits, and List keywords.

Syntax **zoning**
active
cancel
clear
edit
history
limits
list
restore
save

Keywords **active**
Displays information for the active zone set including component zones and zone members. This keyword does not require an Admin session.

cancel
Closes the current Zoning Edit session. Any unsaved changes are lost.

clear
Clears all inactive zone sets from the volatile edit copy of the zoning database. This keyword does not affect the non-volatile zoning database. However, if you enter the Zoning Clear command followed by the Zoning Save command, the non-volatile zoning database will be cleared from the switch.

Note: The preferred method for clearing the zoning database from the 6-port Switch Module is the Reset Zoning command.

edit
Opens a Zoning Edit session.

history
Displays a history of zoning modifications. This keyword does not require an Admin session. History information includes the following:

- Time of the most recent zone set activation or deactivation and the user who performed it
- Time of the most recent modifications to the zoning database and the user who made them.
- Checksum for the zoning database

limits

Displays the number of zone sets, zones, aliases, members per zone, members per alias, and total members in the zoning database. This keyword also displays the 6-port Switch Module zoning database limits, excluding the active zone set, which are described in [Table 2-17](#). This keyword does not require an Admin session.

Table 2-17. Zoning Database Limits

Limit	Description
MaxZoneSets	Maximum number of zone sets (256)
MaxZones	Maximum number of zones (1000)
MaxAliases	Maximum number of aliases (2500)
MaxTotalMembers	Maximum number of zone and alias members (10000) that can be stored in the switch's zoning database.
MaxZonesInZoneSets	Maximum number of zones that are components of zone sets (1000), excluding those in the orphan zone set, that can be stored in the switch's zoning database. Each instance of a zone in a zone set counts toward this maximum.
MaxMembersPerZone	Maximum number of members in a zone (2000)
MaxMembersPerAlias	Maximum number of members in an alias (2000)

list

Lists all fabric zoning definitions. This keyword does not require an Admin session.

restore

Reverts the changes to the zoning database that have been made during the current Zoning Edit session since the last Zoning Save command was entered.

save

Saves changes made during the current Zoning Edit session. The system will inform you that the zone set must be activated to implement any changes. This does not apply if you entered the Zoning Clear command during the Zoning Edit session.

Examples

The following is an example of the Zoning Edit command:

```
FCSM6: user1> admin start

FCSM6 (admin): user1> zoning edit

FCSM6 (admin-zoning): user1>
```

```
.
.
FCSM6 (admin-zoning): user1> zoning cancel

    Zoning edit mode will be canceled. Please confirm (y/n): [n] y

FCSM6 (admin): user1> admin end
```

The following is an example of the Zoning Limits command:

```
FCSM6: user1> zoning limits
```

Zoning Attribute	Maximum	Current	[Name]
MaxZoneSets	256	6	
MaxZones	256	19	
MaxAliases	256	1	
MaxTotalMembers	2000	166	
MaxZonesInZoneSets	1000	19	
MaxMembersPerZone	2000		
		10	D_1_JBOD_1
		23	D_1_Photons
		9	D_2_JBOD1
		16	D_2_NewJBOD_2
		5	E1JBOD1
		5	E2JBOD2
		3	LinkResetZone
		3	LinkResetZone2
		8	NewJBOD1
		8	NewJBOD2
		12	Q_1Photon1
		12	Q_2Photon2
		8	Q_1_NewJBOD1
		13	Q_1_Photon_1
		8	Q_2_NewJBOD2
		13	Q_2_Photon_2
		3	ZoneAlias
		3	ZoneDomainPort
		4	ZoneFCAddr
MaxMembersPerAlias	2000		
		2	AliasInAZone

The following is an example of the Zoning List command:

```
FCSM6: user1> zoning list
```

Active ZoneSet Information

ZoneSet	Zone	ZoneMember

wnn		
	wnn_b0241f	
		50:06:04:82:bf:d2:18:c2
		50:06:04:82:bf:d2:18:d2
		21:00:00:e0:8b:02:41:2f
	wnn_23bd31	
		50:06:04:82:bf:d2:18:c2
		50:06:04:82:bf:d2:18:d2
		10:00:00:00:c9:23:bd:31
	wnn_221416	
		50:06:04:82:bf:d2:18:c2
		50:06:04:82:bf:d2:18:d2
		10:00:00:00:c9:22:14:16
	wnn_2215c3	
		50:06:04:82:bf:d2:18:c2
		50:06:04:82:bf:d2:18:d2
		10:00:00:00:c9:22:15:c3

Configured Zoning Information

ZoneSet	Zone	ZoneMember

wnn		
	wnn_b0241f	
		50:06:04:82:bf:d2:18:c2
		50:06:04:82:bf:d2:18:d2
		21:00:00:e0:8b:02:41:2f
	wnn_23bd31	
		50:06:04:82:bf:d2:18:c2
		50:06:04:82:bf:d2:18:d2
		10:00:00:00:c9:23:bd:31

```
wwn_221416
    50:06:04:82:bf:d2:18:c2
    50:06:04:82:bf:d2:18:d2
    10:00:00:00:c9:22:14:16
```

```
wwn_2215c3
    50:06:04:82:bf:d2:18:c2
    50:06:04:82:bf:d2:18:d2
    10:00:00:00:c9:22:15:
```

Notes

Section 3

Using SAN Utility

You can use the SAN Utility application to access and configure Fibre Channel switch modules. For information about installing, uninstalling, and starting the SAN Utility application, see the *QLogic 6-Port Enterprise Fibre Channel Switch Module for IBM Eserver BladeCenter Installation Guide*. The SAN Utility application can be installed on a server or an external network management workstation configured with one of the operating systems described in the *QLogic 6-Port Enterprise Fibre Channel Switch Module for IBM Eserver BladeCenter Installation Guide*.

Online help is available for the SAN Utility application and its functions. The two ways to open the online help file are:

- Open the Help menu and select **Help Topics**
- Click the **Help** button in the tool bar.

Choose the Help button to display context-sensitive help for SAN Utility windows.

3.1

Fabric Management Workstation

The requirements for fabric management workstations running SAN Utility are described in [Table 3-1](#):

Table 3-1. Management Workstation Requirements

Operating System	<ul style="list-style-type: none">■ Windows NT® 4.0/2000/2003■ Linux Red Hat® 7.2, Gnome™ 1.4■ Solaris 2.8/2.9, CDE
Memory	256 MB or more
Disk Space	150 MB per installation
Processor	500 MHz or faster
Hardware	CD-ROM drive, RJ-45 Ethernet port, RS-232 serial port (optional)
Internet Browser	Microsoft® Internet Explorer® 5.0 and later Netscape Navigator® 4.72 and later Mozilla™ 1.02 and later

Telnet workstations require an operating system with a Telnet client.

3.2 SAN Browser

The switch module contains a web server interface known as SAN Browser. This server enables a web-based client to establish a web-interface session with the Fibre Channel switch module. One instance of the SAN Browser can be run at a time by opening the switch IP address with a web browser. The switch module comes from the factory with the SAN Browser enabled, but you can disable it using the EmbeddedGUIEnabled parameter of the Set Setup System command. Refer to "[Set Setup Command](#)" on page 2-52 for more information.

The SAN Browser possesses the same capabilities and features as the workstation-based SAN Utility with the following exceptions:

- Management is limited to a single fabric
- Zoning Wizard is excluded
- SAN Utility Performance View is excluded
- Condensed online help

Note: Before configuring your 6-port Switch Module, be sure that the management modules in your server unit are properly configured. In addition, to access and manage your 6-port Switch Module from an external environment, you might need to enable features, such as the external ports and external management over all ports.

3.3 SAN Utility User Interface

Note: The sample screens that appear in this document may differ from the screens displayed by your system. Screen content varies based on the type of server unit that you are using and the options that are installed.

To manage your switch modules and fabrics, the SAN Utility application provides two basic windows: Topology and Faceplate. The Topology window and Faceplate window share the following common elements:

- [Menu Bars](#)
- [Tool Bar](#)
- [Fabric Tree](#)
- [Graphic Window](#)
- [Data Window and Tabs](#)
- [Working Status Indicator](#)

The Topology window displays all enabled switch modules and the connections between switch modules and other devices, as shown in [Figure 3-1](#).

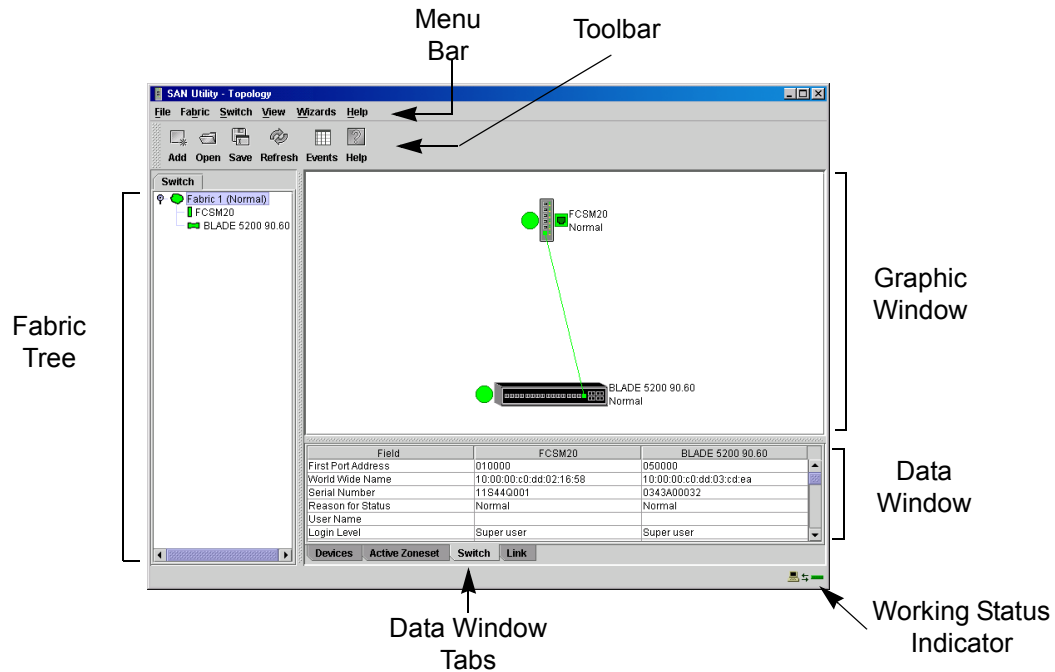


Figure 3-1. Topology Window

The Faceplate window displays the front of a switch module and its active ports. The Faceplate window for a 6-port Switch Module installed in a BladeCenter unit is shown in [Figure 3-2](#). The Faceplate window for a 6-port Switch Module installed in a BladeCenter T unit is shown in [Figure 3-2](#).

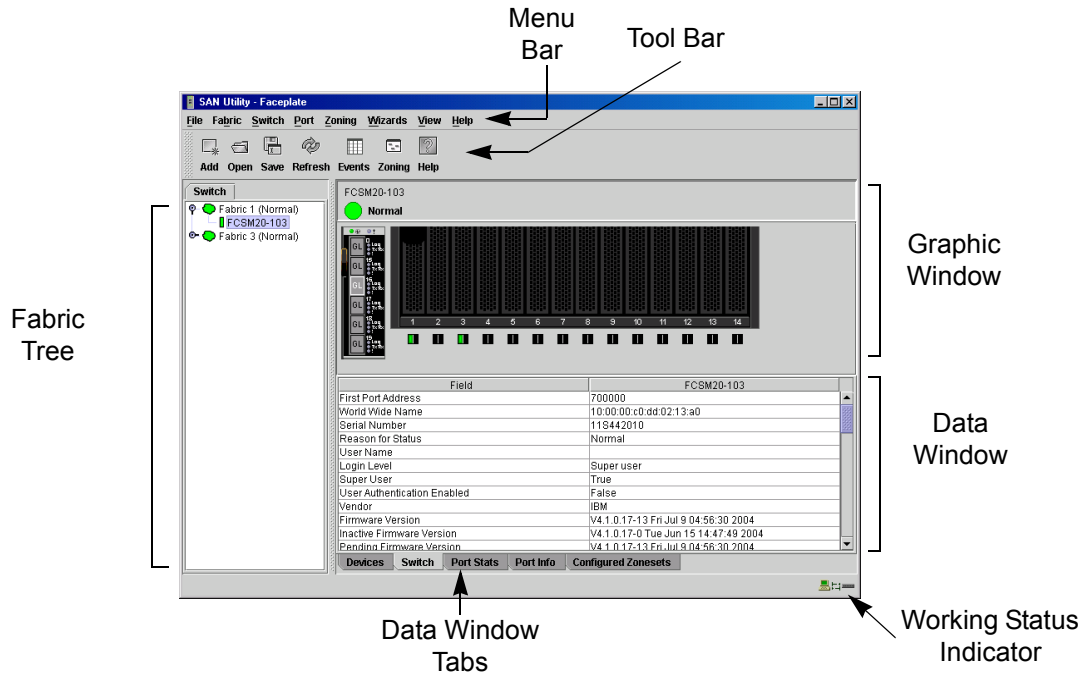


Figure 3-2. BladeCenter Faceplate Window

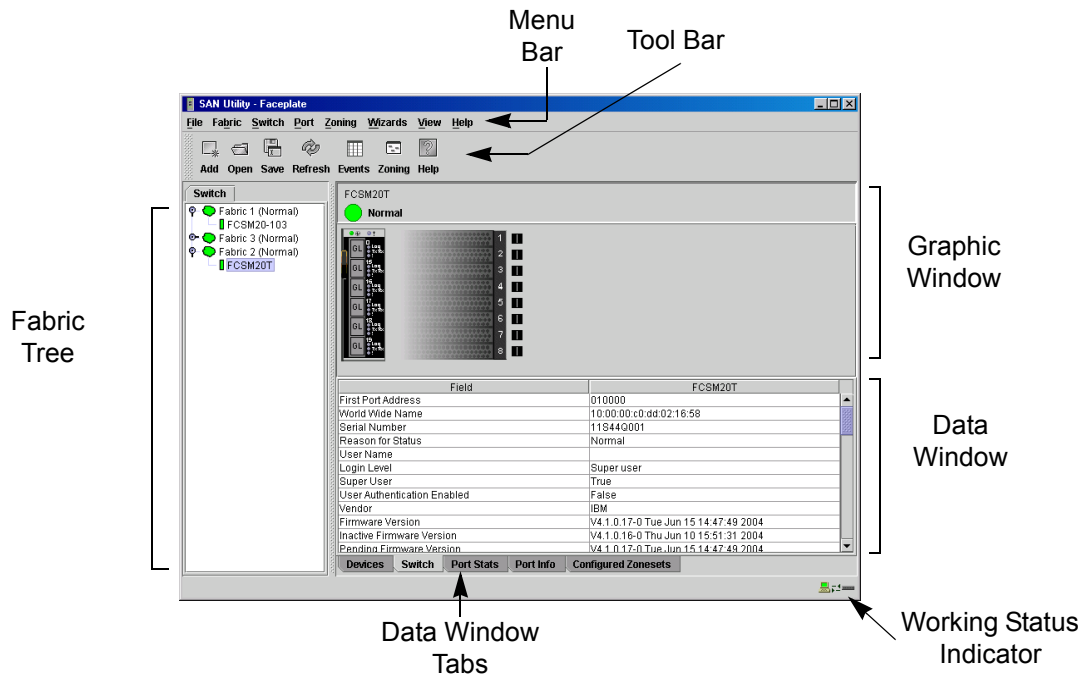


Figure 3-3. BladeCenter T Faceplate Window

3.3.1

Menu Bars

The menus and the options offered in them vary depending on the display. For example, the Port menu and many of the Switch menu selections are available only in the Faceplate window.

3.3.1.1

Topology Window Menu

The menu options available in the Topology window are shown in [Figure 3-4](#).

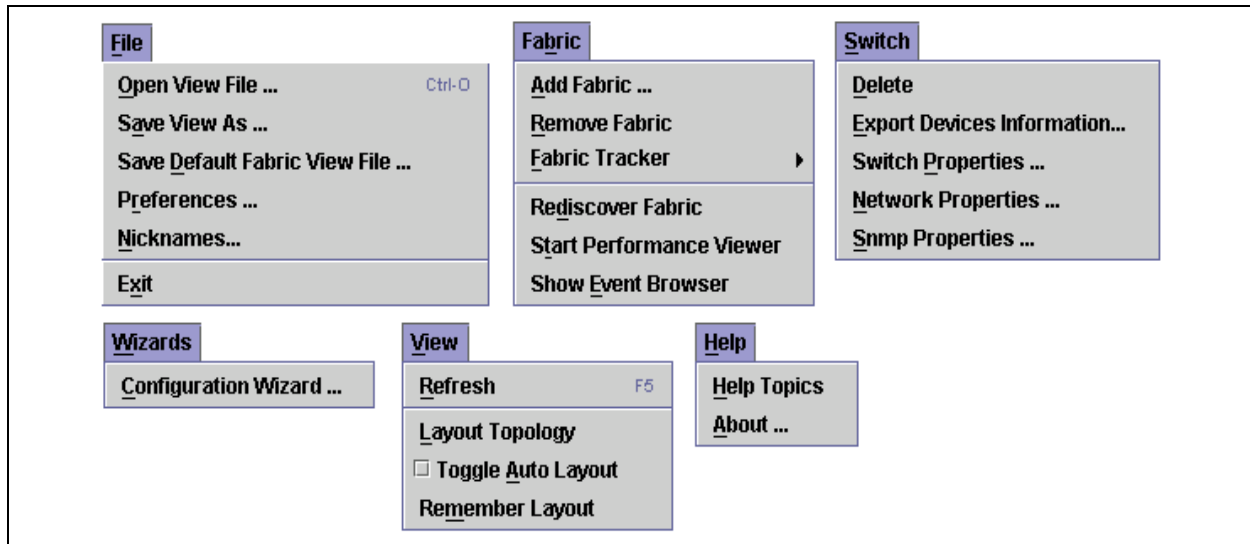


Figure 3-4. Topology Window Menu

3.3.1.2

Faceplate Window Menu

The menu options available in the Faceplate window are shown in [Figure 3-5](#).

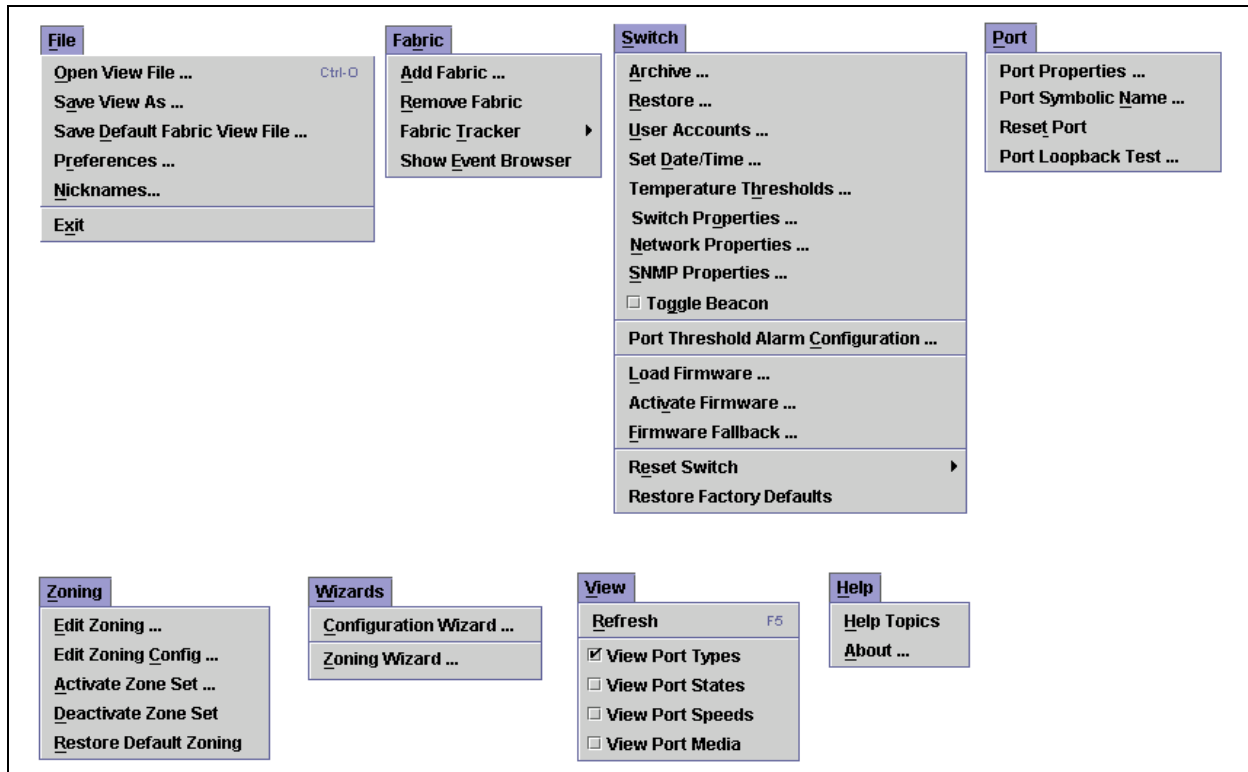


Figure 3-5. Faceplate Window Menu

The keyboard shortcut keys vary by display type: Topology window and Faceplate window. In addition to the menu bar, both the topology and Faceplate windows have context sensitive menus that pop up when you right-click in the graphic window. Refer to ["Opening the Faceplate Popup Menu"](#) on page 3-17 for more information about these popup menus.

3.3.1.3

Topology Window Shortcut Keys

The shortcut keys for the Topology window are shown in [Table 3-2](#). The shortcut key combinations are not case-sensitive.

Table 3-2. Topology Window Menu Shortcut Keys

Shortcut	Selection	Shortcut	Selection
Ctrl+O Alt+F, O	File>Open View File	Alt+S, D	Switch>Delete
Alt+F, A	File>Save View As	Alt+S, E	Switch>Export Devices Information
Alt+F, D	File>Save Default Fabric View File	Alt+S, P	Switch>Switch Properties (active only when one switch is selected)
Alt+F, R	File>Preferences	Alt+S, N	Switch>Network Properties (active only when one switch is selected)
Alt+F, N	File>Nicknames	Alt+S, S	Switch>SNMP Properties (active only when one switch is selected)
Alt+F, X	File>Exit	Alt+W, C	Wizards> Configuration Wizard
Alt+B, A	Fabric>Add Fabric	Alt+V, R F5	View>Refresh
Alt+B, R	Fabric>Remove Fabric	Alt+V, L	View>Layout Topology
Alt+B, F +S +A	Fabric>FabricTracker Save Snapshot Analyze Snapshot	Alt+V, A	View>Toggle Auto Layout
Alt+B, D	Fabric>Rediscover Fabric	Alt+V, M	View>Remember Layout
Alt+B, T	Fabric>Start Fabric View	Alt+H, H	Help>Help Topics
Alt+B, E	Fabric>Show Event Browser	Alt+H, A	Help>About

3.3.1.4

Faceplate Window Shortcut Keys

The shortcut keys for the Faceplate window are shown in [Table 3-3](#). The shortcut key combinations are not case-sensitive.

Table 3-3. Faceplate Window Shortcut Keys

Shortcut	Selection	Shortcut	Selection
Ctrl+O Alt+F, O	File>Open View File	Alt+S, V	Switch>Activate Firmware
Alt+F, A	File>Save View As	Alt+S, F	Switch>Firmware Fallback
Alt+F, D	File>Save Default Fabric View File	Alt+S, E +R +H +A	Switch>Reset Switch Reset Hot reset Hard Reset
Alt+F, R	File>Preferences	Alt+S, Y	Switch>Restore Factory Defaults
Alt+F, N	File>Nicknames	Alt+P, 2	Port>Port Properties
Alt+F, X	File>Exit	Alt+P, N	Port>Port Symbolic Name
Alt+B, A	Fabric>Add Fabric	Alt+P, T	Port>Reset Port
Alt+B, R	Fabric>Remove Fabric	Alt+P, L	Port>Port Loopback Test
Alt+B, F +S +A	Fabric>FabricTracker Save Snapshot Analyze Snapshot	Alt+Z, E	Zoning>Edit Zoning
Alt+B, E	Fabric>Show Event Browser	Alt+Z, C	Zoning>Edit Zoning Config
Alt+S, A	Switch>Archive	Alt+Z, A	Zoning>Activate Zone Set
Alt+S, R	Switch>Restore	Alt+Z, D	Zoning>Deactivate Zone Set
Alt+S, U	Switch>User Accounts	Alt+Z, R	Zoning>Restore Default Zoning
Alt+S, D	Switch>Set Date/Time	Alt+W, C	Wizards> Configuration Wizard
Alt+S, H	Switch>Temperature Thresholds	Alt+V, R F5	View>Refresh
Alt+S, P	Switch>Switch Properties	Alt+V, T	View>View Port Types
Alt+S, N	Switch>Network Properties	Alt+V, S	View>View Port States
Alt+S, S	Switch>SNMP Properties	Alt+V, E	View>View Port Speeds
Alt+S, G	Switch>Toggle Beacon	Alt+V, M	View>View Port Media








Table 3-3. Faceplate Window Shortcut Keys (Continued)

Shortcut	Selection	Shortcut	Selection
Alt+S, C	Switch>Port Threshold Alarm Configuration	Alt+H, H	Help>Help Topics
Alt+S, L	Switch>Load Firmware	Alt+H, A	Help>About

3.3.2 Tool Bar

The tool bar consists of a row of graphical buttons that you can use to access SAN Utility functions as shown in [Table 3-4](#). The tool bar buttons are an alternative method to using the menu bar. The tool bar can be relocated in the display by clicking and dragging the handle at the left edge of the tool bar.

Table 3-4. Tool Bar Buttons

Toolbar Button	Toolbar Button Name	Description
 Add	Add Fabric	Adds a new fabric to the fabric view.
 Open	Open View File	Opens an existing fabric view file.
 Save	Save View As	Saves the current fabric view to a file.
 Refresh	Refresh	Updates the topology or Faceplate window with current information.
 Events	Event Browser	Opens the events browser.
 Zoning	Edit Zoning	Opens the Edit Zoning window (available only in Faceplate window).
 Help	Help Topics	Opens the online help file.

3.3.3 Fabric Tree

The fabric tree lists the managed fabrics and their switches as shown in [Figure 3-6](#). The window width can be adjusted by clicking and dragging the moveable window border. An entry handle located to the left of an entry in the tree indicates that the entry can be expanded or collapsed. Click this handle or double-click the entry to expand or collapse a fabric tree entry. A fabric entry expands to show its member switches.

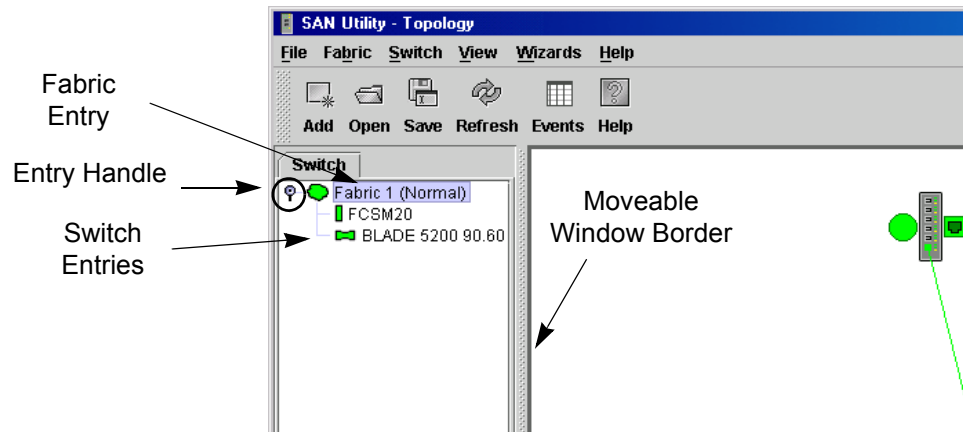


Figure 3-6. Fabric Tree

Each 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, non-operational state (if switch is offline), or a switch with user authentication enabled when the fabric management switch has user authentication disabled.
- A blue icon indicates that a switch is unknown, unreachable, or unmanageable.

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

The fabric tree provides access to the topology and Faceplate windows for any fabric or switch.

- To open the Topology window from the fabric tree, click a fabric entry.
- To open the Faceplate window from the fabric tree, click a switch entry.

3.3.4

Graphic Window

The graphic window, as shown in [Figure 3-1](#), presents graphic information about fabrics and switches such as the fabric topology and the switch faceplate. The window height can be adjusted by clicking and dragging the window border that it shares with the data window. This only works when displaying a fabric.

3.3.5

Data Window and Tabs

The data window presents a table of data and statistics associated with the selected tab. Use the scroll bar to browse through the data. The window length can be adjusted by clicking and dragging the border that it shares with the graphic window.

Adjust the column width by moving the pointer over the column heading border shared by two columns until a right/left arrow graphic is displayed. Click and drag the arrow to the desired width.

The data window tabs present options for the type of information to display in the data window. These options vary depending on the display.

3.3.6

Working Status Indicator

The working status indicator, located in the lower right corner of the SAN Utility window, shows when the management workstation is exchanging information with the fabric. As conditions change, the fabric forwards this information to the management workstation where it is reflected in the various displays.

3.3.7 Using the Topology Window

The Topology window shown in [Figure 3-7](#) receives information from the selected fabric and displays its topology. Switches and interswitch links (ISLs) appear in the graphic window and use color to indicate status. Consider the following Topology window features:

- [Fibre Channel Switch Module and Link Status](#)
- [Working with Switch Modules and Links](#)

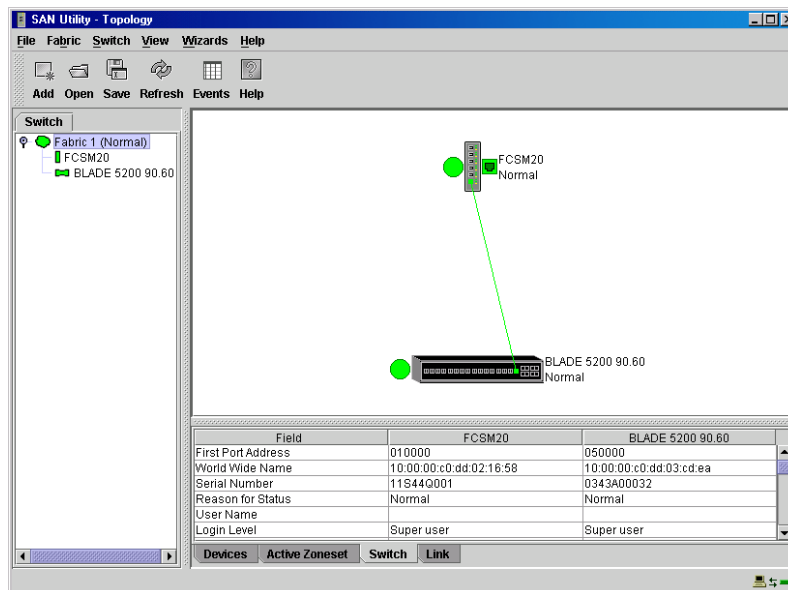


Figure 3-7. Topology Window

3.3.7.1

Fibre Channel Switch Module and Link Status

Fibre Channel Switch Module icon shape and color provide information about the Fibre Channel Switch Module and its operational state. Lines represent links between switches. Refer to ["Fabric Status" on page 3-29](#) for more information about Topology window icons.

Table 3-5. Fibre Channel Switch Module and Link Status Indicators

Switch Module Icon Color	Status
Green	Normal Fibre Channel Switch module operation
Amber	Operational with errors
Red	Inoperable or Fibre Channel Switch module failure
Blue	Unknown, unreachable, or unmanageable Fibre Channel device

3.3.7.2

Working with Switch Modules and Links

Switch modules and link icons are selectable and moveable, and serve as access points for other displays and menus. You select switch modules and links to display information, modify their configuration, or delete them from the display. The context-sensitive pop-up menus are accessible through the switch module and link icons.

Click a switch module or link in the graphic window to display its status in the data window. To select multiple switch modules or links, hold down the Ctrl key while selecting. When no switch modules or links are selected, information about all switch modules is displayed. To deselect a switch module or link that is currently selected, click the switch or link.

Different switch module icons will be displayed depending on the different switch vendor products present in the attached fabric. See [Table 3-6](#) for a list of switch module icons and vendors.

3.3.7.2.1

Arranging Switch Modules in the Window

You can use the following two methods to arrange individual switch module icons:

- To move an individual switch icon, click and drag the icon to another location in the graphic window. Links stretch or contract to remain connected.
- To arrange all switch icons in the Topology window automatically, open the View menu and select **Layout Topology**.

The **Toggle Auto Layout** check box in the View menu is selected by default so that SAN Utility can arrange the icons when you select **Layout Topology**.

You can save a custom arrangement, or layout, and restore that layout during a SAN Utility session. Begin by arranging the icons, then open the View menu and select **Remember Layout**. To restore the saved layout, open the View menu, uncheck the **Toggle Auto Layout** box, and select **Layout Topology**.

3.3.7.2.2

Selecting Switch Modules and Links

Selected switch module icons are highlighted in violet. Selected ISLs are displayed as a heavier line. You can select switch modules and links in the following ways:

- To select a switch module or a link, click the icon or link.
- To select multiple switch modules or links, hold down the Control key and select.
- To select all switch modules or links, right-click anywhere in the graphic window background. Select **All Switches** or **Select All Links** from the popup menu.

To cancel a selection, press and hold the Control key, and select the item again. To cancel all selections, click in the graphic window background.

3.3.7.2.3

Topology Data Window Tabs

The Topology window provides the following data windows corresponding to the data window tabs:

- **Devices** – displays information about devices (hosts and storage targets) connected to the switch. Refer to ["Devices Data Window" on page 3-68](#) for more information.
- **Active Zoneset** – displays the active zone set for the fabric including zones and their member ports. Refer to ["Active Zone Set Data Window" on page 3-36](#) for more information about this data window. Refer to ["Zoning a Fabric" on page 3-40](#) for information about zone sets and zones.
- **Switch** – displays current network and switch configuration data for the selected switches. Refer to ["Switch Data Window" on page 3-68](#) for more information.
- **Link** – displays information about the interswitch links. Refer to ["Link Data Window" on page 3-71](#) to for more information.

3.3.8

Using the Faceplate Window

The Faceplate window shows the front of a single switch module and its ports. You can open the Faceplate window and pop-up menus when you are in the Topology window by performing the following tasks:

- To open the Faceplate window when viewing the Topology window, click a switch module entry or icon in the fabric tree, or double-click the switch module graphic.
- To open the fabric pop-up menu when viewing the Topology window, right-click the graphic window background. The fabric pop-up menu displays selections to refresh the fabric, select all switch modules, select all links, or layout topology.
- To open the switch module pop-up menu when viewing the Topology window, right-click the switch module icon in the graphic window. The switch pop-up menu displays selections to refresh the switch, delete the switch from the display, open the Switch Properties window, open the Network Properties window, or open the SNMP Properties window.
- To open the link pop-up menu, right-click the link. The Link pop-up menu displays a selection to delete the link from the display.
- To open a Faceplate window pop-up menu, right-click the faceplate graphic in the Graphic window. The faceplate pop-up menu displays selections to refresh the switch module, select all ports, manage switch, port, network, and SNMP properties, and run the port loopback tests.

The Faceplate window shown in [Figure 3-8](#) displays the switch name and operational state, and port status. Consider the following functional elements of the Faceplate window:

- [Port Views and Status](#)
- [Working with Ports](#)
- [Faceplate Data Window Tabs](#)

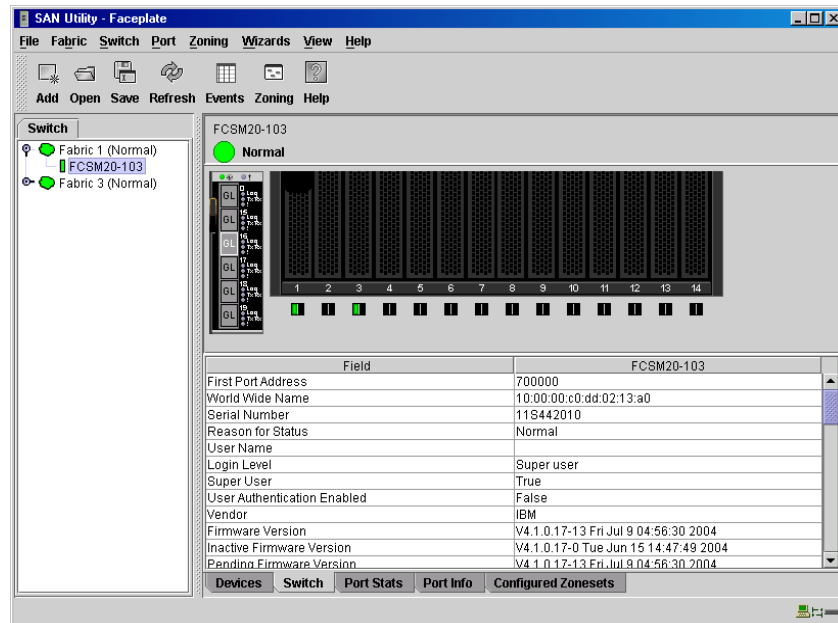


Figure 3-8. Faceplate Window

3.3.8.1 Port Views and Status

Port color and text provides information about the port and its operational state. Green indicates active; gray indicates inactive. The Faceplate window displays the following views of port status corresponding to the View menu options in the Faceplate window.

- Port type
- Port state
- Port speed
- Port media

Context-sensitive popup menus are displayed when you right-click the faceplate image or a port icon in the Faceplate window. Refer to ["Monitoring Port Status"](#) on [page 3-94](#) for more information about these displays.

3.3.8.2

Working with 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. You cannot use SAN Utility to select internal bays and external ports at the same time. Context-sensitive popup menus and properties windows are accessible through the Faceplate window and port icons.

3.3.8.2.1

Selecting Ports

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

- To select one port, click the port in the Faceplate window.
- To select a range of either internal or external consecutive ports, select a port and then press and hold the shift key and select another port. The application selects both end ports and all ports in between in port number.
- To select several nonconsecutive ports, hold the Control key while selecting ports.
- To select all ports, right-click on the faceplate image. Select **All Ports** from the popup menu.

To cancel a selection, press and hold the Control key and select it again.

3.3.8.2.2

Opening the Faceplate Popup Menu

You can manage the switch module and its ports using the following methods:

- To open the pop-up menu, right-click anywhere in the graphic window. If no ports are selected, port specific tasks are unavailable in the menu. If no ports are selected, the port-related tasks will be unavailable in the menu.
- To select a port and open the Port pop-up menu, right-click a port.
- To select more than one port, hold down the Control key and click the ports; or hold the Shift key and click two ports to select a range. To open the Port pop-up menu, right-click one of the selected ports.

3.3.8.3

Faceplate Data Window Tabs

The Faceplate Data window contains six tabs at the bottom of the display. When you click a tab, the following information is displayed:

- Devices – Click the **Devices** tab to display information about devices (hosts and storage targets) connected to the switch.
- Switch – Click the **Switch** tab to display current switch module configuration data.

- Port statistics – Click the **Port Stats** tab to display performance data for the selected ports.
- Port information – Click the **Port Info** tab to display the port detail information for the selected ports.
- Configured zone sets – Click the **Configured Zonesets** to display all zone sets, zones, and zone membership in the zoning database.

3.4

Configuring the SAN Utility Environment

You can configure your SAN Utility environment through the use of fabric view files and SAN Utility preferences.

3.4.1

Working with Fabric View Files

A fabric view file is one or more fabrics that you save to a file that you can retrieve with each SAN Utility session. In addition to the SAN Utility default fabric view file, you can save and open your own fabric view files. A fabric view file can have an encryption key that functions like a password to make your fabrics secure on the workstation.

3.4.1.1

Saving a Fabric View File

To save a set of fabrics to a file, do the following:

1. Open the File menu and select **Save View As** to open the Save View window.
2. Enter a name for the fabric view file or click the **Browse** button to select an existing file. Files are saved in the working directory.
3. Enter a password. When you attempt to open this fabric view file, you will be prompted for this password. If you leave the File Password field blank, no password will be required when attempting to open this fabric view file.
4. Click the **OK** button to save the view.

3.4.1.2

Opening a Fabric View File

To open a fabric view file, do the following:

1. Open the File menu and select **Open View File** to open the Open View window.
2. Enter a name for the fabric view file or click the **Browse** button to select an existing file.
3. If the fabric view file was saved with a password, enter the password and click the **OK** button.
4. Click the **OK** button to open the view.

3.4.1.3

Changing the Encryption Key for the Default Fabric View File

To change the encryption key for the SAN Utility default fabric view file, do the following:

1. Open the File menu and select **Save Default Fabric View File** to open the Save Default Fabric View File window. Enter an encryption key in the Default Fabric File Encryption Key field.
2. Re-enter the same encryption key in the Re-enter Encryption Key to Confirm field.
3. Click the **OK** button to save the current set of fabrics to the default fabric view file in the working directory.

3.4.2

Setting SAN Utility Preferences

Using the preferences settings, you can:

- Change the location of the working directory in which to save files.
- Change the location of the browser used to view the online help.
- Choose the fabric discovery interval. The fabric discovery interval is how often the SAN Utility application receives information from the fabric. Choose 30 (default), 45, or 60 seconds. The smaller the interval, the more often the application talks to the switch and thus the greater impact to performance.
- Enable (default) or disable the fabric view file auto save and load feature. This preference prompts you save the fabric view file upon exiting a SAN Utility session and prompts you to load a fabric view file upon opening a SAN Utility session.
- Enable (default) or disable the use of the Initial Start window at the beginning of a SAN Utility session.
- Enable (default) or disable the Event Browser. Refer to ["Displaying the Event Browser" on page 3-31](#). If the Event Browser is enabled using the Preferences window as shown in [Figure 3-9](#), the next time SAN Utility is started, all events will be displayed. If the Event Browser is disabled when SAN Utility 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 window. 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 window by opening the View menu and selecting a different port view option. Refer to the corresponding subsection for more information:
 - ["Displaying Port Types" on page 3-95](#)
 - ["Displaying Port Operational States" on page 3-96](#)
 - ["Displaying Port Speeds" on page 3-96](#)
 - ["Displaying Transceiver Media Status" on page 3-97](#)

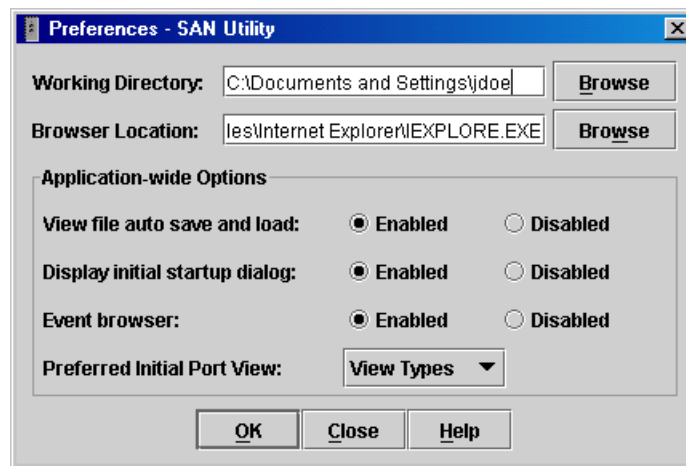


Figure 3-9. Preferences Window – SAN Utility

To set preferences for your SAN Utility sessions, do the following:

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

3.5

Managing Fabrics

This section describes the following tasks that manage fabrics:

- [Securing a Fabric](#)
- [Tracking Fabric Version Information](#)
- [Managing the Fabric Database](#)
- [Displaying Fabric Information](#)
- [Working with Device Information and Nicknames](#)
- [Zoning a Fabric](#)

3.5.1

Securing a Fabric

The components of Fibre Channel fabric security are:

- [User Account Security](#)
- [Fabric Services](#)

3.5.1.1

User Account Security

Access to a switch module and permission to configure a switch is managed through user accounts created by a fabric administrator. A user account consists of an account name, a password, an authority level, and an expiration date. The authority level determines whether an account can merely monitor the switch module and fabric activity (User authority), or change switch module configurations (Administrative authority). See ["Managing User Accounts" on page 3-61](#) for information about administrating user accounts. User authentication determines the enforcement of user accounts on a switch module. A fabric administrator can enable or disable user authentication on a switch module using the Set Setup System command.

If user authentication is disabled (default), you can use SAN Utility to log in to a switch module without an account name and password. The Login name and Password fields in the Add a Fabric window are ignored, and you are granted Admin authority. If user authentication is enabled, you must enter an account name and password to log in to a switch module and add the fabric to the workspace. Having successfully added a fabric, you can perform only those tasks in SAN Utility that are granted by the authority level for that account. All switch modules in a fabric must use the same user authentication value. See ["Set Setup Command" on page 2-52](#) for information about the System keyword and the UserAuthentication parameter.

- Note:** The fibre channel switch module supports a combined maximum of 19 logins or sessions reserved as follows:
- 4 logins or sessions for internal applications such as management server and SNMP
 - 9 high priority Telnet sessions
 - 6 logins or sessions for SAN Utility in-band and out-of-band logins, Application Programming Interface (API) in-band and out-of-band logins, and Telnet logins.

When you add a fabric and the UserAuthentication parameter is disabled, SAN Utility ignores the user account and password entries and logs you in using the default user account (USERID). The Admin account possesses Admin authority which grants full access to all tasks of the SAN Utility menu system. If the UserAuthentication parameter is enabled, you must enter a user account and password. The switch module validates your user account and SAN Utility 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 module using SAN Utility or CLI, and an administrator changes user access rights, passwords, or UserAuthentication security settings, existing logins will not be affected by the new settings. Login access and privileges are only checked for a new login request.

3.5.1.2

Fabric Services

Fabric services security includes SNMP and In-band management. Simple Network Management Protocol (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 SNMP Properties window. 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. Refer to ["Switch Module Monitoring Using SNMP" on page 4-5](#) for more information. SNMP is enabled by default.

In-band management is the ability to manage switch modules across interswitch links using SAN Utility, SNMP, management server, or the application programming interface. The switch module comes from the factory with in-band management enabled. If you disable in-band management on a particular switch module, you can no longer communicate with that switch module by means other than a direct Ethernet or serial connection. Refer to ["In-band Management" on page 3-82](#) for more information.

3.5.2

Tracking Fabric Version Information

The Fabric Tracker feature enables you to generate a snapshot or baseline of current system version information, which can be viewed, analyzed and compared to other snapshot files, and exported to a file. Information includes date and time, SAN Utility version, switch module firmware version, device hardware, device drivers, and device firmware version. The Snapshot Analyzer enables you to:

- Compare two snapshots
- Detect mismatches of firmware and driver versions
- Detect devices that have been moved, added to or removed from the fabric.

3.5.2.1

Saving a Version Snapshot

To save the current snapshot to an XML file, open the Fabric menu, select **Fabric Tracker**, and select **Save Snapshot**. To view and analyze system version information, open the Fabric menu, select **Fabric Tracker**, and select **Analyze Snapshots**. The Fabric Version Snapshot Analysis window, shown in [Figure 3-10](#), opens with the Summary, Differences and Reports tab pages. Click the **Browse** buttons to open and view the snapshot files in the corresponding tab pages. Click the **Close** button to exit the Fabric Version Snapshot Analysis window. The color key below the scrollable area defines the meanings of the colors used. The Summary tab page shows a brief description of the changes that have occurred between the older snapshot and the newer one. Use the Summary tab page quickly view what has changed.

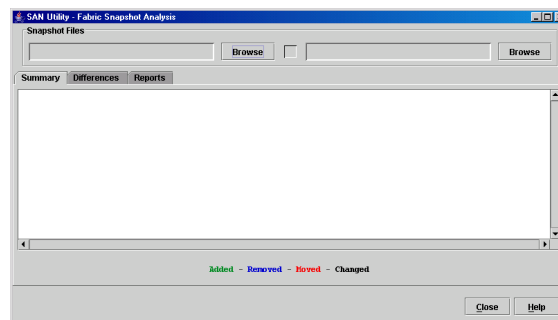


Figure 3-10. Fabric Version Snapshot Analysis Window

3.5.2.2

Viewing and Comparing Version Snapshots

The Differences tab page shows a side-by-side comparison of two snapshots. The timestamp of each snapshot is displayed above the scroll area showing that snapshot. The background color of the older snapshot is darker than the background of the newer snapshot. The arrow icon between the snapshot selectors always points from the older snapshot to the newer one. If the two snapshots have the same timestamp, the arrow will not be displayed. The scroll bars are synchronized to view the same portion of each snapshot file simultaneously. Click and drag the separator bar between the two panes to resize each pane. At the top of the separator bar between the two panes, click the left/right arrows to close the corresponding pane. The left/right arrows move to one side.

3.5.2.3

Exporting Version Snapshots to a File

The Reports tab page enables you to select one of several reports to save to a text file. There are two types of reports. The Summary report type shows the same format displayed on the Summary tab page without the color highlighting. The Detail report type shows a detailed breakdown of the differences. Use the **Export** button to save the selected report to a text file.

3.5.3

Managing the Fabric Database

A fabric database contains the set of fabrics that you have added during a SAN Utility session. If you do not open an existing fabric or fabric view file, a Topology window opens with an empty fabric database. This section describes the following fabric database management tasks:

- [Adding a Fabric](#)
- [Removing a Fabric](#)
- [Rediscovering a Fabric](#)
- [Adding a New Switch Module to a Fabric](#)
- [Replacing a Failed Switch Module in a Fabric](#)
- [Deleting Switches and Links from the Topology Window](#)

3.5.3.1

Adding a Fabric

To add a fabric to the database, do the following:

1. Open the Fabric menu and select **Add Fabric** to open the Add a New Fabric window as shown in [Figure 3-11](#).

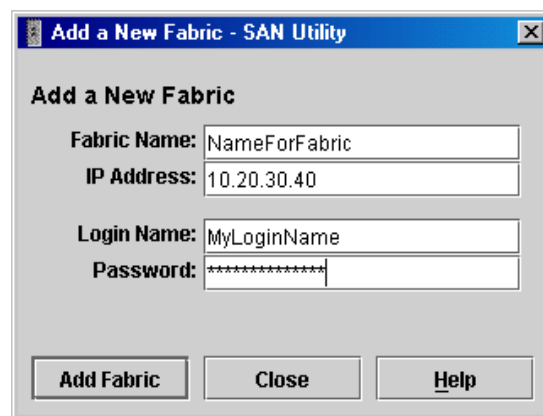


Figure 3-11. Add a New Fabric Window

2. In the Fabric Name field, type a fabric name.
3. In the IP Address field, type the IP address of the switch module through which to manage the fabric.

4. In the Login Name field, type the initial default account name, `USERID`. In the Password field, type the initial default password, `PASSWORD` (the sixth character is a zero, not the letter O). The account name and password are case sensitive.

Note: The password is for the fibre channel switch module and is stored in the fibre channel switch module firmware. You are not required to type an account name or password if user authentication is disabled. See ["Securing a Fabric" on page 3-21](#). See ["Set Setup Command" on page 2-52](#) for information about setting user authentication.

5. Click the **Add Fabric** button.

3.5.3.2

Removing a Fabric

To delete a fabric file from the database, do the following:

1. Select a fabric in the fabric tree.
2. Open the Fabric menu and select **Remove Fabric**.

3.5.3.3

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 module information. To rediscover a fabric, open the Fabric menu, and select **Rediscover Fabric**. The rediscover function is more comprehensive than the refresh function.

3.5.3.4

Adding a New Switch Module to a Fabric

After you install a fibre channel switch module into your server unit, the switch module uses the default fabric configuration settings. The default fabric configuration settings are as follows:

- Fabric zoning is sent to the fibre channel switch module from the fabric.
- All external ports (0, 15, 16, 17, 18, 19) are GL_Ports; all internal ports (1 through 14) are F_Ports.
- The default IP addresses are:
For I/O-module bay 3:
192.168.70.129
For I/O-module bay 4:
192.168.70.130

Complete the following steps to add a new fibre channel switch module to a fabric and not make changes to the default fabric configuration settings:

1. Use the Management module to restore factory defaults. In the Faceplate window, open the Switch menu and select **Restore Factory Defaults**.
2. If you want to manage the switch module through the Ethernet port, you must first configure the IP address using the Network Properties window.
3. Configure any special switch module settings.

Note: To prevent communication with other switch modules in the fabric until the new fibre channel switch module is configured, in the Zoning Config window, click **None** in the Default Visibility field. For more information, see ["Configuring the Zoning Database" on page 3-48](#).

4. Plug in the interswitch links (ISL), but do not connect the devices.
5. In the Port Properties window, configure the port types for the new switch module (GL_Port, Donor).
6. Connect the Fibre Channel devices to the Fibre Channel switch module.
7. Make any necessary zoning changes using the Edit Zoning window. To open the Edit Zoning window, open the Zoning menu, and select **Edit Zoning**. If you changed the Default Visibility setting in the Zoning Config window from All to None, change that setting back to All. To open the Zoning Config window, open the Zoning menu, and select **Edit Zoning Config**.

3.5.3.5

Replacing a Failed Switch Module in a Fabric

Use the following procedure to replace a failed switch module for which an archive is available.

1. Remove the failed fibre channel switch module. For more information, see the *QLogic 6-Port Enterprise Fibre Channel Switch Module for IBM Eserver BladeCenter Installation Guide*.
2. Install the new replacement fibre channel switch module. For more information, see the *QLogic 6-Port Enterprise Fibre Channel Switch Module for IBM Eserver BladeCenter Installation Guide*.
3. Log in to the fabric through the replacement fibre channel switch module. In the Topology window, select the replacement fibre channel switch module from the fabric tree.
4. Open the Switch menu and select **Restore**. The Restore Switch window opens.
5. In the Restore Switch window, type a name or select the archived fibre channel switch module configuration file to copy to the switch module. For more information, see "[Archiving a Switch Module Configuration](#)" on [page 3-86](#).
6. Click **OK** to write the configuration file to the Fibre Channel switch module.

3.5.3.6

Deleting Switches and Links from the Topology Window

The SAN Utility application does not automatically delete switch modules or links that have failed or have been physically removed from the fabric Fibre Channel network. In this case, you can delete switch modules and links to bring the display up to date. If you delete a switch module or a link that is still active, the SAN Utility application will restore it automatically. You can also refresh the display.

To delete a switch module from the Topology window, do the following:

1. Select one or more switches in the Topology window.
2. Open the Switch menu and select **Delete**.

To delete a link, do the following:

1. Select one or more links in the Topology window.
2. Open the Switch menu and select **Delete**.

3.5.4

Displaying Fabric Information

The Topology window is your primary tool for monitoring a fabric. The graphic window of the Topology window provides status information for switch modules, interswitch links, and the Ethernet connection to the network management workstation.

The data window tabs show device, switch, and active zone set information. The **Active Zoneset** tab shows the zone definitions for the active zone set. Refer to ["Devices Data Window" on page 3-35](#) and ["Switch Data Window" on page 3-68](#) for information about the Devices and Switch data windows.

3.5.4.1

Fabric Status

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

- In the Topology window, click the **Refresh** button.
- Open the View menu and select **Refresh**.
- Press the F5 key.
- Right-click anywhere in the background of the Topology window and select **Refresh Fabric** from the popup menu.

The Topology window displays switch module and status icons to provide status information about switch module, interswitch links, and the Ethernet connection. The switch module status icons, displayed on the left side of a switch, vary in shape and color. Each switch module that is managed by an Ethernet Internet Protocol (IP) has a colored Ethernet icon displayed on the right side of the switch module. A green Ethernet icon indicates normal operation, amber indicates a condition that may require attention to maintain maximum performance, and red indicates a potential failure. [Table 3-6](#) shows the different switch icons and their meanings.

Note: Different switch module icons are displayed depending on the different switch vendor products presented in the attached fabric. For a list of switch module icons and vendors, see [Table 3-6](#). Switches that are not manageable through SAN Utility are displayed as third-party unmanageable switch icons.

Table 3-6. Topology Window Switch and Status Icons















Switch Icon	Description
	QLogic 6-Port Enterprise Fibre Channel Switch Module for a BladeCenter unit
	QLogic 6-Port Enterprise Fibre Channel Switch Module for a BladeCenter T unit
	QLogic 2-Port Fibre Channel Switch Module
	SANbox®2-8c Fibre Channel switch
	SANbox2-16 Fibre Channel switch
	SANbox 5200 Fibre Channel switch
	Switch is not manageable with this version of SAN Utility. Use the management application that was shipped with this switch.
	Switch communication normal (green)

Table 3-6. Topology Window Switch and Status Icons (Continued)

Switch Icon	Description
	Switch operational with errors (amber)
	Switch status critical–potential failure (red)
	Switch communication status unknown, unreachable, or unmanageable (blue)
	Fabric management switch Ethernet connection normal (green)
	Fabric management switch Ethernet connection warning (amber)
	Fabric management switch Ethernet connection critical (red)

3.5.4.2

Displaying the Event Browser

The Event Browser displays a list of recorded events and alarms generated by the switches in the fabric and the SAN Utility application. Events that are generated by the SAN Utility application and are not saved on the switch, but can be saved to a file during the SAN Utility session. An alarm is also an event, but is generated by the switch, stored on the switch, and will be retrieved when restarting the SAN Utility application.

Entries in the Event Browser shown in [Figure 3-12](#), are formatted by severity, time stamp, source, type, and description. The maximum number of entries allowed is 1500. Once the maximum is reached, the event list wraps and the oldest events are discarded and replaced with the new events. Alarm entries have a switch time stamp, while event entries 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 SAN Utility is running. If the Event Browser is enabled using the Preferences window, the next time SAN Utility is started all events from the switch module alarm log will be displayed. If the Event Browser is disabled when SAN Utility is started and later enabled, only those events from the time the Event Browser was enabled and forward will be displayed.

To display the Event Browser, open the Fabric menu and select **Show Event Browser**, or click the **Events** button on the tool bar. If the **Show Event Browser** selection or the **Events** button is grayed-out, you must first enable the **Events Browser** preference. Refer to ["Setting SAN Utility Preferences"](#) on page 3-19.

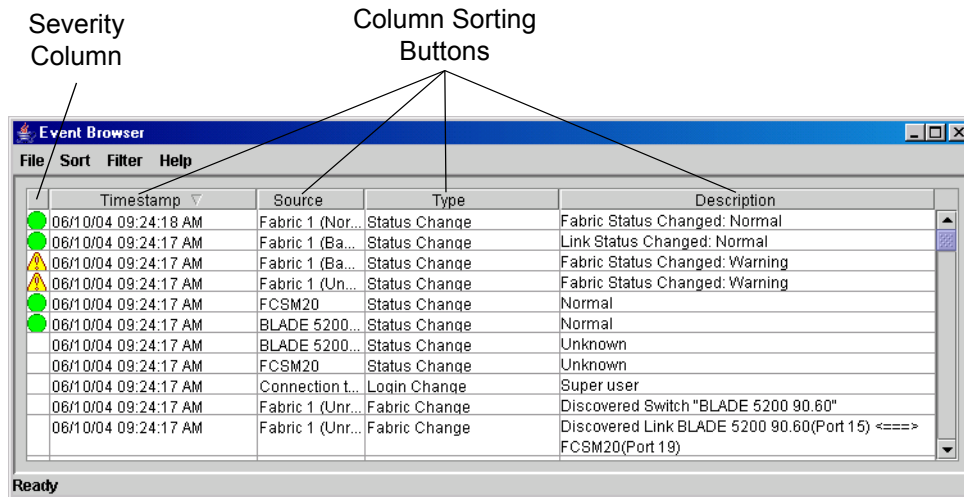


Figure 3-12. Events Browser

Severity is indicated in the severity column using icons as described in [Table 3-7](#).

Table 3-7. Severity Levels





Severity Icon	Description
	Alarm – An alarm is an event generated by the switch that specifically requests attention.
	Critical event – An event generated by the SAN Utility application and indicates a potential failure.
	Warning event – An event generated by the SAN Utility application that indicates errors or other conditions that may require attention to maintain maximum performance.

Table 3-7. Severity Levels (Continued)

Severity Icon	Description
	Normal event – An event generated by the SAN Utility application that indicates a transition from a non-normal to normal operation.
No icon	Informative – An unclassified event generated by the SAN Utility application that provides supporting information.

- Note:**
- Events (Critical, Warning, Normal, and Informative) are generated by the application and are not saved on the switch module. They are permanently discarded when you close a SAN Utility session, but you can save these events to a file on the workstation before you close SAN Utility and read it later with a text editor or browser.
 - Alarms are generated by the switch module, stored on the switch module, and will be retrieved when the application is restarted. Some alarms are configurable. Refer to ["Configuring Port Threshold Alarms"](#) on page 3-73.

3.5.4.2.1

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 window shown in [Figure 3-13](#). The Event Browser displays those events that meet all of the criteria in the Filter Events window. 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** – Check one or more of the corresponding check boxes to display alarm events, critical events, warning events, normal events, or informative events.
- **Date/Time** – Check one or both of the From: and To: check boxes. 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 – Check one or more of the corresponding check boxes 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.

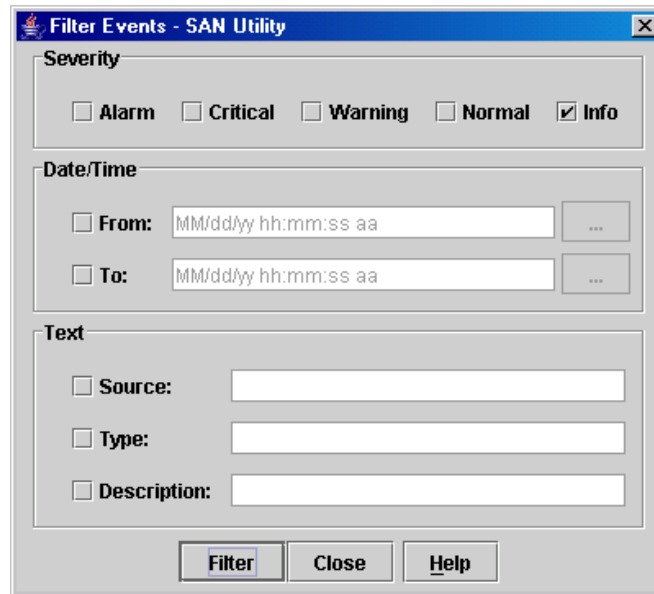


Figure 3-13. Filter Events Window

3.5.4.2.2

Sorting the Event Browser

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

3.5.4.2.3

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.

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

3.5.4.3

Devices Data Window

The Devices data window displays information about devices (hosts and storage targets) connected to the switch. Click the **Devices** tab below the data window to display device 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 or the Topology window. [Table 3-8](#) describes the entries in the Devices data window. Refer to ["Exporting Device Information to a File" on page 3-38](#) for exporting device information.

Table 3-8. 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 window. Refer to "Managing Device Port Nicknames" on page 3-38 for more information.
Details	Click the (i) to display additional detail about the device. Refer to "Displaying Detailed Device Information" on page 3-37 .
FC Address	Fibre Channel address
Switch	Switch module name
Port	Switch module port number
Target/Initiator	Device type: target or initiator
Vendor	Host Bus Adapter/Device Vendor
Host Name	Name of host
Active Zones	The active zone to which the device belongs
Row #	Number of port as displayed in the Faceplate window

3.5.4.4

Active Zone Set Data Window

The Active Zoneset data window 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 – you can confirm this by adding a fabric through another switch and comparing Active Zone Set displays.

To open the Active Zoneset data window, click the **Active Zoneset** tab below the data window in the Topology window. Refer to ["Configured Zonesets Data Window" on page 3-72](#) for information about the zone set definitions on a particular switch. Refer to ["Zoning a Fabric" on page 3-40](#) for more information about zone sets and zones.

The Active Zoneset data window, shown in [Figure 3-14](#), uses display conventions for expanding and contracting entries that are similar to the fabric tree. An entry handle located to the left of an entry in the tree indicates that the entry can be expanded. Click this handle or double-click the following entries:

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

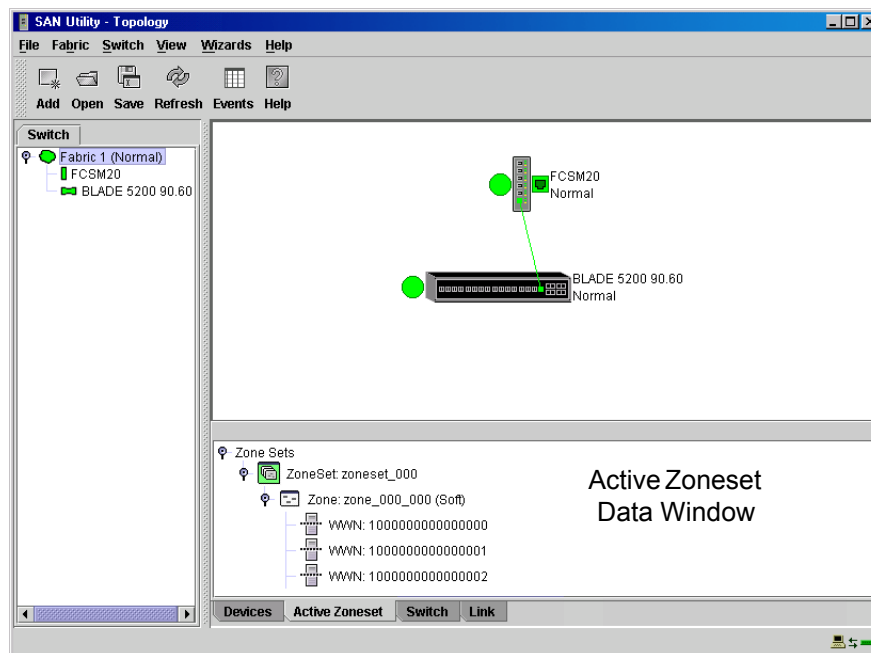


Figure 3-14. Active Zone Set Data Window

3.5.5

Working with Device Information and Nicknames

SAN Utility enables you to do the following tasks:

- [Displaying Detailed Device Information](#)
- [Exporting Device Information to a File](#)
- [Managing Device Port Nicknames](#)

3.5.5.1

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 3-15](#).

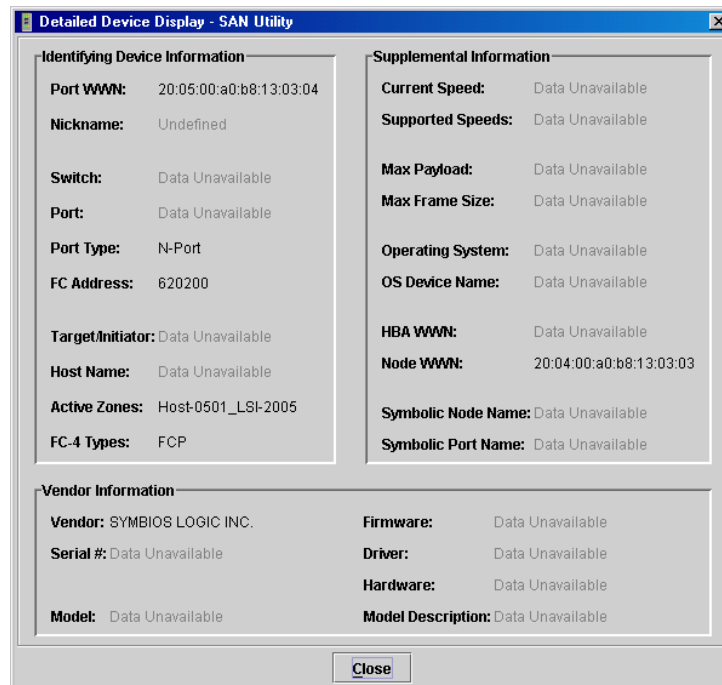


Figure 3-15. Detailed Devices Display Window

3.5.5.2

Exporting Device Information to a File

To save device information to a file, open the Topology window and do the following:

1. Select one or more switch modules. If no switch modules are selected, Devices information is gathered for all switch modules.
2. Open the Switch menu and select **Export Devices Information**.
3. In the Save window, enter a file name.
4. Click the **Save** button.

3.5.5.3

Managing Device Port Nicknames

You can assign a nickname to a device port World Wide Name. A nickname is a user-definable, meaningful name that can be used in place of the World Wide Name. Assigning a nickname makes it easier to recognize device ports when zoning your fabric or when viewing the Devices data window.

SAN Utility maintains nicknames in Nicknames.xml, which is found in your working directory. In addition to creating, editing, and deleting nicknames, you can also export the nicknames to a file, which can then be imported into the Nicknames.xml file on other workstations.

3.5.5.3.1

Creating a Nickname

To create a device port nickname, do the following:

1. Open the File menu and select **Nicknames** to open the Nicknames window.
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 [\$ _ - ^].
 - Click on a device in the table. Open the Edit menu and select **Create Nickname** to open the Add Nickname window. In the Add Nickname window, enter a nickname and WWN and click the **OK** button.
 - Double-click a cell in the **Nicknames** column, and enter a new nickname in the text field. Click the **Save** button to save the changes and exit the Nicknames window.

You can also create a nickname by double clicking a cell in the Nickname column of the Devices data window. Refer to ["Devices Data Window" on page 3-35](#).

3.5.5.3.2

Editing a Nickname

To edit a device port nickname, do the following:

1. Open the File menu and select **Nicknames** to open the Nicknames window.
2. Click on a device in the table. Open the Edit menu, and select **Edit Nickname**.
3. 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 [\$ _ - ^].
 - In the Edit Nickname window, enter a new nickname and click the **OK** button.
 - Double-click a cell in the **Nicknames** column, and edit an existing nickname in the text field. Click the **Save** button to save the changes and exit the Nicknames window.

You can also edit a nickname by double-clicking a cell in the Nickname column of the Devices data window. Refer to ["Devices Data Window" on page 3-35](#).

3.5.5.3.3

Deleting a Nickname

To delete a device port nickname, do the following:

1. Open the File menu and select **Nicknames** to open the Nicknames window.
2. Click a device in the table. Open the Edit menu and select **Delete Nickname**.

3.5.5.3.4

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, do the following:

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

3.5.5.3.5

Importing a Nicknames File

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

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

3.5.6

Zoning a Fabric

Fibre Channel fabrics use zoning to restrict or extend access to devices in the fabric. A zone is a named group of devices that can communicate with each other. You can use zoning to divide the ports and devices of the fabric into zones for more efficient and secure communication among functionally grouped nodes. You can set the Auto Save and Default Visibility zoning configuration parameters using SAN Utility or the Set Config Zoning command. See ["FC-SW-2 Auto Save" on page 3-48](#) for information about the Auto Save parameter, see ["Default Visibility" on page 3-49](#) for information about the Default Visibility parameter, and see ["Set Config Command" on page 2-35](#) for information about the Set Config Zoning command.

3.5.6.1

Zoning Concepts

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

- [Zones](#)
- [Aliases](#)
- [Zone Sets](#)
- [Zoning Database](#)

3.5.6.1.1

Zones

A zone is a named group of ports or devices that can communicate with each other. Devices within a zone can only communicate with other devices in the same zone. A device may participate in more than one zone.

Membership in a zone can be defined by 6-port Switch Module 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.
- FCID entries define zone membership by the Fibre Channel address of the attached device. With this membership method you can replace a device on the same port without having to edit the member entry as you would with a WWN member.
- Domain ID/Port number entries define zone membership by 6-port Switch Module 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.

Two types of zones are supported:

- Soft zone
- Hard zone - Access Control List (ACL)

3.5.6.1.1.1

Soft Zones

Soft zoning divides the fabric for purposes of controlling discovery. Devices within the same soft zone automatically discover and communicate freely with all other members of the same zone. The soft zone boundary is not secure; traffic across soft zones can occur if addressed correctly. Soft zones that include members from multiple switches need not include the ports of the interswitch links. Soft zone boundaries yield to ACL zone boundaries. Soft zones can overlap; that is, a device can participate in more than one soft zone. Zone membership can be defined by Fibre Channel address, domain ID and port number, World Wide Name, or a combination. Soft zoning supports all port types.

3.5.6.1.1.2

Access Control List Hard Zones

Access Control List (ACL) zoning divides the fabric for purposes of controlling discovery and inbound traffic. ACL zoning is a type of hard zoning that is hardware enforced. This type of zoning is useful for controlling access to certain devices without totally isolating them from the fabric. Devices can communicate with each other and transmit outside the ACL zone, but cannot receive inbound traffic from outside the zone. The ACL zone boundary is secure against inbound traffic. ACL zones can overlap; that is, a port can be a member of more than one ACL zone. ACL zones that include members from multiple switches need not include the ports of the interswitch links. ACL zone boundaries supersede soft zone boundaries. Membership can be defined only by domain ID and port number. ACL zoning supports all port types.

3.5.6.1.2

Aliases

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

3.5.6.1.3

Zone Sets

A zone set is a named group of zones. A zone can be a member of more than one zone set. All zones that are not members of a zone set belong to the orphan zone set. The orphan zone set is saved on the switch. Each switch in the fabric maintains its own zoning database containing one or more zone sets. This zoning database resides in non-volatile or permanent memory and is therefore retained after a reset. Refer to ["Configured Zonesets Data Window" on page 3-72](#) for information about displaying the zoning database.

To apply zoning to a fabric, choose a zone set and activate it. When you activate a zone set, the switch distributes that zone set and its zones, excluding aliases, to every switch in the fabric. This zone set is known as the active zone set. Refer to ["Active Zone Set Data Window" on page 3-36](#) for information about displaying the active zone set.

3.5.6.1.4

Zoning Database

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

There are two configuration parameters that affect the zoning database: FC-SW-2 Auto Save and Default Visibility. The Auto Save parameter determines whether changes to the active zone set that a switch module receives from another switch in the fabric will be saved to permanent memory on that switch. The Default Visibility parameter permits or prohibits communication among ports/devices when there is no active zone set. Refer to ["Configuring the Zoning Database" on page 3-48](#) for information about zoning configuration.

The zoning limits for a fabric are as follows:

- **MaxZoneSets is 256.** 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 1000.** 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.
- **MaxAliases is 2500.** The maximum number of aliases 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 and alias 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. Aliases are considered zone members since they can be added to a zone just like a normal zone member.
- **MaxZonesInZoneSets is 1000.** The maximum number of zone linkages to zonesets 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 zoneset this constitutes a linkage.
- **MaxMembersPerZone is 2000.** 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. Aliases are considered zone members when added to a zone.
- **MaxMembersPerAlias is 2000.** The maximum number of zone members that can be added to any alias on the switch. This will be enforced during the configuration of zoning and during a zoning database merge from the fabric.

3.5.6.2

Using the Zoning Wizard

The Zoning Wizard is a series of windows that leads you through the process of zoning a fabric. To open the Zoning Wizard, open the Wizards menu in the Faceplate window, and select **Zoning Wizard**.

The Zoning Wizard helps you with the two most typical reasons for zoning:

- Zoning Windows servers storage
- Assign storage to servers.

To solve these problems, there must be at least one target and at least one initiator in the name server. Windows servers do not share devices well, but sometimes they must share devices, such as a tape drive. The wizard helps you define which devices are sharable and which ones are not. Once a device is in a Windows group, it can no longer be in any other group.

3.5.6.3

Managing the Zoning Database

Managing the zoning database consists of the following:

- [Editing the Zoning Database](#)
- [Configuring the Zoning Database](#)
- [Saving the Zoning Database to a File](#)
- [Restoring the Zoning Database from a File](#)
- [Restoring the Default Zoning Database](#)
- [Deleting the Zoning Database](#)

3.5.6.3.1

Editing the Zoning Database

To edit the zoning database for a particular switch module, open the Zoning menu from the Faceplate window and select **Edit Zoning** to open the Edit Zoning window shown in [Figure 3-16](#). Changes can only be made to inactive zone sets, which are stored in flash (non-volatile) memory and retained after resetting a switch module.

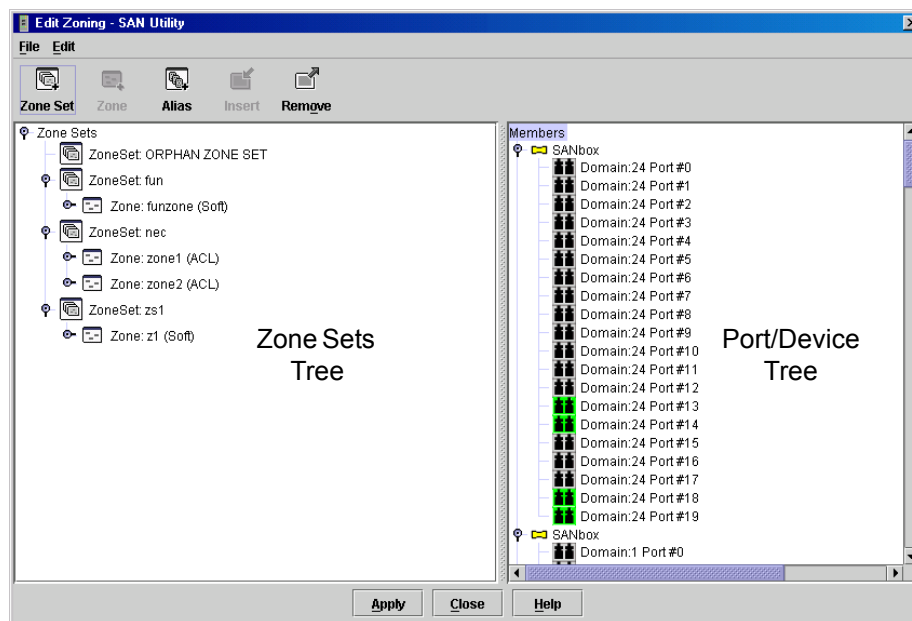


Figure 3-16. Edit Zoning Window

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

You can not edit an active zone set on a switch module. 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 module distributes that zone set to the temporary zoning database on every switch in the fabric. However, in addition to the merged active zone set, each switch maintains its own original zone set in its zoning database. Only one zone set can be active at one time.

Note: If the FC-SW2 Auto Save parameter is enabled on the Switch Properties window, then every time the active zone set changes, the switch module will copy it into an inactive zone set stored on the switch module. 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 window 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 3-9](#) describes the zoning tool bar operations.

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

Table 3-9. Edit Zoning Window Tool Bar Buttons and Icons

Tool Bar Button	Description
 Zone Set	Create Zone Set button - create a new zone set
 Zone	Create Zone button - create a new zone
 Alias	Create Alias button - create another name for a set of objects
 Insert	Add Member button - add the selected zone to a zone set, or add the 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
	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

3.5.6.3.2

Configuring the Zoning Database

Use the Zoning Config window to change the Auto Save and Default Visibility configuration parameters. In the Faceplate window, open the Zoning menu and select **Edit Zoning Config** to open the Zoning Config window shown in [Figure 3-17](#). After making changes, click the **OK** button to put the new values into effect.

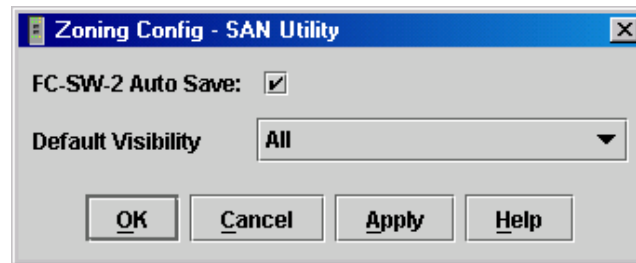


Figure 3-17. Zoning Config Window

3.5.6.3.2.1

FC-SW-2 Auto Save

The FC-SW-2 Auto Save parameter determines whether changes to the active zone set that a switch module 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 Auto Save is enabled, the switch module firmware saves changes to the active zone set in temporary memory and to the zoning database. If Auto Save is disabled, changes to the active zone set are stored only in temporary memory which is cleared when the switch module is reset.

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

3.5.6.3.2.2

Default Visibility

Default visibility determines the level of communication that is permitted among ports/devices when there is no active zone set. The default visibility parameter can be set differently on each switch. When default visibility is enabled (ALL) on a switch, all ports/devices on the switch module can communicate with all ports/devices on switches that also have default visibility enabled. When Default Visibility is disabled (NONE), none of the ports/devices on that switch module can communicate with any other port/device in the fabric.

3.5.6.3.3

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 module or another switch. To save a zoning database to a file, do the following:

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

3.5.6.3.4

Restoring the Zoning Database from a File

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

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

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

3.5.6.3.5

Restoring the Default Zoning Database

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

CAUTION! This command will deactivate the active zone set.

To restore the default zoning for a switch:

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

3.5.6.3.6

Deleting the Zoning Database

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

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

3.5.6.4

Managing Zone Sets

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

- [Creating a Zone Set](#)
- [Activating and Deactivating a Zone Set](#)
- [Copying a Zone to a Zone Set](#)
- [Removing a Zone from a Zone Set or from All Zone Sets](#)
- [Removing a Zone Set](#)

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

3.5.6.4.1

Creating a Zone Set

To create a zone set, do the following:

1. Open the Zoning menu, and select **Edit Zoning** to open the Edit Zoning window.
2. Open the Edit menu, and select **Create Zone Set** to open the Create Zone Set window.
3. Enter a name for the zone set, and click the **OK** button. The new zone set name is displayed in the Zone Sets window. A zone set name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, -, ^, and \$.
4. To create new zones in a zone set, do one of the following:
 - Right-click a zone set and select **Create A Zone** from the popup menu. In the Create a Zone window, enter a name for the new zone, and click the **OK** button. The new zone name is displayed in the Zone Sets window.
 - Copy an existing zone by dragging a zone into the new zone set. Refer to ["Copying a Zone to a Zone Set" on page 3-52](#).
5. Click the **Apply** button to save changes to the zoning database.

3.5.6.4.2

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 module distributes that zone set to the temporary zoning database on every switch in the fabric.

The purpose of the deactivate function is to suspend all fabric zoning which results in free communication fabric wide or no communication depending on the default visibility setting. Refer to ["Default Visibility" on page 3-49](#) for more information. It is not necessary to deactivate the active zone set before activating a new one.

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

3.5.6.4.3

Copying a Zone to a Zone Set

To copy an existing zone and its membership from one zone set to another, select the zone and drag it to the chosen zone set. Click the **Apply** button to save changes to the zoning database.

3.5.6.4.4

Removing a Zone from a Zone Set or from All Zone Sets

You can remove a zone from a zone set or from all zone sets in the database.

1. In the Faceplate window, open the Zoning menu and select **Edit Zoning** to open the Edit Zoning window.
2. In the Zone Sets tree, select the zone(s) to be removed.
3. Open the Edit menu, and select **Remove** to remove the zone from the zone set, or select **Remove from All Zones** to remove the zone from all zone sets.
4. Click the **Apply** button to save changes to the zoning database.

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

3.5.6.4.5

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 is saved on the switch.

To delete a zone set from the database, do the following:

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

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

3.5.6.5

Managing Zones

Managing zones involves the following:

- [Creating a Zone in a Zone Set](#)
- [Adding Zone Members](#)
- [Renaming a Zone or a Zone Set](#)
- [Removing a Zone Member](#)
- [Removing a Zone from a Zone Set](#)
- [Removing a Zone from All Zone Sets](#)
- [Changing Zone Types](#)

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

3.5.6.5.1

Creating a Zone in a Zone Set

When a zone is created, its zone type is soft. To change the zone type to a hard zone, refer to ["Changing Zone Types" on page 3-56](#) for more information. Refer to ["Zones" on page 3-41](#) for information on zone types (soft and hard). To create a zone in a zone set, do the following:

1. Open the Zoning menu, and select **Edit Zoning** to open the Edit Zoning window.
2. Select a zone set.
3. Open the Edit menu and select **Create a Zone**.
4. In the Create a Zone window, enter a name for the new zone, and click the **OK** button. The new zone name is displayed in the Zone Sets window. 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 -.

Note: If you enter the name of a zone that already exists in the database, the SAN Utility application will ask if you would like to add that zone and its membership to the zone set.

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

3.5.6.5.2

Adding Zone Members

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

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

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

- a. Right click the selected zone.
- b. Open the Edit menu and select **Create Members**.
- c. Choose the **WWN, Domain/Port, or First Port Address** radio button.
- d. Enter the hexadecimal value for the port/device according to the radio button selection: 16 digits for a WWN member, 4 digits for a Domain/Port member (DDPP), or a 6-digit Fibre Channel Address for a First Port Address member (DDPPAA) where D=domain ID, P=port number, and A=ALPA.

3. Click the **OK** button to add the member and save the change.

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.

3.5.6.5.3

Renaming a Zone or a Zone Set

To rename a zone, do the following:

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

3.5.6.5.4

Removing a Zone Member

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

1. In the Edit Zoning window, select the zone member to be removed.
2. Open the Edit menu and select **Remove**.
3. Click the **OK** button to save changes and close the Edit Zoning window.

3.5.6.5.5

Removing a Zone from a Zone Set

Zones that are no longer members of any zone set are moved to the orphan zone set. The orphan zone set is saved on the switch module. To remove a zone from a zone set, do the following:

1. In the Edit Zoning window, select the zone to be removed. The selected zone will be removed from that zone set only.
2. Open the Edit menu and select **Remove**.
3. Click the **OK** button to save changes and close the Edit Zoning window.

3.5.6.5.6

Removing a Zone from All Zone Sets

Zones that are no longer members of any zone set are moved to the orphan zone set. The orphan zone set is saved on the switch module. To remove a zone from all zone sets including the orphan zone set, do the following:

1. In the Edit Zoning window, select the zone to be removed.
2. Open the Edit menu and select **Remove Zone from All Sets**.
3. Click the **OK** button to save changes and close the Edit Zoning window.

3.5.6.5.7

Changing Zone Types

To change a zone type, do the following:

1. In the Faceplate window, select the switch module with the zone type to change.
2. Click the **Zoning** button to open the Edit Zoning window.
3. In the Zone Sets tree, select the zone to change.
4. Open the Edit menu and select **Set Zone Type** to open the Set Zone Type window.
5. Open the Zone Type pull-down menu and select **Soft** or **ACL**.
 - Soft zoning is the least restrictive type of zoning.
 - ACL zoning is hard zoning and is enforced by hardware and defines access to a given port. ACL zones need not include interswitch links.

3.5.6.6

Managing Aliases

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

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

You will not see aliases in the active zone set.

3.5.6.6.1

Creating an Alias

To create an alias, do the following:

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

3.5.6.6.2

Adding a Member to an Alias

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

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

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

- a. Right click the selected alias.
- b. Open the Edit menu and select **Create Members**.
- c. Choose the **WWN, Domain/Port**, or **First Port Address** radio button.

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

3.5.6.6.3

Removing an Alias from All Zones

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

1. In the Zone Sets tree in the Edit Zoning window, select the alias to be removed.
2. Open the Edit menu, and select **Remove Alias from All Zones**.
3. Click the **Yes** button in the Remove window.

3.5.6.7

Merging Fabrics and Zoning

If you join two fabrics with an interswitch link, the active zone sets from the two fabrics attempt to merge automatically. The fabrics may consist of a single switch or many switches already connected together. The switches in the two fabrics attempt to create a new active zone set containing the union of each fabric's active zone set. The propagation of zoning information only affects the active zone set, not the configured zone sets, unless FC-SW-2 Auto Save is turned on.

3.5.6.7.1

Zone Merge Failure

If a zone merge is unsuccessful, the interswitch links between the fabrics will isolate due to a zone merge failure, which will generate an alarm. The reason for the E_Port isolation can also be determined by viewing the port information. Refer to ["Port Information Data Window" on page 3-101](#) and the ["Show Command" on page 2-58](#) (Port keyword).

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 soft 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.

3.5.6.7.2

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 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.

If the zone sets to merge have the same Zone A that only differ in the type of zone (soft vs. ACL), the zone sets will merge. If this is a 2 switch fabric, Switch 1 will state that Zone A is soft and Switch 2 will state that Zone A is ACL.

Refer to ["Managing Zones" on page 3-53](#) for information about adding and removing zone members. Refer to ["Resetting a Port" on page 3-107](#) for information about resetting a port.

3.6

Managing Switch Modules

This section describes the following tasks that manage switch modules in the fabric.

- [Managing User Accounts](#)
- [Displaying Switch Module Information](#)
- [Configuring Port Threshold Alarms](#)
- [Paging a Switch Module](#)
- [Setting the Date/Time and Enabling NTP Client](#)
- [Setting Temperature Thresholds](#)
- [Resetting a Switch Module](#)
- [Configuring a Switch Module](#)
- [Archiving a Switch Module Configuration](#)
- [Restoring a Switch Module Configuration](#)
- [Restoring the Factory Default Configuration](#)
- [Managing Firmware](#)

3.6.1

Managing User Accounts

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

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

Switches come from the factory with the following user accounts:

Table 3-10. Factory User Accounts

Account Name	Password	Admin Authority	Expiration
USERID	PASSWORD ("0" is zero)	true	never expires
admin	admin	true	never expires
images	images	false	never expires

The USERID account is the only user that can manage all user accounts with the User Account Administration windows. The USERID account can create, remove, or modify user accounts, and change account passwords. The USERID account can also view and modify the switch module and its configuration with SAN Utility. The USERID account can not be removed.

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

The Images account can not be removed, and is required for exchanging files with the switch module using FTP.

The factory switch module configuration does not enforce user accounts and passwords. This means that no account name and password are required to add a fabric and modify switch module configurations using SAN Utility. You can only use the command line interface to change the enforcement (on or off) of user accounts and authority. To enforce user accounts and authority, set the UserAuthentication parameter to True using the Set Setup System command. Refer to ["Set Setup Command" on page 2-52](#).

3.6.1.1

Creating User Accounts

To create a user account on a switch, open the Switch menu in the Faceplate window and select **User Accounts....** This displays the User Account Administration window shown in [Figure 3-18](#). A switch module can have a maximum of 15 user accounts.

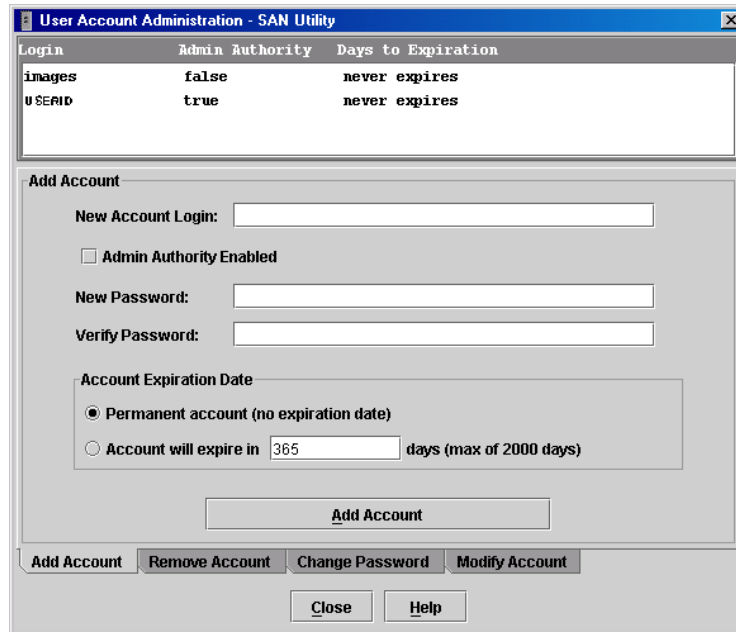


Figure 3-18. User Account Administration Window – Add Account

1. To open the User Account Administration windows, open the Switch menu in the Faceplate window, and select **User Accounts....**
2. Click the **Add Account** tab to open the Add Account tab page.
3. Enter an account name in the New Account Login field. Account names are limited to 15 characters.
4. If the account is to have the ability to modify switch module configurations, check the **Admin Authority Enabled** box.
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 4 characters and no more than 20.
6. If this account is to be permanent with no expiration date, click the **Permanent Account** radio button. Otherwise, click the **Account Will Expire** button and enter the number days in which the account will expire.
7. Click the **Add Account** button to add the newly defined account.

3.6.1.2

Removing a User Account

To remove a user account on a switch, open the Switch menu in the Faceplate window and select **User Accounts....** Click the **Remove Account** tab in the window to present the display shown in [Figure 3-19](#). Select the account (login) name from the list of accounts at the top of the window and click the **Remove Account** button.

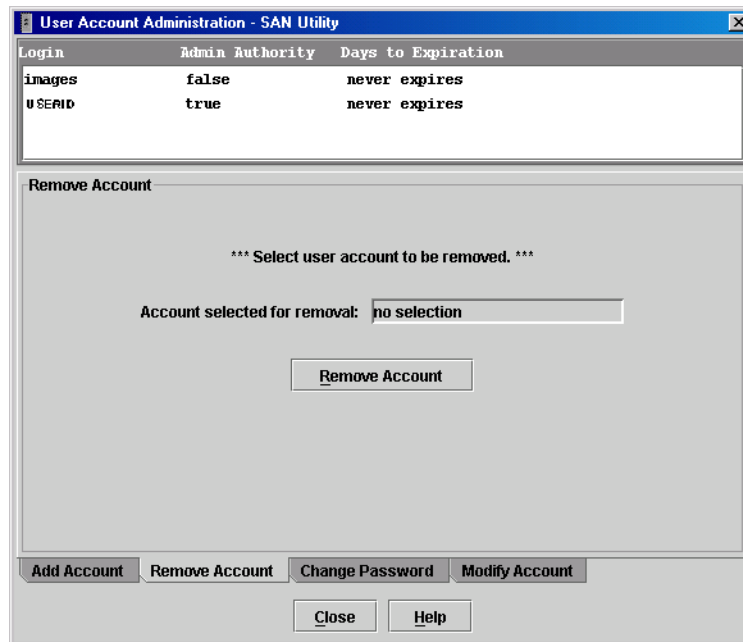


Figure 3-19. User Account Administration Window – Remove Account

3.6.1.3

Changing a User Account Password

To change the password for an account on a switch, open the Switch menu in the Faceplate window and select **User Accounts....** Click the **Change Password** tab in the window to present the display shown in [Figure 3-20](#). Select the account (login) name from the list of accounts at the top of the window, then enter the old password, the new password, and verify the new password in the corresponding fields. Click the **Change Password** button. Any user can change their password for their account, but only the Admin account name can change the password for another user's account. If the administrator does not know the user's original password, the administrator must remove the account and add the account.

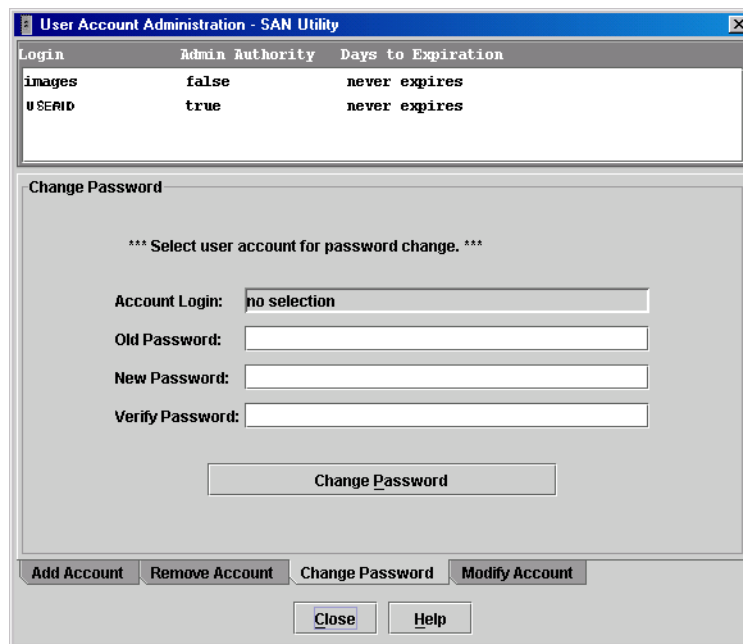


Figure 3-20. User Account Administration Window – Change Password

3.6.1.4

Modifying a User Account

To modify a user account on a switch, open the Switch menu in the Faceplate window and select **User Accounts....** This displays the User Account Administration window shown in [Figure 3-21](#). Click the **Modify Account** tab. Select the account (login) name from the list of accounts at the top of the window. Click the Admin authority Enabled check box to grant admin authority to the account name. Click an Account Expiration Date radio button. If the account is not to be permanent, enter the number of days until the account expires. Click the **Modify Account** button to save the changes. Click the **Close** button to close the User Account Administration window.

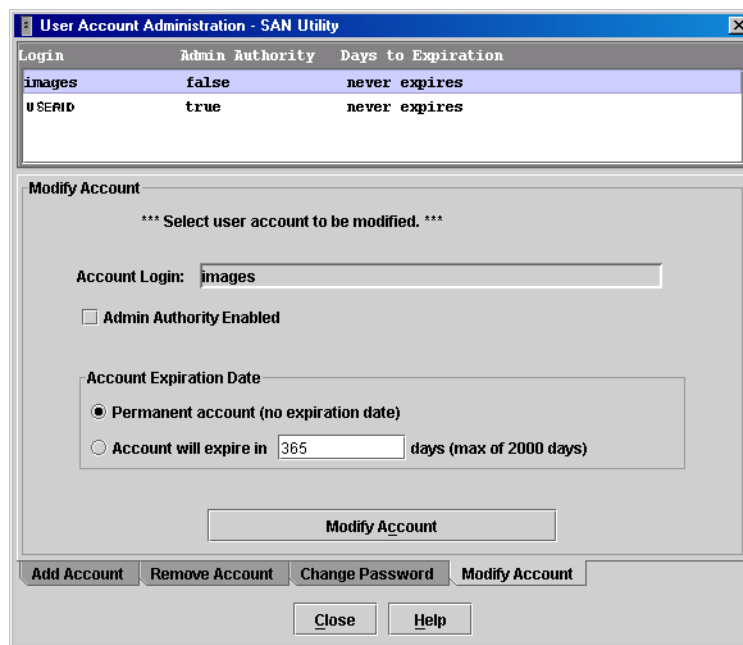


Figure 3-21. User Account Administration Window - Modify Account

3.6.2 Displaying Switch Module Information

The Faceplate window and data windows provide the following switch information:

- [Hardware Status](#)
- [Devices Data Window](#)
- [Switch Data Window](#)
- [Link Data Window](#)
- [Port Statistics Data Window](#)
- [Port Information Data Window](#)
- [Configured Zonesets Data Window](#)

Figure 3-22 shows the Faceplate window for the QLogic 6-Port Enterprise Fibre Channel Switch Module.

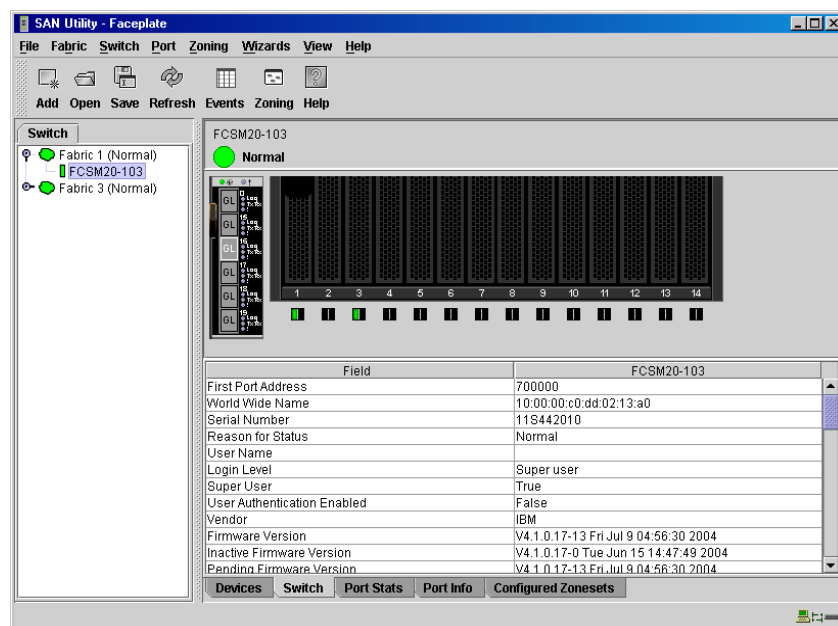


Figure 3-22. Faceplate Window - Switch Information

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

- Click the **Refresh** button.
- Open the View menu and select **Refresh**.

- Press the F5 key.
- Right-click a switch module in the Topology window and select **Refresh Switch** from the popup menu.
- Right-click in the graphic window of the Faceplate window, and select **Refresh Switch** from the popup menu.

3.6.2.1

Hardware Status

The Faceplate window shows the status of the switch module LEDs as shown in [Figure 3-23](#). The switch module LEDs and port LEDs are described as follows:

- Power-On LED – Illuminates green to indicate that the voltage to switch module is in the proper range.
- Switch Fault LED – Illuminates amber to indicate an over temperature condition or a POST (Power On Self Test) error.
- Port Logged-In LED – Illuminates green to indicate that a device is logged into the port.
- Port Activity LED – Illuminates green to indicate that data traffic is passing through the port.
- Port Fault LED – Illuminates amber to indicate a port fault.

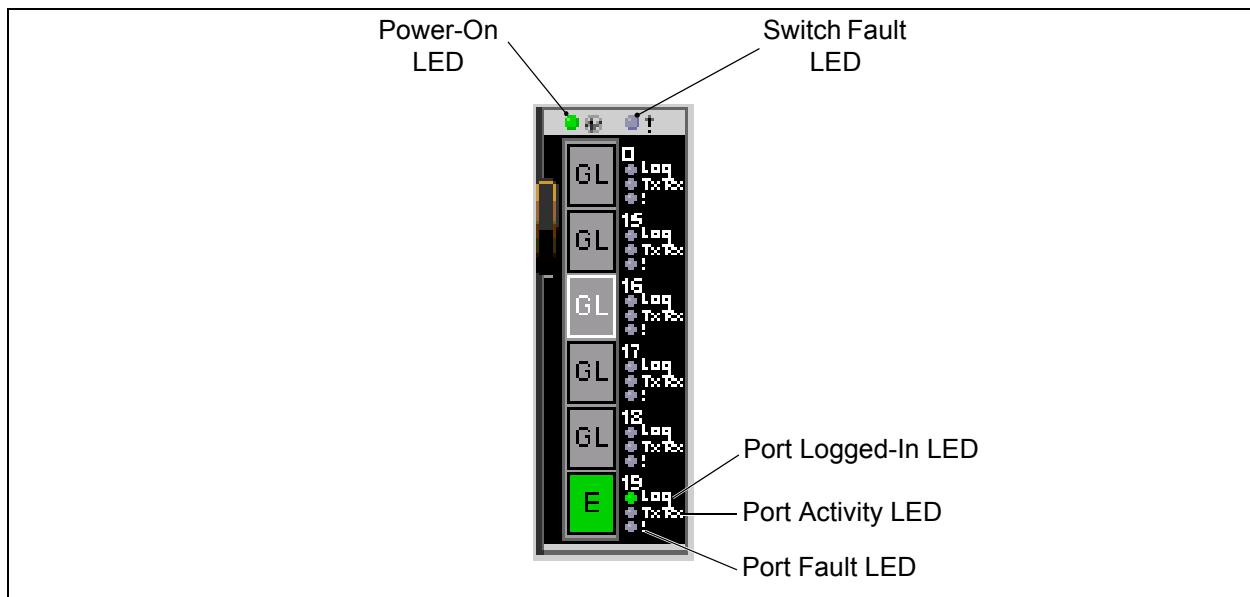


Figure 3-23. Hardware Status LEDs

3.6.2.2

Devices Data Window

The Devices data window displays information about devices (hosts and storage targets) connected to the switch module. Click the **Devices** tab below the data window 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 or the Topology window. Refer to ["Devices Data Window" on page 3-35](#) for a description of the entries in the Devices data window.

3.6.2.3

Switch Data Window

The Switch data window displays current network and switch module information for the selected switch modules. Refer to ["Configuring a Switch Module" on page 3-77](#) for more information about the Switch data window. To open the Switch data window, select one or more switch modules in the Topology window, or open the Faceplate window, and click the **Switch** tab below the window. [Table 3-11](#) describes the Switch data window entries.

Table 3-11. Switch Data Window Entries

Entry	Description
First Port Address	Switch module Fibre Channel address
World Wide Name	Switch module World Wide Name
Serial Number	Number assigned to each switch module
Reason for Status	Additional status information
User Name	Account name
Login Level	Authority level
Super User	Super user privileges enabled/disabled
UserAuthentication Enabled	Enforcement of account names and authority
Vendor	Switch module manufacturer
Firmware Version	Active firmware version
Inactive Firmware Version	Inactive firmware version
Pending Firmware Version	Firmware version that will be activated at the next reset
PROM/Boot Version	PROM boot version
MAC Address	Media Access Control address

Table 3-11. Switch Data Window Entries (Continued)

Entry	Description
IP Address	Internet Protocol address
Subnet Mask	Mask that determines the IP address subnet
Gateway	Gateway address
SNMP Enabled	SNMP enabled or disabled
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.
Switch Type	Switch module model
Operational State	Switch module operational state: Online, Offline, Diagnostic
Administrative State	Current switch module administrative state
Configured Admin State	Switch module administrative state that is stored in the switch configuration
R_A_TOV	Resource allocation timeout value
E_D_TOV	Error detect timeout value
FC-SW-2 Compliant	Zoning merge status. If True, changes to the active zone set are propagated throughout the fabric. If false, changes to both the active zone set and zoning database are propagated throughout the fabric.
Legacy Address Format	Legacy port addressing status. Enabled only for interoperability with non-FC-SW-2 switches.
FC-SW-2 Auto Save	Zoning auto save status. Saves zoning updates in temporary memory and the zoning database (True) or only in temporary memory (False).
Zoning Default Visibility	Zoning visibility status. Permits (All) or prevents (None) communication between attached devices in the absence of an active zone set.
Security Auto Save	Not applicable.
Security Fabric Binding Enable	Not applicable.

Table 3-11. Switch Data Window Entries (Continued)

Entry	Description
Temperature	Internal switch module temperature °C
Fan 1 Status	Not applicable.
Fan 2 Status	Not applicable.
Fan 3 Status	Not applicable.
Power Supply 1 Status	Not applicable.
Power Supply 2 Status	Not applicable.
Beacon Status	Beacon status. Port Logged-In LEDs are blinking (On) or not (off).
Broadcast Support	Broadcast support status. Broadcast support is enabled or disabled (default).
In-band Enabled	In-band management status. Permits (True) or prevents (False) a switch module from being managed over an ISL.
Temperature Failure Port Shutdown	Port shutdown status. If True, all ports are downed when the switch temperature exceeds the Failure Temperature. If False, port operational states remain unchanged. The default is false.
Warning Temperature	Warning temperature threshold in °C above which the switch generates a warning condition alarm. The default warning temperature threshold is 75 °C.
Failure Temperature	Failure temperature threshold in °C above which the switch module generates a failure condition alarm and disables all external ports. The default failure temperature threshold is 80 °C.
NTP Client Enabled	NTP client status. Enables or disables the switch module's ability to synchronize its time with an NTP server.
NTP Server Address	The IP address of the centralized NTP server. Ethernet connection to NTP server is required.
Number of Donor Groups	Total number of donor port groups. A donor group is a set of ports on a switch module that can donate buffer credits to each other.

Table 3-11. Switch Data Window Entries (Continued)

Entry	Description
Embedded GUI	SAN Browser status. Enables or disables the SAN Browser on the switch module.
Inactivity Timeout	Number of minutes the switch module waits before terminating an idle CLI session. Zero (0) disables the time out threshold.

3.6.2.4

Link Data Window

The Link data window displays information about all switch module links in the fabric or selected links. This information includes the switch module name, the port number at the end of each link, and the link status icons. To open the Link data window, click the **Link** tab below the data window in the Topology window.

3.6.2.5

Port Statistics Data Window

The Port Statistics data window displays port performance data for the selected ports. To open the Port Statistics data window, click the **Port Stats** tab below the data window in the Faceplate window. Refer to [Table 3-21](#) for a description of the Port Statistics data window entries.

The Statistics pull-down menu is available on the Port Statistics data window, and provides different ways to view detailed port information. Click the down arrow to open the pull-down menu. In the Statistics menu, you can do the following:

- Select **Absolute** to view the total count of statistics since the last switch module 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 the **Clear Baseline** button to set the current baseline.

3.6.2.6

Port Information Data Window

The Port Information data window displays port detail information for the selected ports. To open the Port Statistics data window, click the **Port Info** tab below the data window in the Faceplate window. Refer to [Table 3-22](#) for a description of the Port Information data window entries.

3.6.2.7

Configured Zonesets Data Window

The Configured Zonesets data window displays all zone sets, zones, aliases, and zone membership in the zoning database, as shown in [Figure 3-24](#). To open the Configured Zonesets data window, click the **Configured Zonesets** tab below the data window in the Faceplate window.

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

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

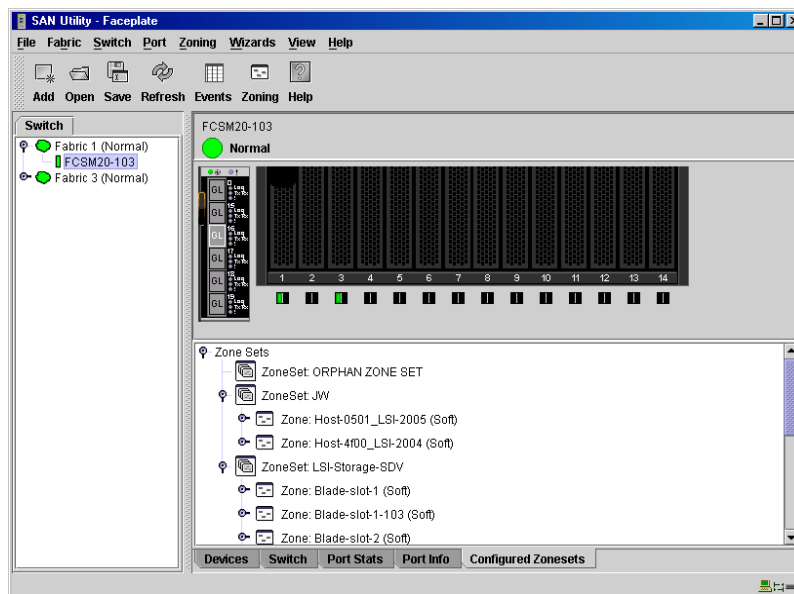


Figure 3-24. Configured Zonesets Data Window

3.6.3

Configuring Port Threshold Alarms

You can configure the switch module 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, do the following:

1. In the Faceplate window, open the Switch menu and select **Port Threshold Alarm Configuration**. The Port Threshold Alarm Configuration window shown in [Figure 3-25](#) prompts you to enable or disable all alarms, select an event, set triggers, set a sample window and enable or disable an individual alarm.

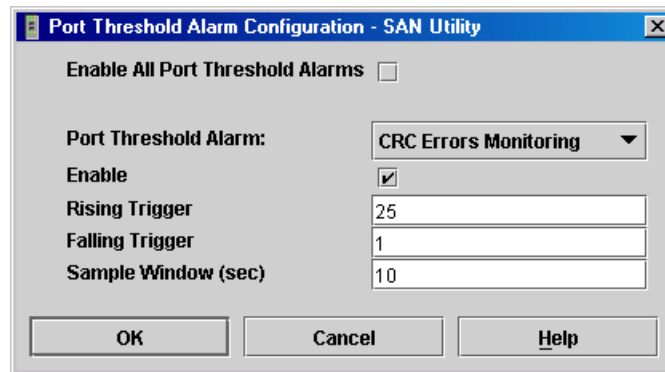


Figure 3-25. Port Threshold Alarm Configuration Window

2. Check the **Enable All Port Threshold Alarms** check box to enable monitoring for all the individual alarm types that are enabled. The **Enable All Port Threshold Alarms** check box is the master control for the individual alarms. For example, the switch module will monitor CRC errors only if both the **CRC Error Monitoring** box and the **Enable All Port Threshold Alarms** check box are checked.
3. Select an event type from the Port Threshold Alarm pull-down menu. Choose from the following options:
 - CRC error monitoring
 - Decode error monitoring
 - ISL monitoring
 - Login monitoring
 - Logout monitoring
 - Loss of signal monitoring
4. Check the **Enable** box to make the alarm eligible for use.

5. 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 module 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 3-26](#).
6. 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 module will down a port if a rising trigger alarm is not cleared after three consecutive sample windows.

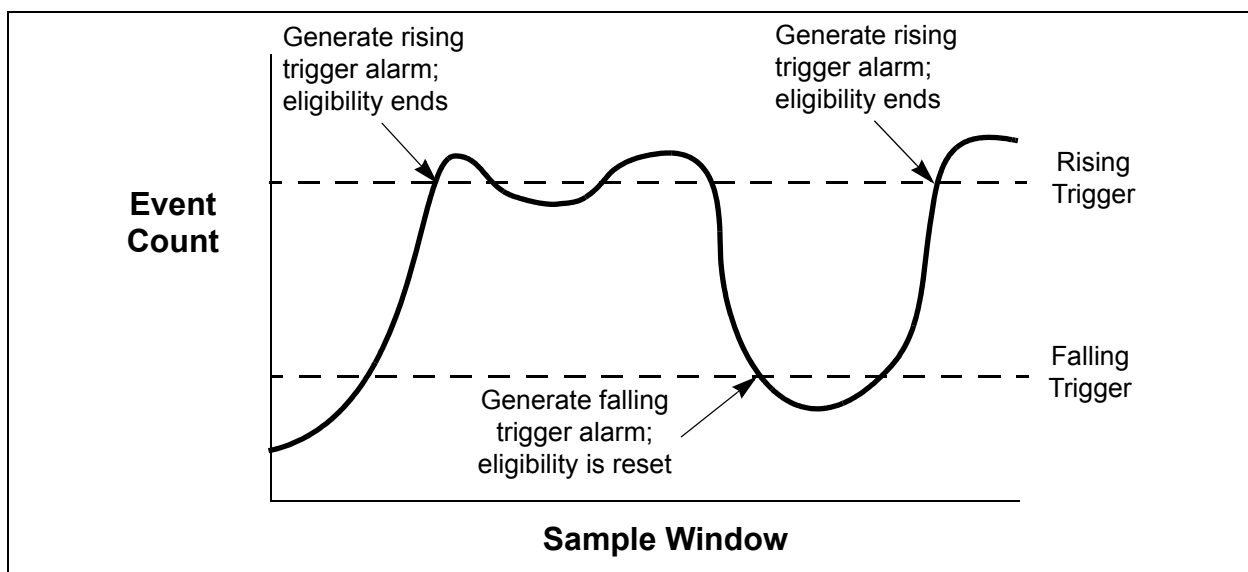


Figure 3-26. Port Threshold Alarm Example

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

3.6.4 Paging a Switch Module

You can use the beacon feature to page a switch module. The beacon feature causes all Port Logged-In LEDs to flash, making it easier to recognize. To page a switch module, open the Switch menu in the Faceplate window and enable the **Toggle Beacon** selection. To cancel the beacon, reselect **Toggle Beacon**.

3.6.5

Setting the Date/Time and Enabling NTP Client

The NTP Client feature allows switch modules to synchronize their date and time with an NTP server. Refer to "NTP Client" on page 3-86 for more information. To set the date/time and enable the NTP Client on a switch module, do the following:

1. Select a switch module, and open the Faceplate window.
2. Open the Switch menu, and select **Set Date/Time** to open the Date and Time window.
3. Select the month, day, year, and time.
4. Click the **NTP Client Enabled** checkbox to allow for switches to synchronize their time a centralized server.
5. Enter the IP address of the NTP server. Ethernet connection to NTP server is required.
6. Click **OK** to save the settings. The new date and time take effect immediately.

3.6.6

Setting Temperature Thresholds

You can set temperature thresholds by which the switch will generate an alarm or place the switch offline. The Temperature Thresholds dialog shown in [Figure 3-27](#) prompts you to enter a warning threshold and a failure threshold temperature (°C). To open the Temperature Thresholds dialog, open the faceplate display, open the Switch menu and select **Temperature Thresholds....**

- If the switch internal temperature exceeds the warning threshold, the switch generates an alarm.
- If the switch internal temperature exceeds the failure threshold and the **Enable Temperature Failure Port Shutdown** box is checked, the switch generates an alarm and places all ports down. After correcting the problem, you must reset the switch to bring the ports back online.

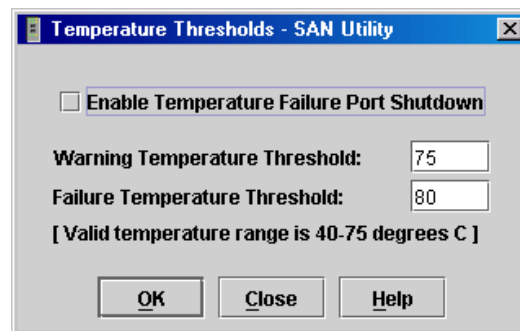


Figure 3-27. Temperature Thresholds Window

3.6.7

Resetting a Switch Module

Resetting a switch module reboots the switch module using configuration parameters in memory. Depending on the reset type, a switch module reset may or may not include a power-on self test or it may or may not disrupt traffic.

[Table 3-12](#) describes the switch module 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 a hot reset. When upgrading firmware across a fabric using non-disruptive activation, upgrade one switch module at a time and allow 75 seconds between switch modules.

CAUTION! Changes to the fabric may disrupt the hot reset process.

Common administrative operations that change the fabric include:

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

Management Interfaces:

After a hot reset is complete, management connections must be re-initiated:

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

Applicable Code Versions:

- Future firmware releases will be upgraded non-disruptively unless specifically indicated in its associated release notes
- A hot reset operation to previous switch module code releases is not supported.

Table 3-12. Switch Module Resets

Type	Description
Hot Reset	Resets a switch module without a power-on self test. This reset activates the pending firmware, but does not disrupt traffic. If errors are detected on a port during a hot reset, the port is reset automatically.
Reset without POST	Resets a switch module without a power-on self test. This reset activates the pending firmware and it is disruptive to switch traffic.
Hard Reset	Resets a switch module with a power-on self test. This reset activates the pending firmware and it is disruptive to traffic.

To reset a switch module using SAN Utility, do the following:

1. Select the switch module to be reset and open the Faceplate window.
2. Open the Switch menu and select the **Reset Switch** pull-down menu:
 - Select **Hot Reset** to perform a hot reset.
 - Select **Reset** to perform a standard reset.
 - Select **Hard Reset** to perform a hard reset.

3.6.8 Configuring a Switch Module

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

You can configure a switch module explicitly or you can use the Configuration Wizard. The Configuration Wizard is a series of windows that guide you through the chassis, network, and SNMP configuration steps on new or replacement switch modules.

3.6.8.1

Using the Configuration Wizard

SAN Utility detects a new switch module and presents the Initial Start window, from which the Configuration Wizard can be launched. The Configuration Wizard allows you to assign a temporary IP address to a connected switch module, eliminating the need to change your workstation's IP address for initial configuration of a new switch module. You can also launch the Configuration Wizard from the Wizards menu in either the Topology or the Faceplate window. Open the Wizards menu and select **Configuration Wizard**.

Use the Configuration Wizard to:

- Configure a new switch module in a fabric.
- Add a new switch module to an existing fabric.
- Replace or restore a switch module in an existing fabric.
- Recover or edit the IP configuration of an existing switch module.

3.6.8.2

Switch Properties

To open the Switch Properties window shown in [Figure 3-28](#), either select a switch module in the Topology window or open the Faceplate window for the switch module you will be configuring, and then open the Switch menu and select **Switch Properties**. You can also right-click a switch module icon in the Topology window or Faceplate window, and select **Switch Properties** from the popup menu.

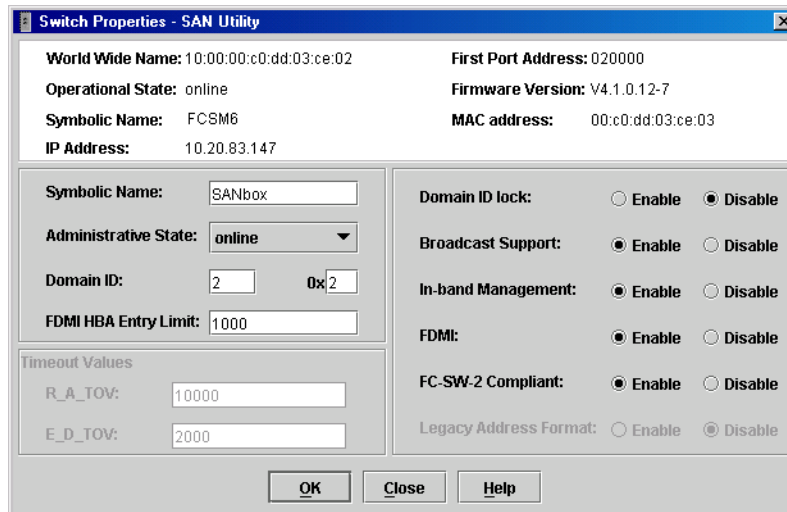


Figure 3-28. Switch Properties Window

Use the Switch Properties window to change the following switch module configuration parameters:

- [Symbolic Name](#)
- [Switch Module Administrative States](#)
- [Domain ID and Domain ID Lock](#)
- [Fabric Device Management Interface](#)
- [Broadcast Support](#)
- [In-band Management](#)
- [FC-SW-2 Compliance for Zoning](#)
- [Legacy Port Address Format](#)
- [Timeout Values](#)

The timeout values are displayed only for reference purposes when the switch module is online; they become active when the switch module is taken offline. After making changes, click the **OK** button to put the new values into effect.

3.6.8.2.1

Symbolic Name

The symbolic name is a user-defined name of up to 63 characters that identifies the Fibre Channel switch module. The symbolic name is used in the Topology and Faceplate windows, as well as many data windows to more easily identify switch modules. The illegal characters are the pound sign (#), semi-colon (;), and comma (,).

3.6.8.2.2

Switch Module Administrative States

The switch module administrative state determines the operational state of the switch module and its ports. The switch module 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 module configuration and is preserved across switch module resets. SAN Utility always makes changes to the configured administrative state. The configured administrative state is displayed in the Switch Properties window.
- The current administrative state is the state that is applied to the switch module for temporary purposes and is not retained across switch module resets. The current administrative state is set using the Set Switch command. Refer to the ["Set Command" on page 2-33](#).

Table 3-13 describes the administrative state values.

Table 3-13. Switch Module Administrative States

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

3.6.8.2.3

Domain ID and Domain ID Lock

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

Switches come from the factory with the domain IDs unlocked. This means that if there is a domain ID conflict in the fabric, the switch module 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 module and a domain ID conflict occurs, one of the switch modules will isolate as a separate fabric and the Logged-In LEDs on both switches will flash to show the affected ports. Refer to the ["Set Config Command" on page 2-35](#) for information about the Switch keyword and the Domain ID Lock and Principal Priority parameters.

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

3.6.8.2.4

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. SAN Utility will report any and all FDMI information reported by the entry switch module, if FDMI is enabled on the entry switch module. To view FDMI data, FDMI must be enabled on the entry switch module and on all other switch modules in the fabric which 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 window to configure the maximum number of HBAs that can be registered with a switch module. If the number of HBAs exceeds the maximum number, the FDMI information for those HBAs can not be registered.

Use the **FDMI Enabled** radio button on the Switch Properties window to enable or disable FDMI. If FDMI is enabled on an HBA, the HBA forwards information about itself to the switch module when the HBA logs into the switch module. If FDMI is enabled on a switch module, the switch module stores the HBA information in its FDMI database. Disabling FDMI on a switch module clears the FDMI database. If you disable FDMI on a switch module, 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 module.

To view detailed FDMI information for a device, open the Topology window, click the **Devices** tab, and click the **Information (i)** button in the Details column of the Devices data window. The Detailed Devices Display window displays the specific information for that device. Refer to "[Devices Data Window](#)" on page 3-35 for more information.

3.6.8.2.5

Broadcast Support

Broadcast is supported which allows for TCP/IP support. Broadcast is implemented using the proposed standard specified in *Multi-Switch Broadcast for FC-SW-3, T11 Presentation Number T11/02-031v0*. Fabric Shortest Path First (FSPF) is used to set up a fabric spanning tree used in transmission of broadcast frames. Broadcast frames are retransmitted on all ISLs indicated in the spanning tree and all online N_Ports and NL_Ports. Broadcast zoning is supported with Access Control List (ACL) hard zones. When a broadcast frame is received, these hard zones are enforced at the N_Ports and NL_Ports. If the originator of the broadcast is in a hard zone, the frame is retransmitted on all online N_Ports and NL_Ports within the hard zone. If the originator of the broadcast frame is not in a hard zone, the frame is retransmitted on online N_Ports and NL_Ports that are not in a hard zone. The default setting is disabled.

3.6.8.2.6

In-band Management

In-band management is the ability to manage switch modules across interswitch links using SAN Utility, SNMP, management server, or the application programming interface. The switch module comes from the factory with in-band management enabled. If you disable in-band management on a particular switch module, you can no longer communicate with that switch module by means other than an Ethernet.

3.6.8.2.7

FC-SW-2 Compliance for Zoning

When a zone set is activated, the QLogic 6-Port Enterprise Fibre Channel Switch Module and other FC-SW-2 compliant switches propagate the active zone set to all switches in the fabric. Some non-FC-SW-2 compliant switches propagate not only the active zone set, but the entire zoning database. Disabling this parameter causes the switch module to propagate the zoning database, and therefore, interoperate with non-FC-SW-2 switches. For FC-SW-2 compliant fabrics, this parameter should be enabled.

Note: The FC-SW-2 Compliant setting must be the same on all switches in the fabric, otherwise the interswitch links will not connect.

3.6.8.2.8

Legacy Port Address Format

Legacy Address Format should be enabled only to permit interoperability with certain older non-FC-SW-2 switches. Enabling this setting under other circumstances will disable zoning that is defined by domain ID and port number. This setting is available only when the FC-SW-2 Compliant setting is disabled. Contact your authorized maintenance provider for assistance in using this feature.

Note: The Legacy Address Format setting must be the same on all switches in the fabric, otherwise the interswitch links will not connect.

3.6.8.2.9

Timeout Values

The switch module timeout values determine the timeout values for all external ports on the switch module. [Table 3-14](#) describes the switch module timeout parameters. The R_A_TOV and E_D_TOV 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. Timeout values can be changed only if the switch module operational state is offline.

Table 3-14. 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.

3.6.8.3

Network Properties

Use the Network Properties window shown in [Figure 3-29](#) to display IP configuration parameters and enable remote logging. After making changes, click the **OK** button to put the new values into effect. To open the Network Properties window, select a switch module in the Topology window or open the Faceplate window, open the Switch menu and select **Network Properties**.

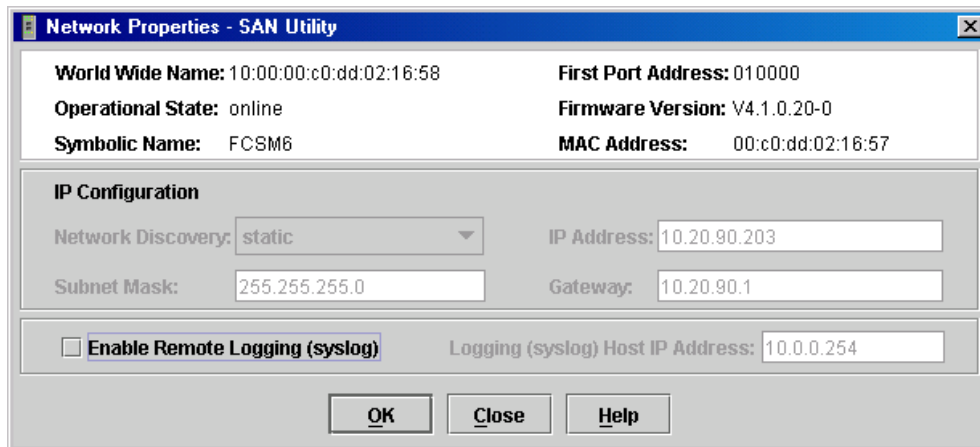


Figure 3-29. Network Properties Window

3.6.8.3.1

IP Configuration

The IP configuration identifies the switch module on the Ethernet network and determines the network discovery method to use. The IP configuration parameters listed in [Table 3-15](#) cannot be changed using SAN Utility. Make changes to the IP configuration parameters through the BladeCenter management module instead.

Table 3-15. IP Configuration Parameters

Parameter	Description
Network Discovery	Static - Uses the IP configuration parameters entered in the Switch Properties window.
IP Address	Internet protocol (IP) address for the Ethernet port. When the server unit is turned on, the management module loads the following factory default Ethernet IP addresses: <ul style="list-style-type: none"> ■ I/O-module bay 3: 192.168.70.129 ■ I/O-module bay 4: 192.168.70.130
Subnet mask	Subnet mask address for the Ethernet port. The default value is 255.255.255.0.
Gateway	IP gateway address. The default value is 10.90.90.254.

3.6.8.3.2

Remote Logging

The Remote Logging (syslog) 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.

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

Use a <tab> to separate the selector field (local0.info) and action field, which contains the log file path name (/var/adm/messages/messages.name).

3.6.8.3.3

NTP Client

The NTP Client feature allows a switch module to synchronize its date and time with an NTP server. NTP client ensures the consistency of date and time stamps in alarms and log entries. An Ethernet connection to the NTP server is required. Refer to ["Setting the Date/Time and Enabling NTP Client" on page 3-75](#).

3.6.9

Archiving a Switch Module Configuration

You can create an .XML archive file containing the configuration parameters. Basically any data received by SAN Utility is archived. However, user authentication and passwords are available only through the command line interface (CLI), and are not received by the SAN Utility, and thus are not archived. Refer to ["Backing up and Restoring Switch Module Configurations" on page 2-4](#) for information about using the CLI to back up and restore switch module configurations.

Archived parameters include the following:

- Switch properties and statistics
- IP configuration
- SNMP configuration
- Port properties and statistics
- Port alarm threshold configuration
- Zoning configuration

You can use this archive file to restore the configuration on the same switch module or on a replacement switch module. You can also use the archive file as a template for configuring new switch modules to add to a fabric. The user authentication parameter and user account information are not archived. You can use the archive later to restore the switch module. Refer to ["Restoring a Switch Module Configuration" on page 3-87](#) for more information.

To archive a switch module, do the following:

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

3.6.10

Restoring a Switch Module Configuration

Restoring a switch module configuration loads the archived configuration parameters to the switch module. The switch module configuration must be archived before it can be restored. The switch module archive must be compatible with the switch module to be restored; that is, you can restore a QLogic 6-Port Enterprise Fibre Channel Switch Module switch only with an archive from a QLogic 6-Port Enterprise Fibre Channel Switch Module. Refer to ["Archiving a Switch Module Configuration" on page 3-86](#) for more information.

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

To restore a switch module, do the following:

1. Log in to the fabric through the switch module you want to restore. You cannot restore a switch module over an ISL.
2. Open the Switch menu in the Faceplate window and select **Restore** to display the Restore window shown in [Figure 3-30](#). The Restore window offers a **Full Restore** and a **Selective Restore** tab.

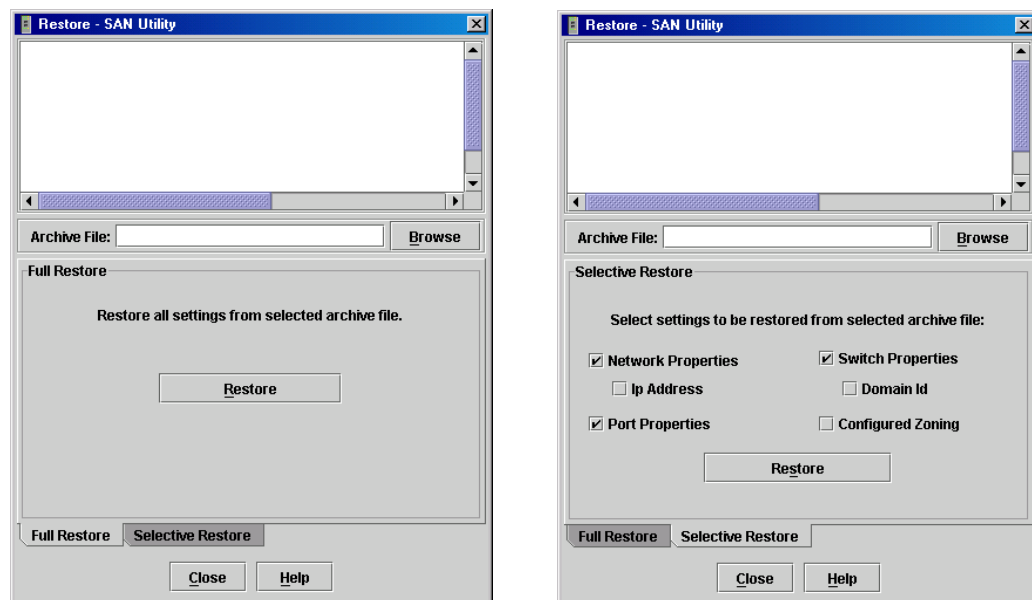


Figure 3-30. Restore Windows – Full and Selective

3. Enter the archive file name or browse for the file. This archive file must be one that was produced by the SAN Utility Archive function. Configuration backup files created with the Config Backup command are not compatible with the SAN Utility Restore function.
4. To restore all configuration settings, click the **Full Restore** tab, then click the **Restore** button. To restore selected configuration settings, click the **Selective Restore** tab and check one or more of the following boxes, then click the **Restore** button:
 - **Network Properties:** Restores all settings presented in the Network properties window except the IP address. Refer to "[Network Properties](#)" on page 3-84.
 - **IP Address:** Restores switch IP address in addition to the other network properties. Refer to "[Network Properties](#)" on page 3-84.
 - **Switch Properties:** Restores all settings presented in the Switch properties window except the domain ID. Refer to "[Switch Properties](#)" on page 3-78.
 - **Domain ID:** Restores switch domain ID in addition to the other switch properties.
 - **Port Properties:** Restores all settings presented in the Port properties window. Refer to "[Configuring Ports](#)" on page 3-103.
 - **Configured Zoning:** Restores all zone sets, zones, and aliases in the switch's zoning database.
5. If the archive file contains zone sets, a window prompts you to activate one of those zone sets:
 - e. Click the **Yes** button, and select a zone set from the drop-down menu in the Select Zone Set to be Activated window.
 - f. Click the **OK** button and view the results in the top pane of the Restore window.

3.6.11

Restoring the Factory Default Configuration

You can restore the switch module and port configuration settings to the factory default values. To restore the factory configuration on a switch module, open the Switch menu and select **Restore Factory Defaults**. [Table 3-16](#) lists the factory default switch configuration settings. Restoring the switch module to the factory default configuration does not restore the account name and password settings.

Table 3-16. Factory Default Configuration Settings

Setting	Value
Module Name	Fibre Channel Switch Module
Administrative State	Online
Domain ID	1
Domain ID Lock	False
In-band Management	True
Broadcast Support	Enable
Resource Allocation Timeout (R_A_TOV)	10000 milliseconds
Error Detect Timeout (E_D_TOV)	2000 milliseconds
IP Address	I/O-module bay 3: 192.168.70.129 I/O-module bay 4: 192.168.70.130
Subnet Mask Address	255.255.255.0
Gateway Address	10.90.90.254
Network Discovery	Static
NTP Client Enabled	False
NTP Server IP Address	10.0.0.254
FC-SW-2 Compliant	True
FDMI Enabled	True
FDMI HBA Entry Level	1000
Port State	Online
Port Speed	Auto-detect – external; 2G – internal
Port Type	GL – external; F – internal
I/O Stream Guard	Disabled

Table 3-16. Factory Default Configuration Settings (Continued)

Setting	Value
Device Scan Enabled	True
Remote Logging	False
Remote Logging Host Ip Address	10.0.0.254
SNMP Enabled	True
SNMP Proxy	True
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

3.6.12

Managing Firmware

The switch module memory is partitioned for two firmware images. One of these partitions contains the active firmware; that is, the firmware version that is in use. The other partition contains the inactive firmware which is not in use. The pending firmware is the firmware that will be activated at the next switch module reset. The pending firmware can be the active firmware or the inactive firmware. When you install new firmware, that image becomes the inactive firmware and the pending firmware. Upon resetting the switch module, this image becomes both the active and pending firmware.

Firmware management tools enable you to do the following:

- [Installing Firmware](#)
- [Activating the Pending Firmware](#)
- [Changing the Pending Firmware](#)

Note: To provide consistent performance throughout the fabric, ensure that all switches are running the same version of firmware.

3.6.12.1

Installing Firmware

Installing firmware involves loading, unpacking, and activating the firmware image on the switch. SAN Utility does this in one operation. Whenever possible, the switch module will attempt a hot reset to activate the firmware without disrupting traffic. During a hot reset operation, fabric services are unavailable for a short period (30-75 seconds). To ensure that a hot reset operation is successful, verify that all administrative changes to the fabric are complete. When you need to perform a hot reset on multiple switch modules, perform the hot reset on one switch module at a time, and allow a 75 second wait before performing the hot reset on the next switch module.

CAUTION! Changes to the fabric may disrupt the hot reset process.

Common administrative operations that change the fabric include:

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

Management Interfaces:

After a hot reset is complete, management connections must be re-initiated:

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

Applicable Code Versions:

- Future firmware releases will be upgraded non-disruptively unless specifically indicated in its associated release notes
- A hot reset to previous firmware releases is not supported.

To install firmware, do the following:

1. In the Faceplate window, open the Switch menu and select **Load Firmware**.
2. In the Firmware Upload window, click the **Select** button to browse and select the firmware file to be uploaded.
3. Click the **Start** button to begin the firmware load process.
4. SAN Utility prompts you to activate the new firmware using a hot reset, if possible. Click the **OK** button to reset the switch module and activate the new firmware.

3.6.12.2

Activating the Pending Firmware

To activate firmware that is both inactive and pending, open the Switch menu in the Faceplate window and select **Activate Firmware**. SAN Utility attempts a non-disruptive activation.

3.6.12.3

Changing the Pending Firmware

To change the pending firmware to the alternate image, do the following:

1. In the Faceplate window, open the Switch menu and select **Firmware Fallback**.
2. The Firmware Fallback window prompts you to confirm the firmware version that is to become the pending firmware. Click the **Yes** button to select the fallback firmware or **No** to cancel.

3.7 Managing Ports

This section describes the following tasks that manage ports and devices:

- [Displaying Port Information](#)
- [Configuring Ports](#)
- [Resetting a Port](#)

3.7.1 Displaying Port Information

Port information is available primarily in the Faceplate window. The Faceplate window data windows provide information and statistics for switch modules and ports. Use the Topology window to view status information on fabrics, switch modules, and links between switch modules. The Port Information data window for a 6-port Switch Module in a BladeCenter unit is shown in [Figure 3-31](#). The Port Information data window for a 6-port Switch Module in BladeCenter T unit is shown in [Figure 3-32](#).

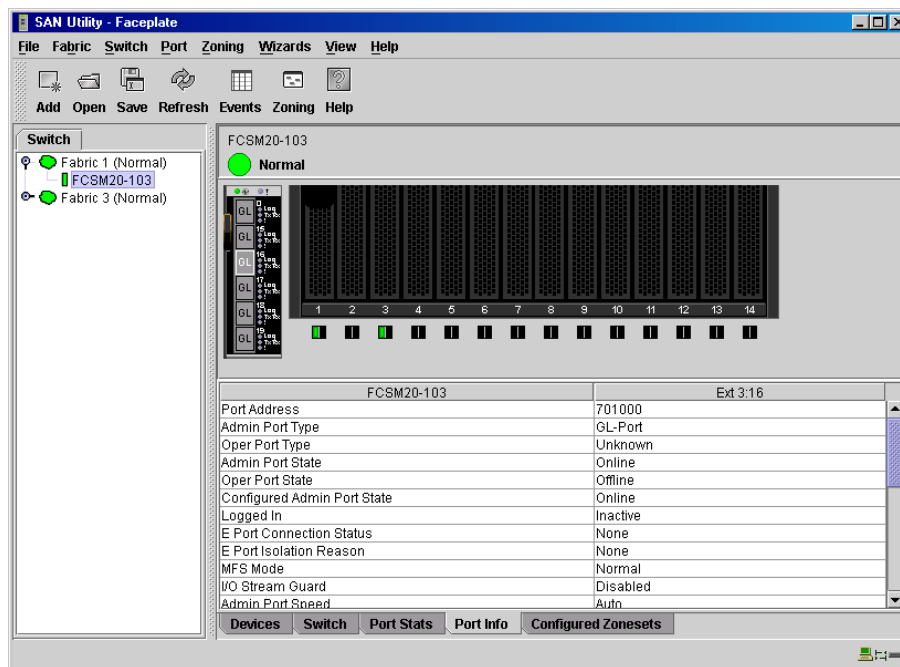


Figure 3-31. BladeCenter Faceplate Window – Port Information

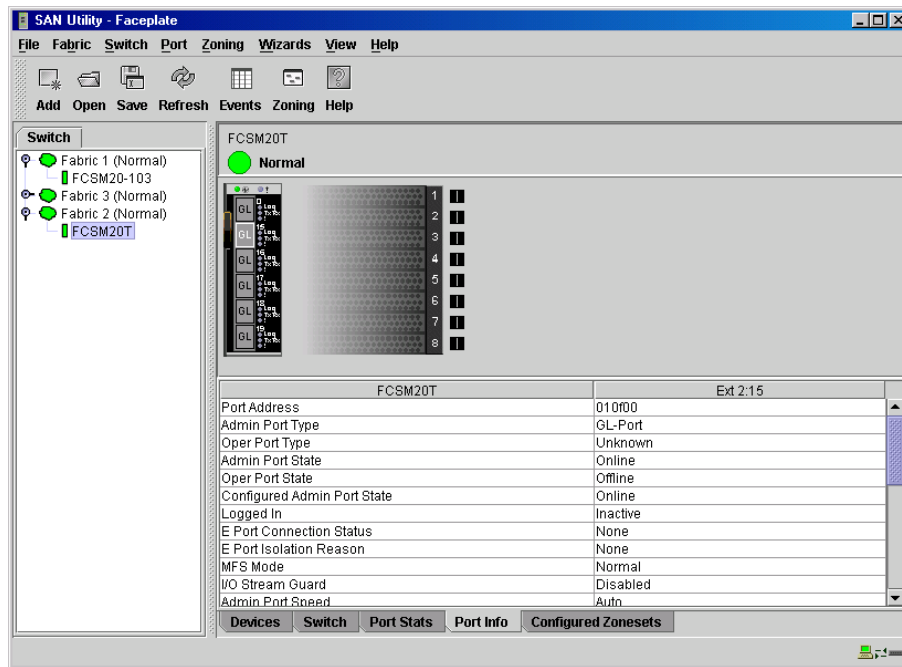


Figure 3-32. BladeCenter T Faceplate Window – Port Information

3.7.1.1

Monitoring Port Status

The Faceplate window provides the following port related information:

- SNMP configuration (see ["Switch Module Monitoring Using SNMP" on page 4-5](#))
- Port type
- Port operational state
- Port speed
- Port media

To display port number and status information for a port, position the cursor over a port on the Faceplate window. The status information changes depending on the View menu option selected.

3.7.1.2

Displaying Port Types

To display port type status, from the Faceplate window, open the View menu, and select **View Port Types**. [Table 3-17](#) lists the possible port types and their descriptions.

Table 3-17. Port Types

Type	Description
F	Fabric port - Supports a single public device (N_Port).
FL	Fabric loop port - Self discovers a single device (N_Port) or a loop of up to 126 public devices (NL_Port).
G	Generic port - Self discovers as an F_Port or an E_Port.
GL	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	Expansion port - The mode that a G_Port or GL_Port is in when attached by an ISL (interswitch link) to another fibre channel switch.
D	Donor port - Allows buffer credits to be used by another port.

3.7.1.3

Displaying Port Operational States

To display the operational state on each port in the Faceplate window, open the View menu and select **View Port States**. [Table 3-18](#) lists the available operational states. The port operational state refers to actual port state and not the administrative state you assigned.

Table 3-18. Port Operational States

State	Description
On	Online – The port is active and ready to send data.
la	Inactive – The port operational state is offline, but administrative state is online.
Iso	Isolated – E_Port has lost its connection. Refer to "Port Information Data Window" on page 3-101 for information about why the E_Port has isolated.
Off	Offline – The port is active, can receive signal, but cannot accept a device login.
Dia	Diagnostics – The port is in diagnostics mode in preparation for testing
Dn	Down – The port is disabled, power is removed from the lasers, and cannot accept a device login.

3.7.1.4

Displaying Port Speeds

To display the speed of each port in the Faceplate window, open the View menu and select **View Port Speeds**. [Table 3-19](#) lists the available port speeds.

Table 3-19. Port Speeds



State	Description
Au	Auto-detect
1-Gbps	1-Gbps transmission speed
2-Gbps	2-Gbps transmission speed

3.7.1.5

Displaying Transceiver Media Status

To display transceiver media status, open the View menu and select **View Port Media**. [Table 3-20](#) lists and describes the port media states.

Table 3-20. Port Transceiver Media View

Media Icon	Description
	Optical SFP module, online (Green)
	Optical SFP module, offline (Gray)
None	Empty port, no transceiver installed

3.7.1.6

Port Graphing and SAN Utility Performance View Application

You can use the SAN Utility Performance View application to view port performance as graphs. The SAN Utility Performance View window displays data communication rates and total errors for selected ports as shown in [Figure 4-4](#). You can graph communication data rates using either frames per second or KB per second. For more information about port graphing, see ["Using the SAN Utility Performance View Application"](#) on page 4-8.

3.7.1.7

Port Statistics Data Window

The Port Statistics data window displays statistics about port performance. To open the Port Statistics window, select one or more ports in the Faceplate window and click the **Port Stats** tab below the data window. [Table 3-21](#) describes the Port Statistics data window entries.

The Statistics pull-down menu is available on the Port Statistics data window. Click the down arrow to open the Statistics menu and then use one of the following methods to view the detailed port information.

- Select **Absolute** to view the total count of statistics since the last switch module or port reset.
- Select **Rate** to view the number of statistics counted per second over the polling period.
- Select **Baseline** to view the total count of statistics since the last time the baseline was set.

When viewing baseline statistics, click the **Clear Baseline** button to set the current baseline. The baseline will also be set when the switch module status changes from unreachable to reachable.

Table 3-21. 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.
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.

Table 3-21. Port Statistics Data Window Entries (Continued)

Entry	Description
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 port 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 module 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.
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.

Table 3-21. Port Statistics Data Window Entries (Continued)

Entry	Description
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.
Total Offline Sequences	Total number of offline sequences transmitted and received by the port.

3.7.1.8

Port Information Data Window

The Port Information data window displays detail information for the selected port. To open the Port Information data window, click the **Port Info** tab below the data window in the Faceplate window.

Table 3-22. Port Information Data Window Entries

Entry	Description
Port Address	Port Fibre Channel address.
Administrative Port Type	The administrative port type (G, GL, F, FL, or Donor). This value is persistent; it will be maintained during a switch module reset. During port an 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) which 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 module 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) which 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 module reset, and will be used after a reset to set the port operational state.
Logged In	Indicates whether logged in or not.
E Port Connection Status	Whether or not the E_Port is currently active. It can hold the values None, Connecting, Connected or Isolated.
E Port Isolation Reason	Why E_Port is isolated.
MFS Mode	Multiple Frame Sequence bundling status.
I/O Stream Guard	Whether RSCN suppression is enabled or disabled.
Administrative Port Speed	The speed requested by the user.

Table 3-22. Port Information Data Window Entries (Continued)

Entry	Description
Operational Port Speed	The speed actually being used by the port.
Max Credits	The maximum number of credits granted to a port that can be used when extending port credits.
Device Scan	Device scan status. Enabled means the switch module queries the connected device during login for FC-4 descriptor information.
Symbolic Name	Port symbolic name
Ext Credits Requested	Number of requested credits
Credits to Donate	The number of credits available to be donated by the selected port.
Donor Group	The donor group of the selected port.
Valid Donor Groups	The number of separate groups within which extended credits may be donated and assigned.
Media	The transceiver type.
Media Speed	The maximum transceiver speed
Media Type	The transceiver fibre type, such as single mode, multi-mode, copper.
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

3.7.2 Configuring Ports

Note: For external ports (0, 15, 16, 17, 18, 19), all port parameters apply. For internal ports, only the port state setting is configurable.

The external Fibre Channel ports are self-configuring GL_Ports that auto-negotiate transmission speeds of 1 Gbps or 2 Gbps depending on the connected device. A GL_Port connects to a loop of public devices or a single device and configures itself as a fabric loop port (FL_Port), fabric port (F_Port), or an expansion port (E_Port). Each external port has 16 buffer credits. This enables a cable length up to 26 km at 1-Gbps or 13 km at 2-Gbps. The buffer credit flow control mechanism provides a way to ensure full use of the media, regardless of length, by providing for frame streaming. With frame streaming, the sender can transmit as many frames as there are credits without having to wait for a response to one frame before transmitting the next frame. The media can then be continuously in use at its rated capacity.

The external port (0, 15, 16, 17, 18, 19) settings or characteristics are configured using the Port Properties window shown in [Figure 3-33](#). To open the Port Properties window, select one or more ports, open the Port menu and select **Port Properties**.

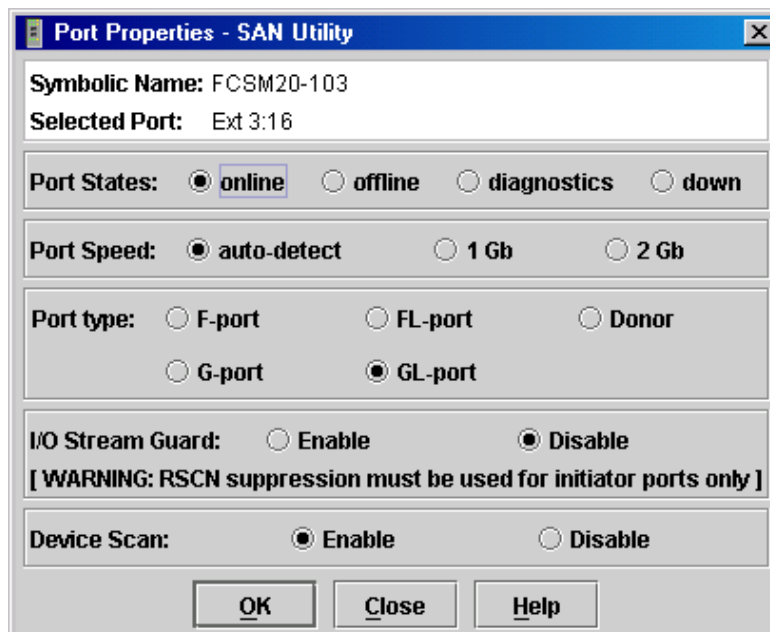


Figure 3-33. External Port Properties Window

The Port Properties window displays the switch module name and the selected external ports. Use the Port Properties window to perform the following tasks:

- [Changing Port Administrative States](#)
- [Changing Port Speeds \(External Ports Only\)](#)
- [Changing Port Types \(External Ports Only\)](#)
- [Changing I/O Stream Guard \(External Ports Only\)](#)
- [Changing Device Scan \(External Ports Only\)](#)
- [Changing Port Symbolic Name \(External Ports Only\)](#)

Internal port (1 through 14) configuration is limited to the port state as shown in [Figure 3-34](#). To open the Port Properties window, select one or more internal ports open the Port menu and select **Port Properties**.

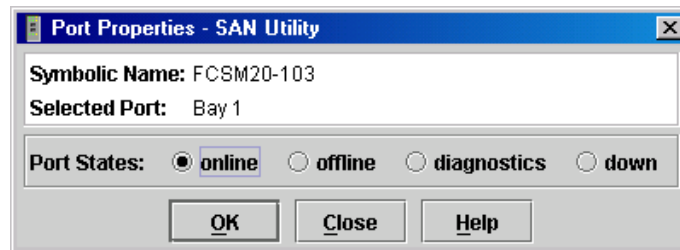


Figure 3-34. Internal Properties Window

3.7.2.1

Changing Port Administrative States

The Port Administrative state determines the internal and external port operational state. The port operational state refers to the state actually used by the port. The port administrative state refers to the requested state in SAN Utility or through a Telnet command. The port 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 module configuration and is preserved across switch module resets. SAN Utility 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 module resets. The current administrative state is set using the Set Port command. Refer to the "[Set Port Command](#)" on page 2-50.

[Table 3-23](#) describes the port administrative states. To change port administrative state, do the following:

1. Select one or more ports in the Faceplate window.
2. Open the Port menu and select **Port Properties** to open the Port Properties window.
3. Click the **Port States** radio button that corresponds to the port state you want.
4. Click the **OK** button to write the new port state to the switch module.

Table 3-23. Port Administrative States

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

3.7.2.2

Changing Port Speeds (External Ports Only)

The switch module external ports (0, 15, 16, 17, 18, 19) are capable of transmitting and receiving at 1- 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 3-24](#) describes the port speeds. To change the port speed, do the following:

1. Select one or more ports in the Faceplate window.
2. Open the Port menu and select **Port Properties**.
3. Click the radio button that corresponds to the port speed you want.
4. Click the **OK** button to write the new port speed to the switch module.

Table 3-24. Port Speeds

State	Description
Auto-Detect	Matches the transmission speed of the connected device. This is the default.
1 Gbps	Sets the transmission speed to 1-Gbps.
2 Gbps	Sets the transmission speed to 2-Gbps.

3.7.2.3

Changing Port Types (External Ports Only)

The switch module external ports (0, 15, 16, 17, 18, 19) can be configured to self-discover the proper type to match the device or switch module to which it is connected. Internal ports (1 through 14) are fixed as F_Ports. [Table 3-25](#) describes the port types.

To change the port type, do the following:

1. Select one or more ports in the Faceplate window.
2. Open the Port menu and select **Port Properties** to open the Port Properties window.
3. Click the **Port Type** radio button for the port type you want.
4. Click the **OK** button to write the new port type to the switch module.

Table 3-25. 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.
Donor	Donor port - Allows buffer credits to be used by another port.

3.7.2.4

Changing I/O Stream Guard (External Ports Only)

The I/O Stream Guard feature suppresses the generation of Registered State Change Notification (RSCN) messages on external ports (0, 15, 16, 17, 18, 19). I/O Stream Guard should be enabled only on ports connected to initiator devices. To change the generation of RSCN messages, do the following:

1. Select one or more ports in the Faceplate window.
2. Open the Port menu, and select **Port Properties** to open the Port Properties window.
3. Click the radio button (**Enable** or **Disable**) in the I/O Stream Guard area of the Port Properties window.
4. Click the **OK** button to write the change to the switch module.

3.7.2.5

Changing Device Scan (External Ports Only)

The Device Scan feature queries the connected device during login for FC-4 descriptor information on external ports (0, 15, 16, 17, 18, 19). Disable this parameter only if the scan creates a conflict with the connected device. To change the Device Scan feature, do the following:

1. Select one or more ports in the Faceplate window.
2. Open the Port menu, and select **Port Properties** to open the Port Properties window.
3. Click the radio button (**Enable** or **Disable**) in the Device Scan area of the Port Properties window.
4. Click the **OK** button to write the change to the switch module.

3.7.2.6

Changing Port Symbolic Name (External Ports Only)

To change the symbolic name of an external port (0, 15, 16, 17, 18, 19), do the following:

1. Open the Faceplate window and select a port.
2. Open the Port menu and select **Port Symbolic Name**.
3. In the Port Symbolic Name window, choose one of the following:
 - Enter a new name for the port in the Set Port Symbolic Name field.
 - Check the **Restore Default Port Symbolic Name** check box to restore the default name.
4. Click the **OK** button.

3.7.3

Resetting a Port

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

1. In the Faceplate window, select one or more ports to be reset.
2. Open the Port menu and select **Reset Port**.

To run an internal, external, or online port loopback test on an external port, see ["Testing Ports" on page 4-3](#).

Notes

Section 4

Switch Module Utility Functions

This chapter contains information about the following topics:

- LED diagnostics
- Port testing
- Fibre Channel switch module monitoring using SNMP
- Using the SAN Utility Performance View application

4.1

LED Diagnostics

The QLogic 6-Port Enterprise Fibre Channel Switch Module performs a POST as part of its power-on procedure. The POST diagnostic program performs the following tests:

- Checksum tests on the boot firmware in PROM and the fibre channel switch module firmware in flash memory
- Internal data loopback test on all ports
- Access and integrity test on the fibre channel switch module ASIC

During the POST, the switch module logs any errors encountered. Some POST errors are fatal; others are non-fatal. The fibre channel switch module uses the Switch Fault LED to indicate switch module and port status. A fatal error disables the fibre channel switch module so that it will not operate. If a non-fatal error occurs, the switch module can still operate, but disables the ports that have errors. Regardless of whether the problem is fatal or nonfatal, contact your authorized maintenance provider.

If a fatal error occurs, the Switch Fault LED illuminates. If there are non-fatal errors, the switch module disables the failed ports and illuminates the corresponding Port Fault LEDs.

There are seven sets of LEDs on the information panel. The first row of LEDs at the top of the fibre channel switch module represent switch-module status. These are the Power On and Switch Fault LEDs. The second through seventh sets of LEDs represent status for the external Fibre Channel ports 0, 16, 16, 17, 18, and 19. The port LEDs include the Port Logged-In, Port Activity, and Port Fault.

Figure 4-1 shows the location of these LEDs on the switch module. For more information about switch module LEDs, see the *QLogic 6-Port Enterprise Fibre Channel Switch Module for IBM Eserver BladeCenter Installation Guide*.

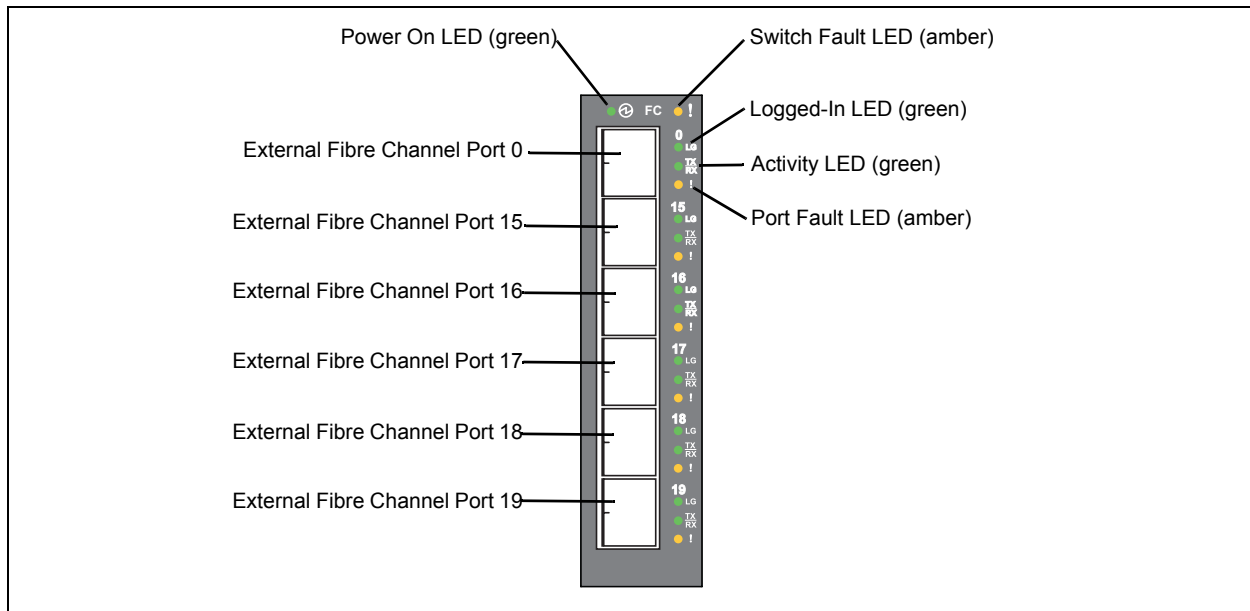


Figure 4-1. Switch Module LEDs

4.2 Testing Ports

The port loopback tests verify correct external port operation by sending a test data frame out through the loop and then verifying that the frame received matches the frame that was sent. You can perform the following port test:

- **Internal SerDes Test (external ports only)** - The SerDes (serializer/deserializer) level test verifies internal and external 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.
- **External SFP test (external ports only)** - 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 a loopback plug, and back to the ASIC for the selected external ports. The external 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.
- **Online Node-to-Node (external ports only)** - The Node-to-Node test verifies communications between the external 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 does not disrupt communication on the selected port. This test requires that the port be online, and therefore, does not disrupt communication.

Note: The internal SerDes and external SFP level tests disrupt communication on the selected port. The online node-to-node level test does not disrupt communication, because it requires that the port is online.

To run the internal, external, or online port loopback test on an external port, do the following:

1. In the Faceplate window, select the port to be tested.
2. Open the Port menu and select **Port Loopback Test** to open the Port Loopback Test window shown in [Figure 4-2](#).

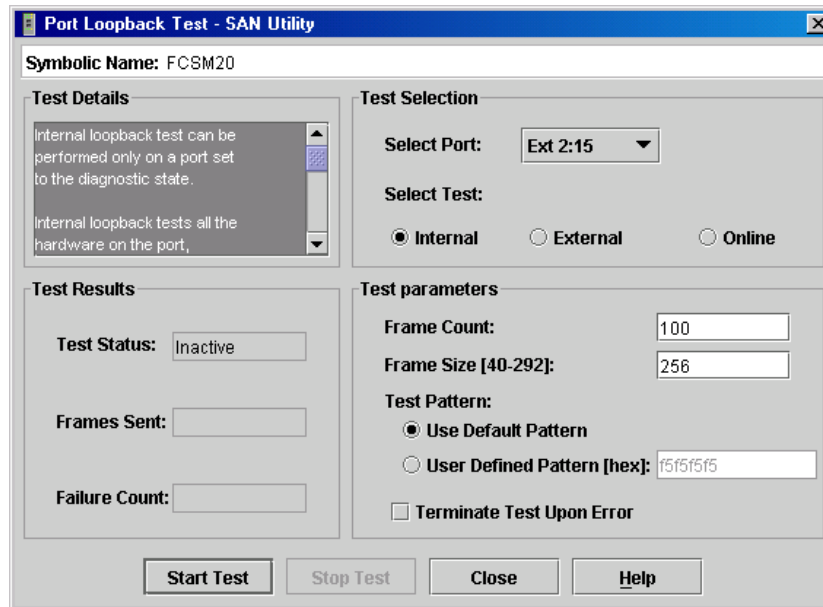


Figure 4-2. Port Loopback Test Window

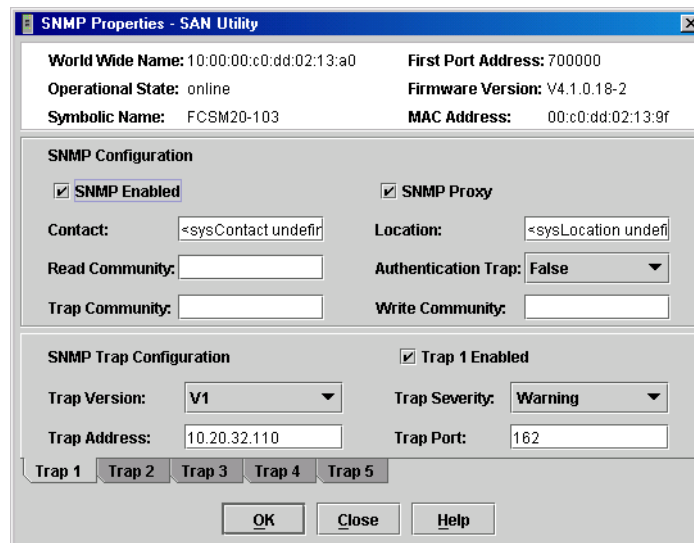
3. In the Test Selection area, click the radio button for the type of loopback test to be run (**Internal**, **External**, or **Online**). If you choose the internal or external test, SAN Utility will prompt you to confirm that the port state needs to be changed to the diagnostic state. Click the **OK** button and SAN Utility will change the port state.
4. Enter the frame count, frame size, and click a test pattern radio button. You may use the default pattern or enter an 8-digit pattern (hex). For online test, you can check the **Terminate Test Upon Error** check box if you want the test to stop should it encounter an error.
5. Click the **Start Test** button 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 pull-down menu and select another port (number) and test type (**Internal**, **External**, or **Online**) in the Test Selection area.
7. Click the **Start Test** button to begin the next test. Observe the results in the Test Results area.

4.3 Switch Module Monitoring Using SNMP

This section describes SNMP configuration and trap parameters. The switch module SNMP agent enables external network management monitoring and notification of switch module status.

Use the SNMP Properties window shown in [Figure 4-3](#) to change SNMP parameters. Enter new values and click the **OK** button to implement the changes. To open the SNMP Properties window, select a switch module in the Topology window or open the Faceplate window. Open the Switch menu and select **SNMP Properties**.

Note: The Read Community, Trap Community, and Write Community are write-only password fields. The current values are not displayed.



SNMP Properties - SAN Utility

World Wide Name: 10:00:00:c0:dd:02:13:a0 First Port Address: 700000
Operational State: online Firmware Version: V4.1.0.18-2
Symbolic Name: FCSM20-103 MAC Address: 00:c0:dd:02:13:9f

SNMP Configuration

SNMP Enabled SNMP Proxy

Contact: <sysContact undefir Location: <sysLocation undefi

Read Community: Authentication Trap: False

Trap Community: Write Community:

SNMP Trap Configuration

Trap 1 Enabled

Trap Version: V1 Trap Severity: Warning

Trap Address: 10.20.32.110 Trap Port: 162

Trap 1 Trap 2 Trap 3 Trap 4 Trap 5

OK Close Help

Figure 4-3. SNMP Properties Window

4.3.1

SNMP Configuration

The SNMP configuration defines how authentication traps are managed. [Table 4-1](#) describes the SNMP configuration parameters. The illegal characters for the user-defined fields are the pound sign (#), semi-colon (;), and comma (,).

Table 4-1. SNMP Configuration Parameters

Parameter	Description
SNMP Enabled	Enables or disables SNMP communication with other switches in the fabric.
SNMP Proxy	Enables or disables the SNMP proxy for the fabric. If enabled, you can use SNMP to monitor and configure any switch module in the fabric.
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 module. 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 module and the SNMP management server must be the same. The default is "public".
Location	Specifies the name (up to 64 characters) for the switch module 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 agent to write information to the switch module. This is a write-only field. The value on the switch and the SNMP management server must be the same. The default is "private".

4.3.2

SNMP Trap Configuration

The SNMP trap configuration defines how traps are set. Choose from the tabs **Trap1 – Trap 5** to configure each trap. [Table 4-2](#) describes the SNMP configuration parameters.

Table 4-2. 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 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 pull-down menu and choose a level. The Trap 1 Enabled check box on the SNMP Properties dialog must be enabled to access this pull-down menu. 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.

4.4 Using the SAN Utility Performance View Application

SAN Utility Performance View application displays port performance using graphs. SAN Utility Performance View plots data communication rates and total errors for selected ports as shown in Figure 4-4. When graphing data communication rates, you can choose either frames/second or KB/second.

Fabric status is displayed in text format after the fabric name in the fabric tree. The color of the icon indicates the current connection status as normal (green), warning (yellow), critical (red), or unmanageable (blue).

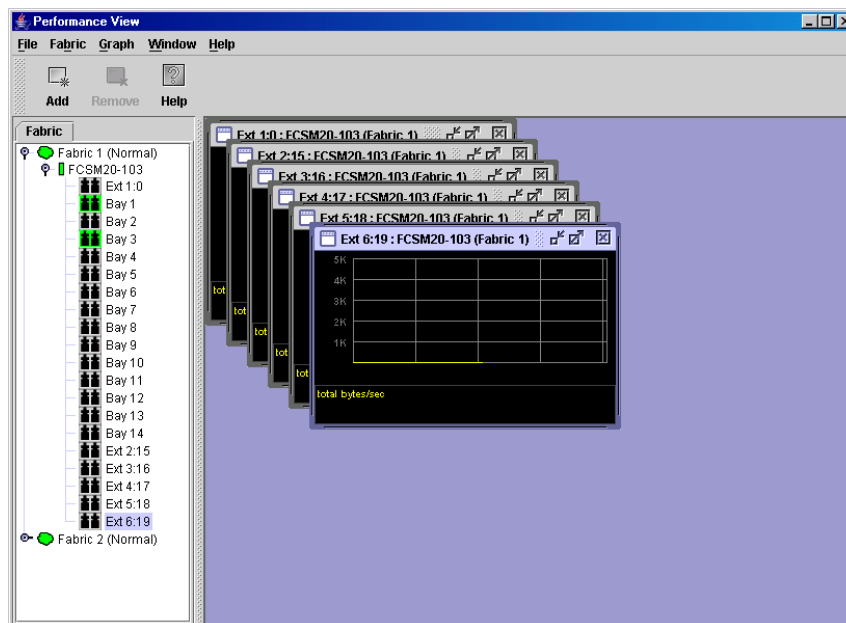


Figure 4-4. Fabric View Graphs

This section describes how to do the following:

- Start and exit SAN Utility Performance View
- Save and open default performance view files
- Change the encryption key for the default performance view file
- Set SAN Utility Performance View preferences
- Set the polling frequency
- Display graphs
- Print graphs
- Rescale a selected graph
- Save graph statistics to a file

4.4.1

Starting SAN Utility Performance View

To start SAN Utility Performance View from within SAN Utility, open the Topology window and select **Start Performance Viewer** from the Fabric menu. Open the fabric in the SAN Utility Performance View Topology window.

4.4.2

Exiting SAN Utility Performance View

To exit a SAN Utility Performance View session, open the File menu and select **Exit**. The current fabric view is automatically saved to your default performance view file upon exit, if you have defined an encryption key. The key is encrypted and saved with your default performance view file. A performance view file contains the set of fabrics that have been added and the graphs that have been opened during a SAN Utility Performance View session. If you have not yet defined an encryption key, the Save Default Performance View File dialog, shown in [Figure 4-5](#), prompts you to save the current performance view file as the default performance view file. Refer to ["Changing the Default Performance View File Encryption Key" on page 4-11](#) for information about defining and changing this encryption key.

In the Save Default Performance View File dialog, enter an encryption key in the Default Performance File Encryption Key field. Re-enter the encryption key in the Re-enter Encryption Key to Confirm field. Click the **OK** button to save the current set of fabrics to the default performance view file in the working directory.

To prevent SAN Utility Performance View from prompting you to save the default performance view file between sessions, set the Auto Load and Save Graphing Environment setting to Enable (default). Refer to ["Setting SAN Utility Performance View Preferences" on page 4-11](#) for more information.



Figure 4-5. Save Default Performance View File Dialog

In your next SAN Utility Performance View session, the Load Default View File dialog shown in [Figure 4-6](#) prompts you to load the default performance view file and to specify its encryption key, if there is one. In the Default Fabric File Encryption Key field, enter the encryption key and click the **Load View File** button. If you do not want to load the default performance view file, click the **Continue Without Loading** button to open the SAN Utility Performance View with no fabric displayed.

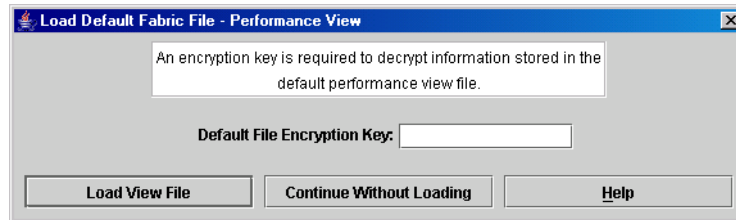


Figure 4-6. Load Default View File Dialog

4.4.3

Saving and Opening Performance View Files

In addition to the default performance view file, you can save and open your own performance view files. The performance view file contains the set of fabrics, graphs, and graphing options. To save a performance view file, do the following:

1. Open the File menu and select **Save View As** to open the Save View dialog.
2. Enter a name for the fabric file or click the **Browse** button to select an existing file. Files are saved in the working directory.
3. Enter a password. When you attempt to open this fabric file, you will be prompted for this password. If you leave the File Password field blank, no password is required.

To open a performance view file, do the following:

1. Open the File menu and select **Open View File** to open the Open View dialog.
2. Enter a name for the fabric file or click the **Browse** button to select an existing file.

4.4.4

Changing the Default Performance View File Encryption Key

To change the encryption key for the default performance view file, do the following:

1. Open the File menu and select **Save Default Performance View File** to open the Save Default Performance View File dialog.
2. Enter the new encryption key in the Default File Encryption Key field.
3. Re-enter the same encryption key in the Re-enter Encryption Key to Confirm field.
4. Click the **OK** button to save the changes.

4.4.5

Setting SAN Utility Performance View Preferences

To set preferences, open the File menu and select **Preferences** to open the Preferences dialog shown in [Figure 4-7](#). Set the following preferences and click the **OK** button to save the changes:

- Change the location of the working directory in which to save files
- Change the location of the browser used to view the online help.
- Enable or disable the **Auto Load and Auto Save Graphing Options** preference. When enabled, SAN Utility Performance View prompts you to save and load the default fabric file between sessions. Refer to ["Exiting SAN Utility Performance View" on page 4-9](#) for more information on the default performance view file.

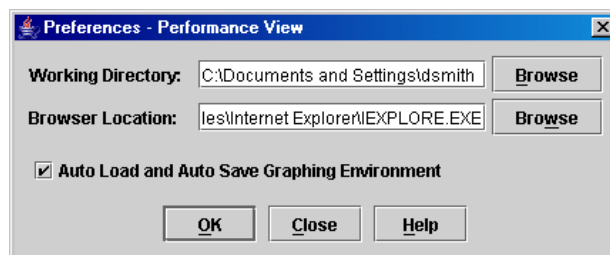


Figure 4-7. Preferences – SAN Utility Performance View

4.4.5.1

Setting the Polling Frequency

SAN Utility Performance View updates the graphs once per second by default. To change this polling frequency, do the following:

1. Open the Graph menu, and select **Set Polling Frequency** to open the Set Graph Polling Frequency dialog.
2. Enter the new polling interval in seconds [1–60]. Performance Viewer will update the graphs once during the interval. For example, setting the polling frequency to 5 seconds will return 1 second's worth of data every 5 seconds.
3. Click the **OK** button to save the changes.

4.4.5.2

Displaying Graphs

To display graphs, do the following:

1. Open the Fabric menu and select **Add Fabric** or click the **Add** button. Enter a fabric name and an IP address in the Add a New Fabric dialog. Include an account name and a password if required.
2. Set the graphing options and polling frequency. By default, SAN Utility Performance View plots total bytes transmitted and received at a polling frequency of once per second. Refer to ["Customizing Graphs" on page 4-13](#) for information about changing what is plotted and how it is plotted.
3. You can display graphs in the following ways:
 - Click on a switch entry handle and select one or more ports.
 - Right click on a switch icon in the fabric tree and select **Open Graph for All Ports on Switch** or **Open Graph for All Logged-In Ports on Switch** from the pull-down menu.
4. You can move graphs around individually by clicking and dragging, or you can arrange them as a group. Refer to ["Arranging Graphs in the Display" on page 4-13](#) for more information.

To remove a graph, click the graph **Remove** button. To remove all graphs, open the Window menu and select **Close All**.

To remove a fabric and its graphs, select the fabric in the fabric tree, then select **Remove Fabric** from the Fabric menu. You can also right click on a fabric and select **Remove Fabric** for the popup menu.

Right clicking on a graph opens a popup menu from which you can change graph options, print a graph, or save the graph statistics to a file.

4.4.5.2.1

Arranging Graphs in the Display

To arrange and size graphs in the display, open the Window menu and select **Cascade**, **Tile**, or **Close All**.

- **Cascade** overlaps the graphs so that all graphs are at least partially visible.
- **Tile** arranges the graphs in non-overlapping rows and columns.
- **Close All** closes all graphs.

You can also click a graph on the Window menu to bring that graph to the front.

4.4.5.2.2

Customizing Graphs

You can customize the graph polling frequency, what is plotted in the graphs, and the graph color scheme. To set the polling frequency for all graphs, open the Graph menu and select **Set Polling Frequency....** Enter an interval in seconds (0–60) in the dialog box and click the **OK** button.

To choose what is to be plotted, open the Graph menu and select **Modify Graph Options....** You can also right click on a graph and select **Change Graph Options**. This opens the Default Graph Options dialog shown in [Figure 4-8](#).

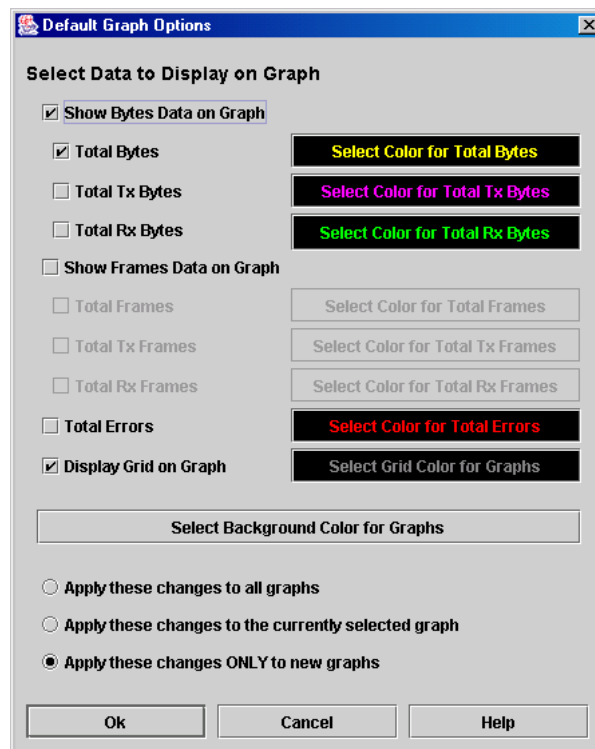


Figure 4-8. Default Graph Options Dialog

To modify the graph options, do the following:

1. Choose the units for the graph:
 - Select the **Show Bytes Data on Graph** check box to plot data in KBytes/second
 - Select the **Show Frames Data on Graph** check box to plot data in frames/second.
2. Choose what data type to plot. For example, if you selected **Show Frames Data on Graph** in [step 1](#), you can plot one or all of the following:
 - Total frames transmitted and received (**Total Frames**)
 - Total frames transmitted (**Total Tx Frames**)
 - Total frames received (**Total Rx Frames**)In addition to these, you can also plot total errors by selecting the **Total Errors** check box.
3. Display or hide the unit grid. Select the **Display Grid on Graph** check box to display the unit grid.
4. Choose the color scheme for the graph. Click a **Select Color** button to open its corresponding Select Color dialog, which allows you to select a new color scheme. You can select the color for each data type, the unit grid, and the background by clicking the corresponding color field or button. In each case, you can choose a color using the Swatches, Red-Green-Blue (RGB), or Hue-Saturation-Brightness (HSB) method.

Note: Clicking the **Reset** button in the Swatches, HSB, and RGB tab pages of the Select Color dialogs will reset the colors in the Preview area to the last saved color scheme. At this point you are only selecting a new color scheme to be saved.

- Swatches – Click the **Swatches** tab. Select a swatch from the palette.
 - HSB – Click the **HSB** tab. Select a color by one of these methods:
 - Click in the color palette.
 - Select the **H**, **S**, or **B** button and use the slide to vary the value.
 - Enter values in the H, S, or B input fields.
 - RGB – Click the **RGB** tab. Select a color by moving the slides to adjust the values for red, blue, and green; or enter values in the input fields.
5. In the Default Graph Options dialog, click the corresponding radio button to apply changes to all graphs, the currently selected graph, or all new graphs.
 6. In the Default Graph Options dialog, click the **OK** button to save the color scheme changes and close the dialog.

4.4.5.2.3

Rescaling a Selected Graph

The Rescale Selected Graph option auto-scales downward and re-positions the data within a graphic window to display all new data captured by the graph. To rescale a selected graph, do the following:

1. Select a displayed graph.
2. Open the Graph menu and select **Rescale Selected Graph**, or right-click on the graph and select **Rescale** from the popup menu.
3. View the data in the graph window.

4.4.6

Printing Graphs

To print a graph, select a graph, then open the File menu and select **Print Graph Window**. You can also right click on a graph and select **Print Graph Window** from the popup menu.

4.4.7

Saving Graph Statistics to a File

Statistics for one or all graphs can be saved to a file that can be opened with a spreadsheet application. To save a graph statistics file, do the following:

1. Select a graph.
2. Open the File menu, and select **Save Current Graph Statistics to a File** to save the selected graph or select **Save All Graph Statistics to a File**. You can also right click on a graph and select **Save Statistics to File**.
3. In the Save dialog, enter a path name for the file. By default, the file is saved in the working directory.
4. Click the **Save** button.

Notes

Appendix A

Mapping Port Locations and Software Numbering

Your switch module has six external Fibre Channel ports (external Fibre Channel ports 0, 15, 16, 17, 18, and 19) and 14 internal Fibre Channel ports that connect to each of the 14 blade server bays (ports 1 to 14). The SAN Utility and CLI for the switch module require port numbering from 0 to 19. The SNMP monitoring agent for the switch module numbers the ports from 1 to 20.

A.1 Port Mapping

[Table A-1](#) shows the mapping of switch module port numbering for the BladeCenter and BladeCenter T configurations and whether these ports have the capability to be configured.

Table A-1. Port Mapping For Server Units

Switch Module Physical Port Connection	SAN Utility and Cli Logical Port Number	SNMP Port Numbering	Configurable
External port 1	0 Ext(1:0 ¹)	1	Yes
Server bay 1	1	2	No
Server bay 2	2	3	No
Server bay 3	3	4	No
Server bay 4	4	5	No
Server bay 5	5	6	No
Server bay 6	6	7	No
Server bay 7	7	8	No
Server bay 8	8	9	No
Server bay 9 ²	9	10	No
Server bay 10 ²	10	11	No
Server bay 11 ²	11	12	No
Server bay 12 ²	12	13	No
Server bay 13 ²	13	14	No
Server bay 14 ²	14	15	No

Table A-1. Port Mapping For Server Units (Continued)

Switch Module Physical Port Connection	SAN Utility and Cli Logical Port Number	SNMP Port Numbering	Configurable
External port 2	15 Ext(2:15 ¹)	16	Yes
External port 3	16 Ext(3:16 ¹)	17	Yes
External port 4	17 Ext(4:17 ¹)	18	Yes
External port 5	18 Ext(5:18 ¹)	19	Yes
External port 6	19 Ext(6:19 ¹)	20	Yes

¹ Indicates a symbolic port name if it is different from the logical port number.

² Bays 9 through 14 are not used for the BladeCenter T units.

Note: The Fibre Channel ports that connect to each of the server bays (1 through 14) are fixed 2-Gbps F_Port configurations. Only the administrative state for these ports can be changed.

Index

A

- access control list zone 3-42, 3-56
- account name
 - description 3-26
 - display 2-92
- active
 - firmware 3-91
 - zone set 3-36, 3-43, 3-82
- Active Zoneset data window 3-36
- Activity LED 3-67
- Admin
 - account name 2-7
 - authority 2-7, 3-22
- Admin command 2-8
- administrative state
 - configured 3-79, 3-104
 - current 3-79, 3-104
 - port 2-50, 3-104
 - switch 2-34, 3-79
- alarm
 - configuration 2-41, 3-73
 - configuration display 2-71
 - log 2-33, 2-58
- alias
 - add members 2-9, 3-57
 - copy 2-9
 - create 2-9, 3-57
 - delete 2-9
 - delete members 2-10
 - description 3-42
 - display list 2-10
 - display members 2-10
 - remove 3-58
 - rename 2-10
- Alias command 2-9
- Arbitrated Loop Physical Address 2-50
- archive configuration 3-86
- authentication
 - trap 4-6
 - user 2-54

- authority 2-7
- auto save
 - default fabric view file 3-19
 - graphing options 4-11
 - zoning configuration 3-48

B

- beacon 2-33
- broadcast 2-58, 3-82
- browser 3-1, 3-19, 4-11

C

- chassis status 2-58, 2-59
- command line interface (CLI) 2-1
- command syntax 2-6
- commands 2-7
- Config command 2-11
- configuration
 - activate 2-11
 - archive 3-86
 - backup 2-11
 - copy 2-11
 - delete 2-11
 - edit 2-11
 - list 2-11
 - reset 2-26
 - restore 2-12, 3-87
 - save 2-12
 - wizard 3-78
- configured administrative state 3-79
- contact 4-6
- CRC error 3-73
- current administrative state 3-79

D

- data window
 - Active Zoneset 3-36
 - Configured Zonesets 3-72
 - description 3-11, 3-15, 3-17
 - Devices 3-35, 3-68

- port information 3-101
- port statistics 3-97
- switch 3-68
- database
 - fabric 3-25
 - zoning 3-45
- date 3-75
- Date command 2-13
- Decode error 3-73
- default
 - configuration 3-89
 - user account 3-22
 - visibility 3-49, 3-51
 - zoning 3-50
- default fabric view file
 - auto save 3-19
 - SAN Utility 3-19
- device information
 - export to file 3-38
 - scan 3-107
- device port nickname
 - create 3-38
 - delete 3-39
 - description 3-38
 - edit 3-39
 - export to file 3-39
 - import 3-40
- Devices data window 3-35, 3-68
- disk space 3-1
- domain ID
 - description 3-80
 - display 2-59
 - lock 3-80
- donor port 2-59, 3-95, 3-106

E

- E_Port isolation 3-58, 3-80
- encryption key 4-11
- Error Detect Timeout 3-83
- event browser
 - display 3-31
 - filter 3-33
 - preference 3-19

- save to file 3-35
- sort 3-34
- event logging
 - by component 2-47, 2-75
 - by port 2-48, 2-76
 - by severity level 2-76
 - display 2-75
 - restore defaults 2-48
 - save settings 2-48
 - settings 2-76
 - severity level 2-48, 3-32
 - start 2-48
 - stop 2-49
- external test 2-85, 4-3

F

- F_Port 3-95, 3-106
- fabric
 - add 3-25
 - add a switch 3-27
 - database 3-25
 - delete 3-26
 - discovery interval 3-19
 - displaying information 3-29
 - loop port 3-95, 3-106
 - management 3-21
 - management workstation 3-1
 - merge 3-58
 - port 3-95, 3-106
 - rediscovery 3-26
 - security 3-21
 - services 3-22
 - status 3-29
 - tree 3-10
 - zoning 3-40
- Fabric Device Management Interface 2-59, 3-81
- fabric tracker 3-23
- fabric view file
 - open 3-18
 - save 3-18
- Faceplate window
 - data window 3-17
 - description 3-16

- menus 3-6
 - shortcut keys 3-8
- factory defaults 2-26, 3-89
- Fallback command 2-14
- Fault LED 3-67
- FC-4 descriptor 3-107
- FC-SW-2 compliance 3-82
- firmware
 - activate pending 3-92
 - active 3-91
 - change pending 3-92
 - fallback 3-92
 - image file 2-20, 3-91
 - inactive 3-91
 - install with SAN Utility 3-91
 - list image files 2-20
 - non-disruptive activation 2-18, 3-91
 - pending 2-14, 3-91
 - remove image files 2-20
 - retrieve image file 2-20
 - unpack image 2-20
 - version 2-66
- FL_Port 3-95, 3-106

G

- gateway address 3-85
- generic port 3-95, 3-106
- graphic window 3-11

H

- hard reset 3-77
- Hardreset command 2-15
- hardware status 3-67
- help 3-1
- Help command 2-16
- History command 2-17
- host bus adapter 2-59
- hot reset 3-77
- Hotreset command 2-18

I

- I/O Steam Guard 3-106
- Image command 2-20

- inactive firmware 3-91
- in-band management 3-82
- Initial Start Dialog 3-19
- internal test 2-85, 4-3
- internet browser 3-1
- IP
 - address 3-85
 - configuration 3-85
- ISL monitoring 3-73

L

- layout 3-14
- legacy address format 3-83
- link
 - delete 3-28
 - selecting 3-14
 - status 3-13
- link control frame preference routing 2-37
- Link data window 3-71
- link state database 2-59
- Lip command 2-21
- log
 - archive 2-47
 - clear 2-47
 - event 2-47, 2-75
 - power-on self test 2-63
- logged in users 2-66
- Logged-In LED 3-67
- login limit 2-2, 3-22
- loop port
 - bypass 2-50
 - enable 2-50
 - fabric 3-95, 3-106
 - initialization 2-21
- loopback test 4-3
- loss of signal monitoring 3-73

M

- management workstation 3-2
- manufacturer information 2-81
- media status 3-97
- memory
 - activity 2-59

workstation 3-1
menu structure 3-5
Multi-frame sequence bundling 2-37

N

name server
 display 2-60
 zone 3-42
network
 configuration reset 2-27
 discovery 3-85
 interfaces 2-59
 properties 3-84
Network Time Protocol
 client 2-54, 3-75
 server 2-55, 3-75
nickname
 create 3-38
 delete 3-39
 description 3-38
 edit 3-39
 export to file 3-39
 import 3-40
node-to-node test 4-3
non-disruptive activation 2-18, 3-92

O

online
 help 3-1
 test 2-85, 4-3
operating systems 3-1
orphan zone set 3-43

P

page break 2-34
Passwd command 2-22
password
 change 2-22
 default fabric view file 3-19
 switch 2-22, 3-26
 user account 3-64
pending firmware 3-91, 3-92
performance

graphs 4-12
 tuning 2-37
Performance View 3-2
performance view file
 auto save 4-11
 encryption key 4-9, 4-11
 open 4-10
 save 4-10
Ping command 2-23
port
 Activity LED 3-67
 administrative state 2-50, 3-104
 configuration 2-35, 3-103
 configuration display 2-71
 counters 2-50
 displaying information 3-93
 external test 2-85
 Fault LED 3-67
 initialize 2-26
 internal test 2-85
 Logged-In LED 3-67
 loopback test 2-85
 mode 3-95
 online test 2-85
 operational information 2-60
 operational state 3-96
 performance 4-8
 performance statistics 2-60, 2-78
 performance tuning 2-37
 reset 3-107
 selecting 3-17
 speed 2-50, 3-96, 3-105
 status 3-16
 symbolic name 3-107
 test 4-3
 view 3-16, 3-20
Port Information data window 3-72, 3-101
Port Statistics data window 3-71, 3-97
port/device tree 3-46
Power On LED 3-67
power on self test 2-63
preferences
 SAN Utility 3-19
 SAN Utility Performance View 4-11

principal switch 3-80
processor 3-1
properties
 network 3-84
 port 3-104
 SNMP 4-5
 switch 3-78
Ps command 2-24

Q

Quit command 2-25

R

read community 4-6
refresh 3-29, 3-66
Registered State Control Notification 3-106
remote logging 3-85, 3-86
reset
 with POST 3-77
 without POST 3-77
Reset command 2-26
Resource Allocation Timeout 3-83
restore configuration 3-87

S

SAN Browser
 description 3-2
 enable 2-55
 status 3-71
SAN Utility
 description 3-1
 Performance View 3-2
 preferences 3-19, 4-11
 SAN Browser 2-55
SAN Utility Performance View
 arrange graphs 4-13
 customize graphs 4-13
 display graphs 4-12
 preferences 4-11
 print a graph 4-15
 rescale a graph 4-15
 save graph to a file 4-15
 start 4-9

scan device 3-107
security 3-21
SerDes level test 4-3
Set command 2-33
Set Config command 2-35
Set Log command 2-47
Set Port command 2-50
Set Setup command 2-52
severity levels 3-32
SFP level test 4-3
shortcut keys 3-7, 3-8
Show command 2-58
Show Config command 2-71
Show Log command 2-75
Show Perf command 2-78
Show Setup command 2-81
Shutdown command 2-84
Simple Network Management Protocol
 configuration 2-52, 4-6
 configuration display 2-81
 properties 4-5
 proxy 4-6
 reset 2-26
 trap configuration 4-7
snapshot
 comparison 3-24
 export to a file 3-24
 save 3-23
SNMP enabled 4-6
soft zone 3-42, 3-56
status icon color 3-10
steering 2-63
subnet mask address 3-85
switch
 add 3-27
 administrative state 2-34, 3-79
 configuration 2-38, 3-77
 configuration display 2-71
 delete 3-28
 displaying information 3-66
 Fault LED 3-67
 hard reset 2-15, 3-77
 hot reset 3-77
 icons 3-29

- location 4-6
- manufacturer information 2-81
- operational information 2-64
- paging 3-74
- properties 3-79
- replace 3-28
- reset 2-88, 3-76
- reset without POST 2-26, 3-77
- restore factory defaults 3-89
- selecting 3-14
- status 3-13
- symbolic name 3-79
- Switch data window 3-68
- Switch Fault LED 3-67
- symbolic name
 - port 3-107
 - switch 3-79
- syslog 3-85, 3-86
- system configuration
 - change 2-53
 - display 2-81

T

- Telnet interface 2-1
- temperature threshold 3-75
- Test command 2-85
- testing ports 4-3
- time
 - set or display 2-13
 - synchronization 2-54, 3-75
- timeout values 3-83
- tool bar
 - standard 3-9
 - zoning 3-46
- Topology window
 - arrange icons 3-14
 - data windows 3-15
 - menus 3-5
 - shortcut keys 3-7
 - usage 3-12
- transceiver status 3-97
- transmission speed 3-105
- trap

- authentication 4-6
- community 4-6
- configuration 4-7
- SNMP version 4-7

U

- Uptime command 2-88
- user
 - authentication 2-54
 - logged in 2-66
- user account
 - create 3-62
 - default 3-61
 - modify 3-65
 - password 3-64
 - remove 3-63
 - security 3-21
- User command 2-89

V

- version snapshot 3-23
- Virtual interface preference routing 2-37

W

- web server 3-2
- Whoami command 2-92
- wizard zoning 3-2
- working
 - directory 3-19, 4-11
 - status indicator 3-11
- workstation 3-1
- write community 4-6

Z

- zone
 - access control list 3-42
 - add member port 2-93, 3-54
 - copy 2-93, 3-52
 - create 2-93, 3-53
 - definition 3-41
 - delete 2-93
 - delete member port 2-94
 - list 2-94

- list members 2-94
- name server 3-42
- remove 3-52, 3-55
- remove all 3-56
- remove member port 3-55
- rename 2-94, 3-55
- soft 3-42
- type 2-94, 3-56
- Zone command 2-93
- zone merge
 - description 3-58
 - failure 3-58
 - failure recovery 3-59
- zone set
 - activate 2-97, 3-51
 - active 2-99, 3-36, 3-43
 - add member zone 2-97
 - copy 2-97
 - create 2-97, 3-51
 - deactivate 2-27, 2-97, 3-51
 - definition 3-43
 - delete 2-97
 - delete member zone 2-98, 3-52
 - display 2-98
 - display active 2-97
 - display members 2-98
 - display zones 2-94
 - management 3-50
 - orphan 3-43
 - remove 3-52
 - rename 2-98, 3-55
 - tree 3-46
- Zoneset command 2-97
- zoning
 - configuration 2-42, 3-48
 - configuration display 2-71
 - database 2-27, 3-43, 3-45, 3-82
 - default 3-50
 - edit 2-99
 - history 2-99
 - limits 2-100
 - list definitions 2-100
 - remove all 3-50
 - revert changes 2-100
 - save edits 2-100
 - wizard 3-44
- Zoning command 2-99
- zoning wizard 3-2



Notes