



Networking the world's business data™

McDATA PRODUCTS

McDATA® 6-Port
Fibre Channel Switch Module
for IBM® eServer™ BladeCenter™
Management Guide

P/N 59143-00
REV A

Simplifying Storage Network Management

McDATA Corporation
380 Interlocken Crescent Broomfield, CO 80021-3464
Corporate Headquarters: 800-545-5773
Sales E-mail: sales@mcddata.com Web: www.mcddata.com

Record of Revisions and Updates

Revision	Date	Description
59143-00 A	5/2005	Initial release of manual.

Copyright © 2005 McDATA Corporation. All rights reserved.

Printed May 2005

First Edition

No part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written consent of McDATA Corporation.

The information contained in this document is subject to change without notice. McDATA Corporation assumes no responsibility for any errors that may appear.

All computer software programs, including but not limited to microcode, described in this document are furnished under a license, and may be used or copied only in accordance with the terms of such license.

McDATA either owns or has the right to license the computer software programs described in this document.

McDATA Corporation retains all rights, title and interest in the computer software programs.

McDATA Corporation makes no warranties, expressed or implied, by operation of law or otherwise, relating to this document, the products or the computer software programs described herein. McDATA CORPORATION DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. In no event shall McDATA Corporation be liable for (a) incidental, indirect, special, or consequential damages or (b) any damages whatsoever resulting from the loss of use, data or profits, arising out of this document, even if advised of the possibility of such damages.

©2004 McDATA Corporation. All rights reserved. McDATA, the McDATA logo, McDATA Eclipse, Fabriccenter, HotCAT, Intrepid, Multi-Capable Storage Network Solutions, Networking the World's Business Data, nScale, nView, OPENready, SANavigator, SANpilot, SANtegrity, SANvergence, SecureConnect and Sphereon are trademarks or registered trademarks of McDATA Corporation. OEM and Reseller logos are the property of such parties and are reprinted with limited use permission. All other trademarks are the property of their respective companies. All specifications subject to change.

Preface	xiii
License Agreement for McDATA Applications	xiv
Technical Support.....	xvi
Chapter 1 Command Line Interface (CLI)	
Logging On to a Switch Module	1-2
Working with Switch Module Configurations	1-2
Modifying a Switch Module Configuration	1-3
Backing up and Restoring Switch Module Configurations	1-4
Command Syntax	1-5
Admin Command	1-7
Alias Command.....	1-8
CIM Command	1-10
CIMListener Command.....	1-11
CIMSubscription Command.....	1-13
Config Command	1-15
Create Command.....	1-18
Date Command.....	1-21
Feature Command.....	1-22
Firmware Install Command.....	1-23
Group Command	1-24
Hardreset Command	1-31
Help Command	1-32
History Command.....	1-33
Hotreset Command.....	1-34
Image Command	1-36
Lip Command (for external ports only).....	1-39
Passwd Command	1-40
Ping Command	1-41
Ps Command	1-42
Quit Command	1-43
Reset Command	1-44
Security Command.....	1-52
Securityset Command.....	1-55
Set Command.....	1-57
Set Config Command.....	1-59
Set Log Command.....	1-69

Set Port Command	1-72
Set Setup Command.....	1-74
Show Command	1-83
Show Config Command	1-96
Show Log Command	1-99
Show Perf Command.....	1-102
Show Setup Command.....	1-105
Shutdown Command.....	1-108
Test Command	1-109
Uptime Command.....	1-112
User Command.....	1-113
Whoami Command.....	1-116
Zone Command	1-117
Zoneset Command	1-120
Zoning Command	1-122

Chapter 2 Using SANsurfer Switch Manager

Fabric Management Workstation	2-2
McDATA SANbrowser	2-3
SANsurfer Switch Manager User Interface	2-3
Menu Bars.....	2-6
Topology Window Menu	2-6
Faceplate Window Menu	2-7
Topology Window Shortcut Keys	2-7
Tool Bar	2-8
Fabric Tree	2-9
Graphic Window	2-10
Data Window and Tabs	2-10
Working Status Indicator.....	2-10
Using the Topology Window	2-11
Fibre Channel Switch Module and Link Status	2-11
Working with Switch Modules and Links.....	2-12
Using the Faceplate Window	2-13
Port Views and Status.....	2-14
Working with Ports.....	2-14
Faceplate Data Window Tabs	2-15
Configuring the SANsurfer Switch Manager Environment.....	2-16
Working with Fabric View Files	2-16
Saving a Fabric View File	2-16
Opening a Fabric View File.....	2-16
Changing the Encryption Key	2-16
Setting SANsurfer Switch Manager Preferences	2-17

Managing Fabrics	2-19
RADIUS Servers	2-19
Adding a RADIUS Server	2-20
Removing a RADIUS Server.....	2-21
Editing RADIUS Server Information	2-22
Modifying Authentication Order.....	2-23
Securing a Fabric	2-24
Connection Security	2-24
User Account Security.....	2-25
Security Consistency Checklist	2-25
Device Security	2-26
Creating a Security Set.....	2-28
Create Security Group	2-28
Creating a Security Group	2-29
Create Security Group Member	2-30
Creating a Security Group Member	2-31
Editing the Security Configuration on a Switch.....	2-32
Viewing Properties of a Security Set, Group, or Member	2-32
Using the Security Config	2-33
Archiving a Security Configuration to a File	2-33
Activating a Security Set	2-34
Deactivating a Security Set	2-34
Fabric Services	2-34
Tracking Fabric Version Information.....	2-35
Saving a Version Snapshot.....	2-35
Viewing and Comparing Version Snapshots	2-35
Exporting Version Snapshots to a File.....	2-36
Managing the Fabric Database	2-36
Adding a Fabric	2-36
Removing a Fabric	2-37
Rediscovering a Fabric	2-37
Adding a New Switch Module to a Fabric.....	2-37
Replacing a Failed Switch Module in a Fabric.....	2-38
Deleting Switches and Links from the Topology Window	2-38
Displaying Fabric Information	2-39
Fabric Status.....	2-39
Displaying the Event Browser.....	2-42
Devices Data Window	2-45
Active Zone Set Data Window	2-46
Working with Device Information and Nicknames	2-47
Displaying Detailed Device Information.....	2-47
Exporting Device Information to a File.....	2-47
Managing Device Port Nicknames	2-48
Zoning a Fabric	2-50
Zoning Concepts	2-50
Using the Zoning Wizard.....	2-53
Managing the Zoning Database	2-54
Managing Zone Sets	2-59
Managing Zones.....	2-61
Managing Aliases	2-64
Merging Fabrics and Zoning	2-65

Managing Switch Modules	2-66
Managing User Accounts	2-67
Creating User Accounts	2-68
Removing a User Account	2-69
Changing a User Account Password.....	2-70
Modifying a User Account.....	2-71
Displaying Switch Module Information	2-72
Hardware Status.....	2-73
Devices Data Window	2-73
Switch Data Window	2-74
Link Data Window	2-76
Port Statistics Data Window	2-76
Port Information Data Window	2-76
Configured Zonesets Data Window	2-77
Configuring Port Threshold Alarms	2-78
Paging a Switch Module.....	2-79
Setting the Date/Time and Enabling NTP Client.....	2-80
Resetting a Switch Module	2-80
Configuring a Switch Module	2-82
Using the Configuration Wizard.....	2-82
Switch Properties.....	2-83
Advanced Switch Properties	2-86
System Services Window	2-88
Network Properties.....	2-89
Archiving a Switch Module Configuration	2-91
Restoring a Switch Module Configuration.....	2-92
Restoring the Factory Default Configuration.....	2-94
Installing Firmware.....	2-96
Upgrading the Switch Using PFE Keys	2-97
Downloading a Support File.....	2-98
Managing Ports.....	2-99
Displaying Port Information.....	2-99
Monitoring Port Status	2-100
Displaying Port Types	2-101
Displaying Port Operational States	2-101
Displaying Port Speeds	2-102
Displaying Transceiver Media Status.....	2-102
Port Graphing and Performance Viewer Application	2-102
Port Statistics Data Window	2-103
Port Information Data Window	2-106
Configuring Ports.....	2-108
Changing Port Administrative States	2-109
Changing Port Speeds (External Ports Only).....	2-110
Changing Port Types (External Ports Only).....	2-111
Changing Device Scan (External Ports Only)	2-111
Changing Port Symbolic Name (External Ports Only)	2-112
Resetting a Port.....	2-112
Chapter 3 Switch Module Utility Functions	
LED Diagnostics	3-1
Testing Ports	3-2

Switch Module Monitoring Using SNMP	3-4
SNMP Configuration	3-5
SNMP Trap Configuration	3-6
Using the Performance Viewer Application.....	3-7
Starting Performance Viewer.....	3-8
Exiting Performance Viewer	3-8
Saving and Opening Performance View Files.....	3-9
Changing the Default Performance View File Encryption Key	3-10
Setting Performance Viewer Preferences	3-10
Setting the Polling Frequency	3-11
Displaying Graphs	3-11
Arranging Graphs in the Display	3-11
Customizing Graphs.....	3-12
Setting Global Graph Type.....	3-13
Rescaling a Selected Graph.....	3-13
Printing Graphs	3-14
Saving Graph Statistics to a File	3-14
Appendix A Mapping Port Locations and Software Numbering	
Port Mapping	A-1
Index	i-1

2-1	Topology Window	2-4
2-2	BladeCenter Faceplate Window	2-5
2-3	BladeCenter T Faceplate Window	2-5
2-4	Topology Window Menu.....	2-6
2-5	Faceplate Window Menu.....	2-7
2-6	Fabric Tree.....	2-9
2-7	Topology Window	2-11
2-8	Faceplate Window	2-14
2-9	Preferences Window – SANsurfer Switch Manager.....	2-17
2-10	Add Server	2-20
2-11	Remove Server.....	2-21
2-12	Edit Server Information	2-22
2-13	Modify Authentication Order - RADIUS Server Information.....	2-23
2-14	Edit Security Window	2-27
2-15	Create Security Group Window	2-28
2-16	Create a Security Group Member Window	2-30
2-17	Security Config Window	2-33
2-18	Fabric Version Snapshot Analysis Window.....	2-35
2-19	Add a New Fabric Window	2-36
2-20	Events Browser.....	2-42
2-21	Filter Events Window.....	2-44
2-22	Active Zone Set Data Window.....	2-46
2-23	Detailed Devices Display Window	2-47
2-24	Edit Zoning Window	2-54
2-25	Zoning Config Window	2-57
2-26	User Account Administration Window – Add Account.....	2-68
2-27	User Account Administration Window – Remove Account	2-69
2-28	User Account Administration Window – Change Password.....	2-70
2-29	User Account Administration Window - Modify Account	2-71
2-30	Faceplate Window - Switch Information.....	2-72
2-31	Hardware Status LEDs.....	2-73
2-32	Configured Zonesets Data Window	2-77
2-33	Port Threshold Alarm Configuration Window	2-78
2-34	Port Threshold Alarm Example	2-79
2-35	Switch Properties Window	2-83
2-36	Advanced Switch Properties Window.....	2-86
2-37	System Services window	2-88
2-38	Network Properties Window	2-89
2-39	Restore Windows – Full and Selective.....	2-92

2-40	Add License Key Dialog	2-97
2-41	BladeCenter Faceplate Window – Port Information.....	2-99
2-42	BladeCenter T Faceplate Window – Port Information	2-100
2-43	External Port Properties Window.....	2-108
2-44	Internal Properties Window	2-109
3-1	Switch Module LEDs.....	3-2
3-2	Port Loopback Test Window.....	3-3
3-3	SNMP Properties Window	3-4
3-4	Fabric View Graphs	3-7
3-5	Save Default Performance Viewer File Window.....	3-9
3-6	Load Default View File Window	3-9
3-7	Preferences – Performance Viewer.....	3-10
3-8	Default Graph Options Window	3-12

1-1	Command-Line Completion	1-5
1-2	Commands Listed by Authority Level	1-6
1-3	CIM Listener Configuration Parameters	1-11
1-4	CIM Subscription Configuration Parameters	1-13
1-5	ISL Group Member Attributes	1-25
1-6	Port Group Member Attributes	1-26
1-7	MS Group Member Attributes	1-26
1-8	Group Member Attributes	1-28
1-9	Switch Module Configuration Defaults	1-45
1-10	Port Configuration Defaults	1-46
1-11	Port Threshold Alarm Configuration Defaults	1-47
1-12	Zoning Configuration Defaults	1-47
1-13	SNMP Configuration Defaults	1-48
1-14	RADIUS Configuration Defaults	1-49
1-15	Services Configuration Defaults	1-49
1-16	System Configuration Defaults	1-50
1-17	Security Configuration Defaults	1-50
1-18	Set Config Port Parameters	1-60
1-19	Security Configuration Parameters	1-61
1-20	Set Config Switch Parameters	1-62
1-21	Set Config Threshold Parameters	1-63
1-22	Set Config Zoning Parameters	1-64
1-23	RADIUS Service Settings	1-74
1-24	Switch Module Services Settings	1-75
1-25	SNMP Configuration Settings	1-77
1-26	System Configuration Settings	1-79
1-27	Show Port Parameters	1-85
1-28	Switch Module Operational Parameters	1-89
1-29	Zoning Database Limits	1-123
2-1	Management Workstation Requirements	2-2
2-2	Tool Bar Buttons	2-8
2-3	Fibre Channel Switch Module and Link Status Indicators	2-11
2-4	Topology Window Switch and Status Icons	2-40
2-5	Severity Levels	2-43
2-6	Devices Data Window Entries	2-45
2-7	Edit Zoning Window Tool Bar Buttons and Icons	2-56
2-8	Factory User Accounts	2-67
2-9	Switch Data Window Entries	2-74
2-10	Switch Module Resets	2-81

2-11	Switch Module Administrative States	2-84
2-12	Timeout Values	2-87
2-13	IP Configuration Parameters.....	2-90
2-14	Factory Default Configuration Settings.....	2-94
2-15	Port Types	2-101
2-16	Port Operational States	2-101
2-17	Port Speeds.....	2-102
2-18	Port Transceiver Media View.....	2-102
2-19	Port Statistics Data Window Entries	2-103
2-20	Port Information Data Window Entries	2-106
2-21	Port Administrative States.....	2-110
2-22	Port Speeds.....	2-110
2-23	Port Types	2-111
3-1	SNMP Configuration Parameters.....	3-5
3-2	SNMP Trap Configuration Parameters	3-6
A-1	Port Mapping For Server Units.....	A-1

You can manage and configure your McDATA 6-Port Fibre Channel Switch Module through a Telnet connection to the embedded command line interface (CLI) or by using the SANsurfer Switch Manager application. The SANsurfer Switch Manager 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 SANsurfer Switch Manager application is referred to throughout this document as SANsurfer Switch Manager. The McDATA 6-Port 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 SANsurfer Switch Manager or the CLI. The SANsurfer Switch Manager is installed on a Microsoft® Windows® 2000, Microsoft Windows 2003, Windows XP, 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 [Chapter 1](#) 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 SANsurfer Switch Manager 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 *McDATA 6-Port Fibre Channel Switch Module for IBM Eserver BladeCenter Installation Guide*.

License Agreement for McDATA Applications

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

ANY OTHER USE OF THIS SOFTWARE MAY CAUSE UNFORSEEABLE PROBLEMS INCLUDING DATA ERRORS. McDATA 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 McDATA 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 McDATA Corporation ("McDATA"). After you agree to the terms and conditions of this Agreement, you will be allowed to install and use the SANsurfer Switch Manager with the applicable McDATA products. This agreement is not a transfer of rights, title or interest between McDATA 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. You may use each software module only with the associated McDATA hardware. Besides the copy of the software module necessary to operate that associated McDATA 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 McDATA legend or notice on any copy. Each software module contains or embodies proprietary intellectual property of McDATA or its licensors. The structure, organization or code are valuable trade secrets of Logic or its licensors. McDATA 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. McDATA 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 McDATA's distributors or any licensor of McDATA) assume the entire cost of all necessary servicing, repair or correction. There is no warranty by McDATA 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 McDATA 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 McDATA 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 McDATA 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 McDATA and you.

Technical Support

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

Command Line Interface (CLI)

Your McDATA 6-Port 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.

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 1-5](#) for more information about authority levels. See the [“User Command” on page 1-113](#) for information about creating user accounts.

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 SANsurfer Switch Manager inband and out-of-band logins, Application Programming Interface (API) inband and out-of-band logins, and Telnet logins.

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.

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 SANsurfer Switch Manager. 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.

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 SANsurfer Switch Manager.

```
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
xxxxxx 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 1-74](#). 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
```

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 1-1](#) describes the command-line completion keystrokes.

Table 1-1. 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.

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 1-7.

The commands and their page numbers are listed in Table 1-2.

Table 1-2. Commands Listed by Authority Level

Monitoring Commands		Configuration Command	
Help	(1-32)	Admin	(1-7)
History	(1-33)	Admin Session Commands	
Ping	(1-41)	Alias ¹	(1-8)
Ps	(1-42)	CIM ¹	(1-10)
Quit	(1-43)	CIMListener	(1-11)
Show	(1-83)	CIMSubscription	(1-13)
Show Config	(1-96)	Config ¹	(1-15)
Show Log	(1-99)	Create	(1-18)
Show Perf	(1-102)	Date ¹	(1-21)
Show Setup	(1-105)	Feature	(1-22)
Uptime	(1-112)	Firmware Install	(1-23)
Whoami	(1-116)	Group ¹	(1-24)
		Hardreset	(1-31)
		Hotreset	(1-34)
		Image	(1-36)
		Lip	(1-39)
		Passwd	(1-40)
		Reset	(1-44)
		Security	(1-52)
		Securityset ¹	(1-55)
		Set ¹	(1-57)
		Set Config	(1-59)
		Set Log	(1-69)
		Set Port ¹	(1-72)
		Set Setup	(1-74)
		Shutdown	(1-108)
		Test	(1-109)
		User ¹ ²	(1-113)
		Zone ¹	(1-117)
		Zoneset ¹	(1-120)
		Zoning ¹	(1-122)

¹Some keywords do not require an Admin session.

²Some 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 1-74](#).

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 for all keywords except List and Members. Refer to the [“Zoning Command” on page 1-122](#) for information about starting 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].

CIM Command

Manages CIM listener and subscription configurations on the switch. Refer to the [“CIMListener Command” on page 1-11](#) for information about creating and modifying CIM listeners. Refer to the [“CIMSubscription Command” on page 1-13](#) for information about creating and modifying CIM subscriptions.

Authority

Admin session

Syntax

```
cim
  cancel
  clear
  edit
  limits
  save
```

Keywords

cancel

Terminates the current CIM edit session without saving changes that were made.

clear

Clears all CIM listener and subscription configurations from the switch.

edit

Opens a CIM edit session.

limits

Displays the maximum allowed number of CIM listeners, subscriptions, and subscriptions per listener. This keyword does not require an Admin session nor a CIM edit session.

save

Saves all changes made during the current CIM edit session.

Examples

The following is an example of the CIM Edit command:

```
FCSM6 (admin): user1> cim edit
FCSM6 (admin-cim): user1> cimlistener create CIM_listener_1
.
.
.
FCSM6 (admin-cim): user1> cim save
```

The following is an example of the CIM Limits command:

```
FCSM6: user1> cim limits

  Cim Attribute                Maximum
  -----
  MaxListeners                  32
  MaxSubscriptions              50
  MaxSubscriptionsPerListener   6
```

CIMListener Command

Configures CIM indication service listeners and adds subscriptions to listeners. Refer to the “[CIMSubscription Command](#)” on page 1-13 for information about configuring subscriptions.

Authority

Admin session and a CIM Edit session. Refer to the “[CIM Command](#)” on page 1-10 for information about opening a CIM edit session.

Syntax

```
cimlistener
  add [listener_name] [subscription_list]
  create [listener_name]
  delete [listener_name]
  edit [listener_name]
```

Keywords

add [listener_name] [subscription_list]

Adds the set of subscriptions given by [subscription_list] to the listener given by [listener_name]. Use a <space> to delimit subscription names in [subscription_list].

create [listener_name]

Prompts you in a line-by-line fashion to create a CIM listener with the name given by [listener_name]. [listener_name] can have up to 32 characters: 0-9, A-Z, a-z, _, \$, ^, and -. The CIM listener configuration parameters are described in [Table 1-3](#).

Table 1-3. CIM Listener Configuration Parameters

Parameter	Description
Name	Listener name
Type	Listener type: <ul style="list-style-type: none"> Permanent – Send indications to the CIM client whether a connection can be established or not. This is the default. Transient – Sends indications to the CIM client, but ceases if a connection cannot be established after 60 minutes.
URL	IP address of the CIM client and the port number to which to send indications. The default is 10.0.0.1:5000.

delete [listener_name]

Deletes the listener given by [listener_name] from the CIM database.

edit [listener_name]

Opens an editing session in which you can modify the CIM listener given by [listener_name]. Refer to [Table 1-3](#) for a description of the CIM listener configuration parameters.

Examples

The following is an example of the CIMListener Create command:

```
FCSM6 (admin-cim): user1> cimlistener create listener_1
```

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.

```
Name listener_1
Type (2=Permanent, 3=Transient) [Permanent ]
URL (IP address:port format) [10.0.0.1:5000]
```

Finished configuring attributes.

This configuration must be saved with the cim save command before it can take effect, or to discard this configuration use the cim cancel command.

CIMSubscription Command

Creates, edits, or removes CIM subscriptions.

Authority

Admin session and a CIM Edit session. Refer to the [“CIM Command” on page 1-10](#) for information about opening a CIM edit session.

Syntax

```
cimsubscription
  create [subscription_name]
  delete [subscription_name]
  edit [subscription_name]
```

Keywords

create [subscription_name]

Prompts you in a line-by-line fashion to create a CIM subscription with the name given by [subscription_name]. [subscription_name] can have up to 32 characters: 0-9, A-Z, a-z, _, \$, ^, and -. [Table 1-4](#) describes the CIM subscription configuration parameters.

Table 1-4. CIM Subscription Configuration Parameters

Parameter	Description
Name	Subscription name.
FilterID	Event type for which the switch module monitors and sends an indication to the CIM client. The event types are as follows: <ul style="list-style-type: none"> • CreateComputerSystem – A switch is added to the fabric. This is the default. • ModifyComputerSystem – A switch state change. • DeleteComputerSystem – A switch is removed from the fabric. • CreateFCPort – Not supported. • ModifyFCPort – A Fibre Channel port state change. • DeleteFCPort – Not supported.
EnabledState	Enable (True) or disable (False) the subscription. The default is True.
Duration	Subscription life span in seconds. The subscription life span begins when the subscription is created. Expired subscriptions do not send indications to the CIM client though they remain in the CIM database. Values can be 1–720000. 0 indicates indefinite, which is the default.

delete [subscription_name]

Deletes the subscription given by [subscription_name] from the CIM database.

edit [subscription_name]

Opens an editing session in which you can modify the CIM subscription given by [subscription_name]. Refer to [Table 1-4](#) for a description of the CIM subscription configuration parameters.

Examples

The following is an example of the CIMSubscription Create command:

```
FCSM6 (admin-cim): user1> cimsubscription create subscription_1
```

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.

```
FilterID values:  1 = Create:ComputerSystem
                  2 = Modify:ComputerSystem
                  3 = Delete:ComputerSystem
                  4 = Create:FCPort
                  5 = Modify:FCPort
                  6 = Delete:FCPort
```

```
Name           subscription_1
FilterID       (see allowed options above)      [Create:ComputerSystem]
EnabledState   (True / False)                   [True           ]
Duration       (decimal value, 0-720000 secs, 0=forever) [0               ]
```

Finished configuring attributes.

This configuration must be saved with the cim save command before it can take effect, or to discard this configuration use the cim cancel command.

Config Command

Manages the switch module configurations. For information about setting the port and switch module configurations, refer to the [“Set Config Command” on page 1-59](#).

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 1-4](#).

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 switch module supports up to 10 configurations including the default configuration.

delete [config_name]

Deletes the configuration given by [config_name] from the switch module. You cannot delete the default configuration (Default Config) nor the active configuration.

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 switch module. This keyword does not require an admin session.

restore

Restores configuration settings to an out-of-band switch module from a backup file named *configdata*, which must be first uploaded on the switch using FTP. You create the backup file using the Config Backup command. Use FTP to load the backup file on a switch module, then enter the Config Restore command. After the restore is complete, the switch module automatically resets. Refer to [“Backing up and Restoring Switch Module Configurations” on page 1-4](#).

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 1-74](#).

NOTE: Configuration archive files created with the SANsurfer Switch Manager 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 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
```

The following is an example of how to create a backup file (configdata) and download the file to the workstation.

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

#>ftp symbolic_name or ip_address
user: images
password: images
ftp> bin
ftp> get configdata
ftp> quit
```


The following is an example of how to upload a configuration backup file (configdata) from the workstation to the switch module, and then restore the configuration.

```
#> ftp symbolic_name or ip_address
user: images
password: images
ftp> bin
ftp> put configdata
ftp> quit

FCSM6: user1> admin start
FCSM6 (admin): user1> config restore
The switch will be reset after restoring the configuration.
  Please confirm (y/n): [n] y
  Alarm Msg: [day month date time year][A1005.0021][SM][Configuration is
being restored - this could take several minutes !]
  Alarm Msg: [day month date time year][A1000.000A][SM][The switch will
be reset in 3 seconds due to a config restore]
FCSM6 (admin): user1: user1>
  Alarm Msg: [day month date time year][A1000.0005][SM][The switch is
being reset]
Good bye.
```

Create Command

Creates support files for troubleshooting switch problems, and certificates for secure communications for SANsurfer Switch Manager.

Authority

Admin session

Syntax

create
certificate
support

Keywords**certificate**

Creates a security certificate on the switch. The security certificate is required to establish an SSL connection with a management application such as SANsurfer Switch Manager. The certificate is valid 24 hours before the certificate creation date and expires 365 days after the creation date. Should the current certificate become invalid, use the Create Certificate command to create a new one.

To insure the creation of a valid certificate, be sure that the switch and the workstation time and date are the same. Refer to the following:

- [“Date Command” on page 1-21](#) for information about setting the time and date
- [“Set Command” on page 1-57](#) (Timezone keyword) for information about setting the time zone on the switch and workstation
- [“Set Setup Command” on page 1-74](#) (System keyword) for information about enabling the Network Time Protocol for synchronizing the time and date on the switch and workstation from an NTP server.

support

Assembles all log files and switch memory data into a core dump file (dump_support.tgz) on the switch. If your workstation has an FTP server, you can proceed with the command prompts to send the file from the switch to a remote host. Otherwise, you can use FTP to download the support file from the switch to your workstation. The support file is useful to technical support personnel for troubleshooting switch problems. Use this command when directed by your authorized maintenance provider.

Examples

The following is an example of the Create Support command when an FTP server is available on the workstation:

```
FCSM6 (admin): user1> create support
Log Msg:[Creating the support file - this will take several seconds]
FTP the dump support file to another machine? (y/n): y
Enter IP Address of remote computer: 10.20.33.130
Login name: johndoe
Enter remote directory name: bin/support
Would you like to continue downloading support file? (y/n) [n]: y
Connected to 10.20.33.130 (10.20.33.130).
220 localhost.localdomain FTP server (Version wu-2.6.1-18) ready.
331 Password required for johndoe.
Password: xxxxxxxx

230 User johndoe logged in.
cd bin/support
250 CWD command successful.
lcd /itasca/conf/images
Local directory now /itasca/conf/images
bin
200 Type set to I.
put dump_support.tgz
local: dump_support.tgz remote: dump_support.tgz
227 Entering Passive Mode (10,20,33,130,232,133)
150 Opening BINARY mode data connection for dump_support.tgz.
226 Transfer complete.
43430 bytes sent in 0.292 secs (1.5e+02 Kbytes/sec)
Remote system type is UNIX.
Using binary mode to transfer files.
221-You have transferred 43430 bytes in 1 files.
221-Total traffic for this session was 43888 bytes in 1 transfers.
221 Thank you for using the FTP service on localhost.localdomain.
```

The following is an example of the Create Support command and how to download the support file to your workstation. When prompted to send the support file to another machine, decline, then close the Telnet session. Open an FTP session on the switch and log in with the account name *images* and password *images*. Transfer the *dump_support.tgz* file in binary mode with the *Get* command.

```
FCSM6 (admin): user1> create support
Log Msg:[Creating the support file - this will take several seconds]
FTP the dump support file to another machine? (y/n): n

FCSM6 (admin): user1> quit
>ftp switch_ip_address
user: images
password: images

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

The following is an example of the Create Certificate command:

```
FCSM6 (admin): user1> create certificate
  The current date and time is day mon date hh:mm:ss UTC yyyy.
  This is the time used to stamp onto the certificate.
  Is the date and time correct? (y/n): [n] y
  Certificate generation successful.
```

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.

Notes

Network Time Protocol (NTP) must be disabled to set the time with the Date command. Refer to the [“Set Setup Command” on page 1-74](#), System keyword, for information about NTP.

When setting the date and time on a switch that is enabled for SSL connections, the switch module time must be within 24 hours of the workstation time. Otherwise, the connection will fail.

Examples

The following is an example of the Date command:

```
FCSM6: user1> date  
Mon Apr 07 07:51:24 2003
```

Feature Command

Adds Product Features Enable (PFE) key features to the switch and displays the PFE key feature log. For additional information about McDATA Product Features Enabled, please contact your McDATA representative or visit the McDATA website at www.mcdata.com.

Authority

Admin session for Add keyword only

Syntax

```
feature  
  add [pfe_key]  
  log
```

Keywords**add [license_key]**

Adds the feature that corresponds to the value given by [pfe_key]. [pfe_key] is case insensitive.

log

Displays a list of installed PFE key features.

Notes

The SANtegrity Enhanced® PFE key is required to configure and activate device security. Device security commands include the following:

- “Group Command” on page 1-24
- “Security Command” on page 1-52
- “Securityset Command” on page 1-55
- “Set Config Command” on page 1-59 (security keyword)

Firmware Install Command

Downloads firmware from a remote host to the switch module, installs the firmware, then resets the switch module (without a power-on self test) to activate the firmware. If possible, a non-disruptive activation is performed. The command prompts you for the following:

- IP address of the remote host
- An account name and password on the remote host
- Pathname for the firmware image file

Authority

Admin

Syntax

firmware install

Examples

The following is an example of the Firmware Install command:

```
FCSM6 (admin): user1> firmware install
Warning: Installing new firmware requires a switch reset.
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.

Do you want to continue? [y/n]: y
  Press 'q' and the ENTER key to abort this command.
  User Account      : johndoe
  IP Address        : 10.20.33.130
  Source Filename   : 5.2.x.00.11_mpc

  About to install image. Do you want to continue? [y/n] y
Connected to 10.20.33.130 (10.20.33.130).
220 localhost.localdomain FTP server (Version wu-2.6.1-18) ready.
331 Password required for johndoe.
Password: xxxxxxxxx
230 User johndoe logged in.
bin
200 Type set to I.
verbose
Verbose mode off.
  This may take several seconds...
  The switch will now reset.
Connection closed by foreign host.
```

Group Command

Creates groups, manages membership within the group, and manages the membership of groups in security sets.

NOTE: This command is available only with the SANtegrity Enhanced PFE key. For additional information about McDATA Product Features Enabled, please contact your McDATA representative or visit the McDATA website at www.mcddata.com.

Authority

Admin session and a Security Edit session. Refer to the “[Security Command](#)” on page 1-52 for information about starting a Security Edit session. The List, Members, Securitysets, and Type keywords are available without an Admin session.

Syntax

```
group
  add [group]
  copy
  create [group] [type]
  delete [group]
  edit [group] [member]
  list
  members [group]
  remove [group] [member_list]
  rename [group_old] [group_new]
  securitysets [group]
  type [group]
```


add [group]

Initiates an editing session in which to specify a group member and its attributes for the existing group given by [group]. ISL, Port, and MS member attributes are described in [Table 1-5](#), [Table 1-6](#), and [Table 1-7](#) respectively. The group name and group type attributes are read-only fields common to all three tables.

Table 1-5. ISL Group Member Attributes

Attribute	Description
Member	Worldwide name of the switch that would attach to the switch module. A member cannot belong to more than one group.
Authentication	Enables (CHAP) or disables (None) authentication using the Challenge Handshake Authentication Protocol (CHAP). The default is None.
Primary Hash	The preferred hash function to use to decipher the encrypted Primary Secret sent by the ISL member. The hash functions are MD5 or SHA-1. If the ISL member does not support the Primary Hash, the switch module will use the Secondary Hash.
Primary Secret	Hexadecimal string that is encrypted by the Primary Hash for authentication with the ISL group member. The string has the following lengths depending on the Primary Hash function: <ul style="list-style-type: none"> • MD5 hash: 16-byte • SHA-1 hash: 20-byte
Secondary Hash	Hash function to use to decipher the encrypted Secondary Secret sent by the ISL group member. Hash values are MD5 or SHA-1. The Secondary Hash is used when the Primary Hash is not available on the ISL group member. The Primary Hash and the Secondary Hash cannot be the same.
Secondary Secret	Hex string that is encrypted by the Secondary Hash and sent for authentication. The string has the following lengths depending on the Secondary Hash function: <ul style="list-style-type: none"> • MD5 hash: 16-byte • SHA-1 hash: 20-byte
Binding	Domain ID of the switch module to which to bind the ISL group member worldwide name. This option is available only if FabricBindingEnabled is set to True using the Set Config Security command. Refer to the “Set Config Command” on page 1-59 . 0 (zero) specifies no binding.

Table 1-6. Port Group Member Attributes

Attribute	Description
Member	Port worldwide name for the N_Port device that would attach to the switch. A member cannot belong to more than one group.
Authentication	Enables (CHAP) or disables (None) authentication using the Challenge Handshake Authentication Protocol (CHAP). The default is None.
Primary Hash	The preferred hash function to use to decipher the encrypted Primary Secret sent by the Port group member. The hash functions are MD5 or SHA-1. If the Port group member does not support the Primary Hash, the switch will use the Secondary Hash.
Primary Secret	Hexadecimal string that is encrypted by the Primary Hash for authentication with the Port group member. The string has the following lengths depending on the Primary Hash function: <ul style="list-style-type: none"> • MD5 hash: 16-byte • SHA-1 hash: 20-byte
Secondary Hash	Hash function to use to decipher the encrypted Secondary Secret sent by the Port group member. Hash values are MD5 or SHA-1. The Secondary Hash is used when the Primary Hash is not available on the Port group member. The Primary Hash and the Secondary Hash cannot be the same.
Secondary Secret	Hex string that is encrypted by the Secondary Hash and sent for authentication. The string has the following lengths depending on the Secondary Hash function: <ul style="list-style-type: none"> • MD5 hash: 16-byte • SHA-1 hash: 20-byte

Table 1-7. MS Group Member Attributes

Attribute	Description
Member	Port worldwide name for the N_Port device that would attach to the switch module.
CTAuthentication	Common Transport (CT) authentication. Enables (True) or disables (False) authentication for MS group members. The default is False.
Hash	The hash function to use to decipher the encrypted Secret sent by the MS group member. Hash values are MD5 or SHA-1.
Secret	Hexadecimal string that is encrypted by the Hash function for authentication with MS group members. The string has the following lengths depending on the Hash function: <ul style="list-style-type: none"> • MD5 hash: 16-byte • SHA-1 hash: 20-byte

copy [group_source] [group_destination]

Creates a new group named [group_destination] and copies the membership into it from the group given by [group_source].

create [group] [type]

Creates a group with the name given by [group] with the type given by [type]. A group name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, \$, ^, and -. The security database supports a maximum of 16 groups. If you omit [type], ISL is used. [type] can be one of the following:

ISL

Configures security for attachments to other switches.

Port

Configures security for attachments to N_Port devices.

MS

Configures security for attachments to N_Port devices that are issuing management server commands.

edit [group] [member]

Initiates an editing session in which to change the attributes of a worldwide name given by [member] in a group given by [group]. Member attributes that can be changed are described in [Table 1-8](#):

Table 1-8. Group Member Attributes

Attribute	Description
Authentication (ISL and Port Groups)	Enables (CHAP) or disables (None) authentication using the Challenge Handshake Authentication Protocol (CHAP).
CTAuthentication (MS Groups)	CT authentication. Enables (True) or disables (False) authentication for MS group members. The default is False.
Primary Hash (ISL and Port Groups)	The preferred hash function to use to decipher the encrypted Primary Secret sent by the member. The hash functions are MD5 or SHA-1. If the member does not support the Primary Hash, the switch module will use the Secondary Hash.
Hash (MS Groups)	The hash function to use to decipher the encrypted Secret sent by the MS group member. Hash values are MD5 or SHA-1.
Primary Secret (ISL and Port Groups)	Hexadecimal string that is encrypted by the Primary Hash for authentication with the member. The string has the following lengths depending on the Primary Hash function: <ul style="list-style-type: none"> • MD5 hash: 16-byte • SHA-1 hash: 20-byte
Secondary Hash (ISL and Port Groups)	Hash function to use to decipher the encrypted Secondary Secret sent by the group member. Hash values are MD5 or SHA-1. The Secondary Hash is used when the Primary Hash is not available on the group member. The Primary Hash and the Secondary Hash cannot be the same.
Secondary Secret (ISL and Port Groups)	Hex string that is encrypted by the Secondary Hash and sent for authentication. The string has the following lengths depending on the Secondary Hash function: <ul style="list-style-type: none"> • MD5 hash: 16-byte • SHA-1 hash: 20-byte
Secret (MS Groups)	Hexadecimal string that is encrypted by the Hash function for authentication with MS group members. The string has the following lengths depending on the Hash function: <ul style="list-style-type: none"> • MD5 hash: 16-byte • SHA-1 hash: 20-byte
Binding (ISL Groups)	Domain ID of the switch to which to bind the ISL group member worldwide name. This option is available only if FabricBindingEnabled is set to True using the Set Config Security command. Refer to the “Set Config Command” on page 1-59 . 0 (zero) specifies no binding.

list

Displays a list of all groups and the security sets of which they are members. This keyword is available without an Admin session.

members [group]

Displays all members of the group given by [group]. This keyword is available without an Admin session.

remove [group] [member_list]

Remove the port/device worldwide name given by [member] from the group given by [group]. Use a <space> to delimit multiple member names in [member_list]

rename [group_old] [group_new]

Renames the group given by [group_old] to the group given by [group_new].

securitysets [group]

Displays the list of security sets of which the group given by [group] is a member. This keyword is available without an Admin session.

type [group]

Displays the group type for the group given by [group]. This keyword is available without an Admin session.

Notes

Refer to the [“Securityset Command” on page 1-55](#) for information about managing groups in security sets.

Examples

The following is an example of the Group Add command:

```
FCSM6 (admin-security): user1> group add Group_1
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
with exception of the Group Member WWN field which is mandatory.
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.
Group Name      Group_1
Group Type      ISL
Member          (WWN)                [00:00:00:00:00:00:00:00]
Authentication  (None / Chap)          [None                    ]
PrimaryHash     (MD5 / SHA-1)          [MD5                      ]
PrimarySecret   (32 hex or 16 ASCII char value) [                          ]
SecondaryHash   (MD5 / SHA-1 / None)   [None                      ]
SecondarySecret (40 hex or 20 ASCII char value) [                          ]
Binding         (domain ID 1-239, 0=None) [0                          ]

Finished configuring attributes.
To discard this configuration use the security cancel command.
```

The following is an example of the Group Edit command:

```
FCSM6 (admin-security): user1> group edit G1 10:00:00:c0:dd:00:90:a3
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.
Group Name          g1
Group Type          ISL
Group Member        10:00:00:c0:dd:00:90:a3
Authentication      (None / Chap)                [None] chap
PrimaryHash         (MD5 / SHA-1)                [MD5 ] sha-1
PrimarySecret       (40 hex or 20 ASCII char value) [  ] 12345678901234567890
SecondaryHash       (MD5 / SHA-1 / None)         [None] md5
SecondarySecret     (32 hex or 16 ASCII char value) [  ] 1234567890123456
Binding             (domain ID 1-239, 0=None)    [3  ]
```

Finished configuring attributes.
To discard this configuration use the security cancel command.

The following is an example of the Group List command:

```
FCSM6: user1> group list
Group          SecuritySet
-----
group1 (ISL)
              alpha
group2 (Port)
              alpha
```

The following is an example of the Group Members command:

```
FCSM6: user1> group members group1
Current list of members for Group: group1
-----
10:00:00:c0:dd:00:71:ed
10:00:00:c0:dd:00:72:45
10:00:00:c0:dd:00:90:ef
10:00:00:c0:dd:00:b8:b7
```

Hardreset Command

Resets the 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 1-69](#).

Authority Admin session

Syntax **hardreset**

Notes To reset the switch module without a power-on self test, refer to the [“Reset Command” on page 1-44](#).

To reset the switch module without disrupting traffic, refer to the [“Hotreset Command” on page 1-34](#).

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 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 event log. After the pending firmware is activated, the configuration is recovered. This process takes less than 80 seconds. To save the event log to a file before resetting, refer to the [“Set Log Command”](#) on page 1-69.

Authority

Admin session

Syntax

hotreset

Notes

You can load and activate version 5.2.x.x firmware on an operating switch module without disrupting data traffic or having to re-initialize attached devices under the following conditions:

- The current firmware version is a 5.2.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 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, SANsurfer Switch Manager 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 switch module firmware.

Authority

Admin session

Syntax

```
image
  cleanup
  fetch [account_name] [ip_address] [file_source] [file_destination]
  install
  list
  unpack [file]
```

Keywords

cleanup

Removes all firmware image files from the switch module. All firmware image files are removed automatically each time the 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 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.

install

Downloads firmware from a remote host to the switch module, installs the firmware, then resets the switch module (without a power-on self test) to activate the firmware. If possible, a non-disruptive activation is performed. The command prompts you for the following:

- IP address of the remote host
- An account name and password on the remote host
- Pathname for the firmware image file

list

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

unpack [file]

Installs the firmware file given by [file]. After unpacking the file, a message appears confirming successful unpacking. The switch module 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.

To install firmware when the management workstation has an FTP server, use the Image Install command or the [“Firmware Install Command” on page 1-23](#). To install firmware when the management workstation does not have an FTP server, do the following:

1. Connect to the switch through the Ethernet port.
2. Move to the folder or directory on the workstation that contains the new firmware image file.

3. Establish communications with the switch module using the File Transfer Protocol (FTP). Enter one of the following on the command line:

```
>ftp xxx.xxx.xxx.xxx
```

or

```
>ftp switchname
```

where *xxx.xxx.xxx.xxx* is the switch IP address, and *switchname* is the switch module name associated with the IP address.

4. Enter the following account name and password:

```
user:images
```

```
password: images
```

5. Activate binary mode and copy the firmware image file on the switch module:

```
ftp>bin
```

```
ftp>put filename
```

6. Wait for the transfer to complete, then close the FTP session.

```
xxxxx bytes sent in xx secs.
```

```
ftp>quit
```

7. Establish communications with the switch using the CLI. Enter one of the following on the command line:

```
telnet xxx.xxx.xxx.xxx
```

or

```
telnet switchname
```

where *xxx.xxx.xxx.xxx* is the switch IP address, and *switchname* is the switch module name associated with the IP address.

8. A Telnet window opens prompting you for a login. Enter an account name and password. The default account name and password are (admin, password).

9. Open an Admin session to acquire the necessary authority.

```
FCSM6 $>admin start
```

10. Display the list of firmware image files on the switch to confirm that the file was loaded.

```
FCSM6 (admin) $>image list
```

11. Unpack the firmware image file to install the new firmware in flash memory.

```
FCSM6 (admin) $>image unpack filename
```

12. Wait for the unpack to complete.

```
image unpack command result: Passed
```

13. A message will prompt you to reset the switch module to activate the firmware. Resetting the switch module is disruptive. Use the Hotreset command to attempt a non-disruptive activation.

```
FCSM6 (admin) $>hotreset
```

Examples

The following is an example of the Image Install command:

```
FCSM6 (admin): user1> image install
Warning: Installing new firmware requires a switch reset.
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.
Do you want to continue? [y/n]: y
    Press 'q' and the ENTER key to abort this command.

User Account      : johndoe
IP Address        : 10.20.33.130
Source Filename   : 5.2.x.00.11_mpc

About to install image. Do you want to continue? [y/n] y

Connected to 10.20.33.130 (10.20.33.130).
220 localhost.localdomain FTP server (Version wu-2.6.1-18) ready.
331 Password required for johndoe.
Password: xxxxxxxxx
230 User johndoe logged in.
bin
200 Type set to I.
verbose
Verbose mode off.
    This may take several seconds...
    The switch will now reset.
Connection closed by foreign host.
```

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 (8-20 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. Broadcast IP addresses, such as 255.255.255.255, are not valid.

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 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]
  radius
  security
  services
  snmp
  switch (default)
  system
  zoning
```

Keywords

config [config_name]

Resets the configuration given by [config_name] to the factory default values for 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 1-9](#) through [Table 1-12](#) for switch, port, and port threshold alarm configuration default values.

factory

Resets switch module configuration, port configuration, port threshold alarm configuration, zoning configuration, SNMP configuration, system configuration, security configuration, RADIUS configuration, switch module services configuration, and zoning to the factory default values. The switch module configuration is activated automatically. Refer to [Table 1-9](#) through [Table 1-17](#).

NOTE: This does not affect installed Product Features Enabled (PFE) keys.

port [port_number]

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

radius

Resets the RADIUS configuration to the default values. Refer to [Table 1-14](#).

security

Clears the security database and deactivates the active security set. The security configuration value, autosave, and fabric binding remain unchanged.

services

Resets the switch module services configuration to the default values. Refer to [Table 1-15](#).

snmp

Resets the SNMP configuration settings to the factory default values. Refer to [Table 1-13](#) for SNMP configuration default values.

switch

Resets the 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 event log. To save the event log before resetting, refer to the [“Set Log Command” on page 1-69](#).

To reset the switch module with a power-on self test, refer to the [“Hardreset Command” on page 1-31](#). To reset the switch module without disrupting traffic, refer to the [“Hotreset Command” on page 1-34](#).

system

Resets the system configuration settings to the factory default values. Refer to [Table 1-16](#) for system configuration default values.

zoning

Clears the zoning database and deactivates the active zone set. The zoning configuration values (InteropAutosave, DefaultVisibility, DefaultZone, DiscardInactive) remain unchanged.

Notes

The following tables specify the various factory default settings:

Enter the Show Config Switch command to display switch configuration values.

Table 1-9. Switch Module Configuration Defaults

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

Enter the Show Config Port command to display port configuration values.

Table 1-10. 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
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
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.

Enter Show Config Threshold command to display threshold alarm configuration values.

Table 1-11. Port Threshold Alarm Configuration Defaults

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

Enter the Show Config Zoning command to display zoning configuration values.

Table 1-12. Zoning Configuration Defaults

Parameter	Default
InteropAutoSave	True
DefaultVisibility	All
DefaultZone	False
DiscardInactive	True

Enter the Show Setup SNMP command to display SNMP configuration values.

Table 1-13. SNMP Configuration Defaults

Parameter	Default
SNMPEnabled	True
Contact	<syscontact undefined>
Location	<sysLocation undefined>
Description	McDATA 6-Port 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

Enter the Show Setup Radius command to display RADIUS configuration values.

Table 1-14. RADIUS Configuration Defaults

Parameter	Default
DeviceAuthOrder	Local
UserAuthOrder	Local
TotalServers	1
DeviceAuthServer	False
UserAuthServer	False
AccountingServer	False
ServerIPAddress	10.0.0.1
ServerUDPPort	1812
Timeout	2 seconds
Retries	0
SignPackets	False

Enter the Show Setup Services command to display switch service configuration values.

Table 1-15. Services Configuration Defaults

Parameter	Default
TelnetEnabled	True
SSHEnabled	False
GUIMgmtEnabled	True
SSLMgmtEnabled	False
EmbeddedGUIEnabled	True
SNMPEnabled	True
NTPEnabled	False
CIMEnabled	True
FTPEEnabled	True.
MgmtServerEnabled	False

Enter the Show Setup System command to display system configuration values.

Table 1-16. 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
LocalLogEnabled	True
RemotelogEnabled	False
RemoteLogHostAddress	10.0.0.254
NTPClientEnabled	False
NTPServerAddress	10.0.0.254
EmbeddedGUIEnabled	True

Enter the Show Config Security command to display security configuration values.

Table 1-17. Security Configuration Defaults

Parameter	Default
AutoSave	True
FabricBindingEnabled	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.
```

Security Command

Opens a Security Edit session in which to manage the security database on a switch. Refer to the [“Group Command” on page 1-24](#) and the [“Securityset Command” on page 1-55](#).

NOTE: This command is available only with the SANtegrity Enhanced PFE key. For additional information about McDATA Product Features Enabled, please contact your McDATA representative or visit the McDATA website at www.mcddata.com.

Authority

Admin session. The keywords Active, History, Limits, and List are available without an Admin session.

Syntax

```
security
  active
  cancel
  clear
  edit
  history
  limits
  list
  restore
  save
```

Keywords

active

Displays the active security set, its groups, and group members. This keyword does not require an Admin session.

cancel

Closes a Security Edit session without saving changes. Use the Edit keyword to open a Security Edit session.

clear

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

NOTE: The preferred method for clearing the security database from the switch is the Reset Security command. Refer to the [“Reset Command” on page 1-44](#).

edit

Initiates a Security Edit session in which to make changes to the security database. A Security Edit session enables you to use the Group and Securityset commands to create, add, and delete security sets, groups, and group members. To close a Security Edit session and save changes, enter the Security Save command. To close a Security Edit session without saving changes, enter the Security Cancel command.

history

Displays history information about the security database and the active security set including the account name that made changes and when those changes were made. This keyword does not require an Admin session.

limits

Displays the current totals and the security database limits for the number of security sets, groups, members per group, and total members. This keyword does not require an Admin session.

list

Displays all security sets, groups, and group members in the security database. This keyword does not require an Admin session.

restore

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

save

Saves the changes that have been made to the security database during a Security Edit session. Changes you make to any security set will not take effect until you activate that security set. Refer to the [“Securityset Command” on page 1-55](#) for information about activating a security set.

Examples

The following is an example of the Security Active command:

```
FCSM6: user1> security active
Active Security Information

SecuritySet  Group  GroupMember
-----  ----  -----
alpha
          group1 (ISL)
          10:00:00:00:00:10:21:16
          Authentication    Chap
          Primary Hash      MD5
          Primary Secret    *****
          Secondary Hash     SHA-1
          Secondary Secret   *****
          Binding            0
          10:00:00:00:00:10:21:17
          Authentication    Chap
          Primary Hash      MD5
          Primary Secret    *****
          Secondary Hash     SHA-1
          Secondary Secret   *****
          Binding            0
```

The following is an example of the Security History command:

```
SB211.192: user1> security history
Active Database Information
-----
SecuritySetLastActivated/DeactivatedBy Remote
SecuritySetLastActivated/DeactivatedOn day month date time year
Database Checksum 00000000

Inactive Database Information
-----
ConfigurationLastEditedBy admin@IB-session11
ConfigurationLastEditedOn day month date time year
Database Checksum 00007558
```

The following is an example of the Security Limits command:

```
FCSM6: user1> security limits
Security Attribute Maximum Current [Name]
-----
MaxSecuritySets 4 1
MaxGroups 16 2
MaxTotalMembers 1000 19
MaxMembersPerGroup 1000
                                4 group1
                                15 group2
```

The following is an example of the Security List command:

```
FCSM6 (admin-security): user1> security list
SB211.192: user1> security list
Active Security Information
SecuritySet Group GroupMember
-----
No active securityset defined.

Configured Security Information
SecuritySet Group GroupMember
-----
alpha
    group1 (ISL)
        10:00:00:00:00:10:21:16
            Authentication Chap
            Primary Hash MD5
            Primary Secret *****
            Secondary Hash SHA-1
            Secondary Secret *****
            Binding 0
        10:00:00:00:00:10:21:17
            Authentication Chap
            Primary Hash MD5
            Primary Secret *****
            Secondary Hash SHA-1
            Secondary Secret *****
            Binding 0
```

Securityset Command

Manages security sets in the security database.

NOTE: This command is available only with the SANtegrity Enhanced PFE key. For additional information about McDATA Product Features Enabled, please contact your McDATA representative or visit the McDATA website at www.mcddata.com.

Authority

Admin session and a Security Edit session. Refer to the “[Security Command](#)” on page 1-52 for information about starting a Security Edit session. The Active, Groups, and List keywords are available without an Admin session. You must close the Security Edit session before using the Activate and Deactivate keywords.

Syntax

```
securityset
  activate [security_set]
  active
  add [security_set] [group_list]
  copy [security_set_source] [security_set_destination]
  create [security_set]
  deactivate
  delete [security_set]
  groups [security_set]
  list
  remove [security_set] [group]
  rename [security_set_old] [security_set_new]
```

Keywords

activate [security_set]

Activates the security set given by [security_set]. This keyword deactivates the active security set. Close the Security Edit session using the Security Save or Security Cancel command before using this keyword.

active

Displays the name of the active security set. This keyword is available to without an Admin session.

add [security_set] [group_list]

Adds one or more groups given by [group_list] to the security set given by [security_set]. Use a <space> to delimit multiple group names in [group_list]. A security set can have a maximum of three groups with no more than one group of each group type.

copy [security_set_source] [security_set_destination]

Creates a new security set named [security_set_destination] and copies into it the membership from the security set given by [security_set_source].

create [security_set]

Creates the security set with the name given by [security_set]. A security 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 security database supports a maximum of 4 security sets.

deactivate

Deactivates the active security set. Close the Security Edit session before using this keyword.

delete [security_set]

Deletes the security set given by [security_set]. If the specified security set is active, the command is suspended until the security set is deactivated.

groups [security_set]

Displays all groups that are members of the security set given by [security_set]. This keyword is available without an Admin session.

list

Displays a list of all security sets. This keyword is available without an Admin session.

remove [security_set] [group]

Removes a group given by [group] from the security set given by [security_set]. If [security_set] is the active security set, the group will not be removed until the security set has been deactivated.

rename [security_set_old] [security_set_new]

Renames the security set given by [security_set_old] to the name given by [security_set_new].

Notes

Refer to the [“Group Command” on page 1-24](#) for information about creating and managing groups.

Examples

The following is an example of the Securityset Active command

```
FCSM6: user1> securityset active
Active SecuritySet Information
-----
ActiveSecuritySet alpha
LastActivatedBy Remote
LastActivatedOn day month date time year
```

The following is an example of the Securityset Groups command

```
FCSM6: user1> securityset groups alpha
Current list of Groups for SecuritySet: alpha
-----
group1 (ISL)
group2 (Port)
```

The following is an example of the Securityset List command

```
FCSM6: user1> securityset list
Current list of SecuritySets
-----
alpha
beta
```


Set Command

Sets a variety of 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]  
  timezone
```

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 switch module, port, port threshold alarm, security, and zoning configuration parameters. Refer to the [“Set Config Command”](#) on page 1-59.

log [option]

Specifies the type of entries to be entered in the event log. Refer to the [“Set Log Command”](#) on page 1-69.

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 switch module reset or a reactivation of a switch module configuration. Refer to the [“Set Port Command” on page 1-72](#).

setup [option]

Changes SNMP and system configuration settings. Refer to the [“Set Setup Command” on page 1-74](#).

switch [state]

Changes the administrative state for all ports on the switch module to the state given by [state]. The previous Set Config Switch settings are restored after a switch reset or a reactivation of a 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.

timezone

Specifies the time zone for the switch module and the workstation. The default is Universal Time (UTC) also known as Greenwich Mean Time (GMT). This keyword prompts you to choose a region, then a subregion to specify the time zone.

Examples

The following examples enables and disables the beacon:

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

```
Command succeeded.
```

```
FCSM6: user1> set beacon off
```

```
Command succeeded.
```

Set Config Command

Sets switch module, port, port threshold alarm, security, and zoning configuration parameters. The changes you make with this command are not retained when you reset or power cycle the switch module unless you save them using the Config Save command. Refer to the [“Config Command” on page 1-15](#).

Authority

Admin session and a Config Edit session

Syntax

```
set config
  port [port_number]
  ports [port_set]
  security
  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 1-18](#) 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 of 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 1-18](#) 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 1-18. 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	Transmission speed: 1-Gbps, 2-Gbps, or Auto. The default is Auto.
PortType	Port type: 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.
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.

Table 1-18. Set Config Port Parameters (Continued)

Parameter	Description
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.
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.
PDISCPingEnable	Enables (True) or disables (False) the transmission of ping messages from the switch to all devices on a loop port. The default is True.

security

Initiates an editing session in which to change the security 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. Enter "q" or "Q" to end the editing session. Table 1-19 describes the Set Config Security parameters.

NOTE: This keyword is available only with the SANtegrity Enhanced PFE key. For additional information about McDATA Product Features Enabled, please contact your McDATA representative or visit the McDATA website at www.mcdata.com.

Table 1-19. Security Configuration Parameters

Parameter	Description
AutoSave	Enables (True) or disables (False) the saving of changes to active security set in the switch module's permanent memory. The default is True.
FabricBindingEnabled	Enables (True) or disables (False) the configuration and enforcement of fabric binding on all switches the fabric. Fabric binding associates switch worldwide names with a domain ID in the creation of ISL groups.

switch

Initiates an editing session in which to change 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 1-20](#) describes the Set Config Switch parameters.

Table 1-20. Set Config Switch Parameters

Parameter	Description
AdminState	Switch 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 switch module over an ISL. The default is True.
FDMEnabled	Fabric Device Monitoring Interface. Enables (True) or disables (False) the monitoring of target and initiator device information. The default is True.
FDMEntries	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 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 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 Config Default.
InteropMode	Interoperability mode for interoperating with McData® switches (McDATA Fabric Mode) or FC-SW-2 compliant switches (Standard). The default is McDATA Fabric Mode.

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 1-15](#) for information about saving and activating a configuration. [Table 1-21](#) describes the Set Config Threshold parameters. The 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 1-21. Set Config Threshold Parameters

Parameter	Description
Threshold Monitoring Enabled	Master enable/disable parameter for all events. Enables (True) or disables (False) the generation of all enabled event alarms. The default is False.
CRCErrorsMonitoringEnabled DecodeErrorsMonitoringEnabled ISLMonitoringEnabled LoginMonitoringEnabled LogoutMonitoringEnabled LOSMonitoringEnabled	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 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 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 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 1-22. Set Config Zoning Parameters

Parameter	Description
InteropAutoSave	Enables (True) or disables (False) the saving of changes to active zone set in the switch's permanent memory. The default is True. Disabling the Autosave parameter can be useful to prevent saving zoning information when experimenting with different zoning schemes. However, leaving the Autosave parameter disabled can disrupt device configurations should a switch have to be reset. For this reason, the Autosave parameter should be enabled in a production environment.
DefaultVisibility	Available only when InteropMode is Standard, this parameter enables (All) or disables (None) communication among the switch module's ports/devices and the fabric in the absence of an active zone set. Refer to " InteropMode " on page 1-62. The default is True. This parameter takes precedence over the DefaultZone parameter when InteropMode=Standard and there is no active zone set.
DefaultZoning	Enables (True) or disables (False) communication among ports/devices that are not defined in the active zone set or when there is no active zone set. This parameter must have the same value throughout the fabric. If InteropMode=McDATA Fabric Mode, the DefaultZoning parameter is automatically distributed throughout the fabric. Otherwise you must set DefaultZoning to be the same on each switch.
DiscardInactive	Enables (True) or disables (False) the discarding of the active zone set when a new zone set is activated from another switch. The default is True.

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)                                    [False ]
LCFEnable       (True / False)                                    [False ]
MFSEnable       (True / False)                                    [False ]
VIEEnable       (True / False)                                    [False ]
MSEnable        (True / False)                                    [True  ]
NoClose         (True / False)                                    [False ]
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.

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

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

FabricBindingEnabled (True / False)      [False]
AutoSave              (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.
```

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      ]
BroadcastEnabled    (True / False)           [True        ]
InbandEnabled       (True / False)           [True        ]
FDMIEnabled         (True / False)           [True        ]
FDMIEntries         (decimal value, 0-1000)      [1000        ]
DefaultDomainID     (decimal value, 1-239)      [2           ]
DomainIDLock        (True / False)           [False       ]
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=64 chars)     [Fibre Channel Switch Module]
InteropMode         (0=Standard, 1=McData Fabric Mode) [McDATA Fabric Mode]
```

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.

```
InteropAutoSave      (True / False) [True ]
DefaultZone          (True / False) [False]
DiscardInactive      (True / False) [False]
```

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 events to record in the event log and display on the screen. You determine what events to record in the switch event log using the Component, Level, and Port keywords. You determine what events are automatically displayed on the screen using the Display keyword. Alarms are always displayed on the screen.

Authority

Admin session

Syntax

```
set log
  archive
  clear
  component [filter_list]
  display [filter]
  level [filter]
  port [port_list]
  restore
  save
  start (default)
  stop
```

Keywords

archive

Collects all log entries and stores the result in new file named *logfile* that is maintained in switch module 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 [filter_list]

Specifies one or more components given by [filter_list] to monitor for events. A component is a firmware module that is responsible for a particular portion of switch module operation. Use a <space> to delimit values in the list. [filter_list] can be one or more of the following:

All

Monitors all components. To maintain optimal 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.

SNMP

Monitors all SNMP events.

Switch

Monitors switch management events.

Zoning

Monitors zoning conflict events.

display [filter]

Specifies the log events to automatically display on the screen according to the event severity levels given by [filter]. [filter] can be one of the following values:

Critical

Critical severity level events. The critical level describes events that are generally disruptive to the administration or operation of the fabric, but require no action.

Warn

Warning severity level events. The warning level describes events that are generally not disruptive to the administration or operation of the fabric, but are more important than the informative level events.

Info

Informative severity level events. The informative level describes routine events associated with a normal fabric.

None

Specifies no severity levels for display on the screen.

level [filter]

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

Critical

Monitors critical events. The critical level describes events that are generally disruptive to the administration or operation of the fabric, but require no action.

Warn

Monitors warning and critical events. The warning level describes events that are generally not disruptive to the administration or operation of the fabric, but are more important than the informative level events.

Info

Monitors informative, warning, and critical events. The informative level describes routine events associated with a normal fabric. This is the default severity level.

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, severity level, port, and display level. These settings remain in effect after a 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

In addition to critical, warn, and informative severity levels, the highest event severity level is alarm. The alarm level describes events that are disruptive to the administration or operation of a fabric and require administrator intervention. Alarms are always logged and always displayed on the screen.

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

Manages configuration settings for Remote Authentication Dial-In User Service (RADIUS) servers, switch services, SNMP, and system configurations. The switch module maintains one SNMP configuration and one system configuration.

Authority Admin session

Syntax

```
set setup
  radius
  services
  snmp
  system
```

Keywords **radius**

NOTE: Device authentication is available only with the SANtegrity Enhanced PFE key. For additional information about McDATA Product Features Enabled, please contact your McDATA representative or visit the McDATA website at www.mcdata.com.

Prompts you in a line-by-line fashion to configure RADIUS servers for user account and device authentication. [Table 1-23](#) describes the RADIUS server configuration fields.

Table 1-23. RADIUS Service Settings

Entry	Description
DeviceAuthOrder ¹	Authenticator priority for devices: <ul style="list-style-type: none"> Local: Authenticate devices using only the local security database. This is the default. Radius: Authenticate devices using only the security database on the RADIUS server. RadiusLocal: Authenticate devices using the RADIUS server security database first. If the RADIUS server is unavailable, then use the local switch security database.
UserAuthOrder	Authenticator priority for user accounts: <ul style="list-style-type: none"> Local: Authenticate users using only the local security database. This is the default. Radius: Authenticate users using only the security database on the RADIUS server. RadiusLocal: Authenticate users using the RADIUS server security database first. If the RADIUS server is unavailable, then use the local switch security database.
TotalServers	Number of RADIUS servers to configure during this session. Setting TotalServers to 0 disables all RADIUS authentication. The default is 0.
ServerIPAddress	IP address of the RADIUS server. The default is 10.0.0.1.
ServerUDPPort	User Datagram Protocol (UDP) port number on the RADIUS server. The default is 1812.

Table 1-23. RADIUS Service Settings (Continued)

Entry	Description
DeviceAuthServer ¹	Enable (True) or disable (False) this server for device authentication. The default is False.
UserAuthServer	Enable (True) or disable (False) this server for user account authentication. A user authentication RADIUS server requires a secure management connection (SSL). The default is True.
AccountingServer	Enable (True) or disable (False) this server for auditing of activity during a user session. When enabled, user activity is audited whether UserAuthServer is enabled or not. The default is False. The accounting server UDP port number is the ServerUDPPort value plus 1 (default 1813).
Timeout	Number of seconds to wait to receive a response from the RADIUS server before timing out. The default is 2.
Retries	Number of retries after the first attempt to establish communication with the RADIUS server fails. The default is 0.
SignPackets	Enable (True) or disable (False) the use of sign packets to protect the RADIUS server packet integrity. The default is False.
Secret	32-byte hex string or 16-byte ASCII string used as a password for authentication purposes between the switch and the RADIUS server.

¹ This parameter is available only with the SANtegrity Enhanced PFE key.

services

Prompts you in a line-by-line fashion to enable or disable switch module services. [Table 1-24](#) describes the switch module service parameters. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets.

NOTE: Use caution when disabling TelnetEnabled and GUIMgmtEnabled; it is possible to disable all Ethernet access to the switch module.

Table 1-24. Switch Module Services Settings

Entry	Description
TelnetEnabled	Enables (True) or disables (False) the ability to manage the switch module over a Telnet connection. Disabling this service is not recommended. The default is True.
SSHEnabled	Enables (True) or disables (False) Secure Shell (SSH) connections to the switch module. SSH secures the remote connection to the switch module. To establish a secure remote connection, your workstation must use an SSH client. The default is False.

Table 1-24. Switch Module Services Settings (Continued)

Entry	Description
GUIMgmtEnabled	Enables (True) or disables (False) out-of-band management of the switch module with SANsurfer Switch Manager, the SANsurfer Switch Manager Application Programming Interface, SNMP, and CIM. If this service is disabled, the switch module can only be managed inband. The default is True.
SSLMgmtEnabled	Enables (True) or disables (False) secure SSL connections for management applications including SANsurfer Switch Manager, the McDATA SANbrowser, Application Programming Interface, and the CIM server. The default is False. <ul style="list-style-type: none"> To enable secure SSL connections, you must first synchronize the date and time on the switch module and workstation. This service must be enabled to authenticate users through a RADIUS server. Enabling SSL automatically creates a security certificate on the switch module. To disable SSL when using a user authentication RADIUS server, the RADIUS server authentication order must be local.
EmbeddedGUIEnabled	Enables (True) or disables (False) the McDATA SANbrowser. The McDATA SANbrowser enables you to point at a switch module with an internet browser and run SANsurfer Switch Manager through the McDATA SANbrowser. This parameter is the master control for the Set Setup System command parameter, EmbeddedGUIEnabled. The default is True.
SNMPEnabled	Enables (True) or disables (False) the management of the switch through third-party applications that use the Simple Network Management Protocol (SNMP). This parameter is the master control for the Set Setup SNMP command parameter, SNMPEnabled. The default is True.
NTPEnabled	Enables (True) or disables (False) the Network Time Protocol (NTP) which allows the synchronizing of switch module and workstation dates and times with an NTP server. This helps to prevent invalid SSL certificates and timestamp confusion in the event log. The default is False. This parameter is the master control for the Set Setup System command parameter, NTPClientEnabled. The default is False.
CIMEnabled	Enables (True) or disables (False) the management of the switch module through third-party applications that use the Common Information Model (CIM). The default is True.
FTPEnabled	Enables (True) or disables (False) the File Transfer Protocol (FTP) for transferring files rapidly between the workstation and the switch module. The default is True.
MgmtServerEnabled	Enables (True) or disables (False) the management of the switch through third-party applications that use GS-3 Management Server (MS). This parameter is the master control for the Set Config Port command parameter, MSEnable. The default is False.

snmp

Prompts you in a line-by-line fashion to change SNMP configuration settings. [Table 1-25](#) 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 1-25. SNMP Configuration Settings

Entry	Description
SNMPEnabled	Enables (True) or disables (False) SNMP on the 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 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).
ReadCommunity	Read community password that authorizes an SNMP agent to read information from the switch module. This is a write-only field. The value on the 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 switch module. This is a write-only field. The value on the 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 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".

Table 1-25. SNMP Configuration Settings (Continued)

Entry	Description
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 1-26](#) 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 1-26. System Configuration Settings

Entry	Description
Eth0NetworkDiscovery	Ethernet boot method: (1 - Static). Bootp, DHCP, and RARP do not apply.
Eth0NetworkAddress	Ethernet Internet Protocol (IP) address.
Eth0NetworkMask	Ethernet subnet mask address.
Eth0GatewayAddress	Ethernet IP address gateway.
AdminTimeout	Amount of time in minutes the 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 switch module waits before terminating an idle Telnet command line interface session. Zero (0) disables the time out threshold. The default is 0, the maximum is 1440.
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 switch 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 switch 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 switch 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. The default is False.
NTPServerAddress	The IP address of the NTP server from which the NTP client acquires the time and date. The default is 10.0.0.254.
EmbeddedGUIEnabled	Enables (True) or disables (False) the McDATA SANbrowser. Changing this parameter to False while the McDATA SANbrowser is running will terminate the McDATA SANbrowser. The default is True.

Examples

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

```
FCSM6 (admin): user1> set setup radius
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
attributes
for the server being processed, press 'q' or 'Q' and the ENTER key to
do so.
If you wish to terminate the configuration process completely, press
'qq' or
'QQ' and the ENTER key to so do.

DeviceAuthOrder (1=Local, 2=Radius, 3=RadiusLocal) [Local]
UserAuthOrder (1=Local, 2=Radius, 3=RadiusLocal) [Local]
TotalServers (decimal value, 0-5) [1 ]

Server: 1
ServerIPAddress (dot-notated IP Address) [10.20.11.8]
ServerUDPPort (decimal value) [1812 ]
DeviceAuthServer (True / False) [True ]
UserAuthServer (True / False) [True ]
AccountingServer (True / False) [False ]
Timeout (decimal value, 10-30 secs) [10 ]
Retries (decimal value, 1-3, 0=None) [0 ]
SignPackets (True / False) [False ]
Secret (32 hex or 16 ASCII char value) [***** ]
Do you want to save and activate this radius setup? (y/n): [n]
```

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

```
FCSM6 (admin): user1> set setup services
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.
*Warning: If services are disabled, the connection to the switch may be
lost.

TelnetEnabled (True / False) [True ]
SSHEnabled (True / False) [False]
GUIMgmtEnabled (True / False) [True ]
SSLMgmtEnabled (True / False) [False]
EmbeddedGUIEnabled (True / False) [True ]
SNMPEnabled (True / False) [True ]
NTPEnabled (True / False) [False]
CIMEnabled (True / False) [True ]
FTPEnabled (True / False) [True ]
MgmtServerEnabled (True / False) [True ]

Do you want to save and activate this services setup? (y/n): [n]
```


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            ]
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, switch module, and port operational information.

Authority

None

Syntax

show
 about
 alarm *[option]*
 audit
 broadcast
 chassis
 cimlistener *[listener_name]*
 cimsubscription *[subscription_name]*
 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
 timezone
 topology
 users
 version

Keywords

about

Displays an introductory set of information about operational attributes of the 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 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.

audit

Displays the most recent 200 records in the administrative audit log. The audit log contains configuration and administrative changes that have been made to the switch including the originating management session and IP address.

broadcast

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

chassis

Displays chassis component status and temperature.

cimlistener [listener_name]

Displays CIM indicator services listener information for the listener given by [listener_name]. If you omit [listener_name], the command displays all listeners.

cimsubscription [subscription_name]

Displays CIM subscription information for the subscription given by [subscription_name]. If you omit [subscription_name], the command displays all subscriptions.

config [option]

Displays switch module, port, and zoning configuration attributes. Refer to the [“Show Config Command” on page 1-96](#).

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 1-99](#). The log is cleared when the 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 1-102](#).

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 1-27](#) describes the port parameters.

Table 1-27. 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
EpIsoReason	E_Port isolation reason
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

Table 1-27. Show Port Parameters (Continued)

Entry	Description
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
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.

Table 1-27. Show Port Parameters (Continued)

Entry	Description
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.
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.

Table 1-27. Show Port Parameters (Continued)

Entry	Description
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 most recently failed POST.

setup [option]

Displays setup attributes for the system, SNMP, and the switch module manufacturer. Refer to the [“Show Setup Command” on page 1-105](#).

steering [domain_id]

Displays the routes that data takes to the 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 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
- Group List
- History
- Ps
- Security (List, Limits, History)
- Securityset (Active, List)
- Show (About, Alarm, Backtrace, Chassis, Config Port, Config Security, Config Switch, Config Threshold, Dev, Dev Settings, Domains, Donor, Fabric, Log, Log Archive, 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 switch module operational information. [Table 1-28](#) describes the switch module operational parameters.

Table 1-28. Switch Module Operational Parameters

Parameter	Description
SymbolicName	Descriptive name for the switch
SwitchWWN	Switch world wide name
SwitchType	Switch model
BootVersion	PROM boot version
CreditPool	Number of port buffer credits available to recipient ports
DomainID	Switch domain ID
FirstPortAddress	FC address of switch port 0
FlashSize - MBytes	Size of the flash memory in megabytes
LogLevel	Event severity level used to record events in the event log
MaxPorts	Number of ports available on the switch
NumberOfResets	Number of times the switch has been reset over its service life
ReasonForLastReset	Action that caused the last reset
ActiveImageVersion - build date	Active firmware image version and build date.
PendingImageVersion - build date	Firmware image version and build date that is pending. This image will become active at the next reset or power cycle.
ActiveConfiguration	Name of the switch configuration that is in use.
AdminState	Switch administrative state
AdminModeActive	Admin session status
BeaconOnStatus	Beacon status as set by the Set Beacon command.
OperationalState	Switch operational state
PrincipalSwitchRole	Principal switch status. True indicates that this switch is the principal switch.
BoardTemp (1) - Degrees Celsius	Internal switch temperature at circuit board sensor 1
SwitchDiagnosticsStatus	Results of the power-on self test
SwitchTemperatureStatus	Switch temperature status: normal, warning, failure

timezone

Displays the current time zone setting.

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 module. This keyword is equivalent to the About keyword.

Examples

The following is an example of the Show Chassis command:

```
FCSM6: user1> show chassis
Chassis Information
-----
BoardTemp (1) - Degrees Celsius    31
PowerSupplyStatus (1)              Good
HeartBeatCode                       1
HeartBeatStatus                     Normal
```

The following is an example of the Show Domains command:

```
FCSM6: user1> show domains
Principal switch is (remote): 10:00:00:60:69:50:0b:6c
Upstream Principal ISL is      : 1
Domain ID List:
Domain 97 (0x61) WWN = 10:00:00:c0:dd:00:71:ed
Domain 98 (0x62) WWN = 10:00:00:60:df:22:2e:0c
Domain 99 (0x63) WWN = 10:00:00:c0:dd:00:72:45
Domain 100 (0x64) WWN = 10:00:00:c0:dd:00:ba:68
Domain 101 (0x65) WWN = 10:00:00:60:df:22:2e:06
Domain 102 (0x66) WWN = 10:00:00:c0:dd:00:90:ef
Domain 103 (0x67) WWN = 10:00:00:60:69:50:0b:6c
Domain 104 (0x68) WWN = 10:00:00:c0:dd:00:b8:b7
```

The following is an example of the Show Fabric command:

```
FCSM6: user1> show fabric
```

Domain	WWN	Enet IP Addr	FC IP Addr	SymbolicName
-----	---	-----	-----	-----
16 (0x10)	10:00:00:c0:dd:00:77:81	10.20.68.11	0.0.0.0	gui sb1 .11
17 (0x11)	10:00:00:c0:dd:00:6a:2d	10.20.68.12	0.0.0.0	sw12
18 (0x12)	10:00:00:c0:dd:00:c3:04	10.20.68.160	0.0.0.0	sw .160
19 (0x13)	10:00:00:c0:dd:00:bc:56	10.20.68.108	0.0.0.0	Sb2 .108

The following is an example of the Show FDMI command:

```
FCSM6: user1> show fdmi
```

HBA ID	PortID	Manufacturer	Model	Ports
21:01:00:e0:8b:27:aa:bc	610000	QLogic Corporation	QLA2342	2
21:00:00:00:ca:25:9b:96	180100	QLogic Corporation	QL2330	2

The following is an example of the Show FDMI WWN command:

```
FCSM6: user1> show fdmi 21:00:00:e0:8b:09:3b:17
```

```
FDMI Information
```

```

-----
Manufacturer          QLogic Corporation
SerialNumber          [04202
Model                 QLA2342
ModelDescription      QLogic QLA2342 PCI Fibre Channel Adapter
PortID                610000
NodeWWN               20:00:00:e0:8b:07:aa:bc
HardwareVersion       FC5010409-10
DriverVersion         8.2.3.10 Beta 2 (W2K VI)
OptionRomVersion      1.21
FirmwareVersion       03.02.13.
OperatingSystem       SunOS 5.8
MaximumCTPayload      2040
NumberOfPorts         1

```

```
Port 21:01:00:e0:8b:27:aa:bc
```

```

SupportedFC4Types     FCP
SupportedSpeed        2Gb/s
CurrentSpeed          2Gb/s
MaximumFrameSize     2048
OSDeviceName
HostName

```

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

```
FCSM6: user1> show ns
```

Seq No	Domain ID	Port ID	Port Type	COS	PortWWN	NodeWWN
1	19 (0x13)	1301e1	NL	3	21:00:00:20:37:73:13:69	20:00:00:20:37:73:13:69
2	19 (0x13)	1301e2	NL	3	21:00:00:20:37:73:12:9b	20:00:00:20:37:73:12:9b
3	19 (0x13)	1301e4	NL	3	21:00:00:20:37:73:05:26	20:00:00:20:37:73:05:26
4	19 (0x13)	130d00	N	3	21:01:00:e0:8b:27:a7:bc	20:01:00:e0:8b:27:a7:bc

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

```
FCSM6: user1> show ns 18
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
```

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:00:BD:ED
          inet addr:10.20.68.107 Bcast:10.20.68.255 Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4712 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3000 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:415313 (405.5 Kb)  TX bytes:716751 (699.9 Kb)
          Interrupt:11 Base address:0xfcc0
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:304 errors:0 dropped:0 overruns:0 frame:0
          TX packets:304 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:20116 (19.6 Kb)  TX bytes:20116 (19.6 Kb)
```

The following is an example of the Show Port command:

```
FCSM6: user1> show port 1
-----
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
BootVersion                  V1.3.0.2.0 (Fri Dec  3 15:30:41 2004)
CreditPool                   0
DomainID                     1 (0x1)
FirstPortAddress             010000
FlashSize - MBytes          128
LogFilterLevel               Info
MaxPorts                     20
NumberOfResets               14
ReasonForLastReset           PowerUp
ActiveImageVersion - build date V5.2.x.10.0(Tue Feb 15 07:00:55 2005)
PendingImageVersion - build date V5.2.x.10.0(Tue Feb 15 07:00:55 2005)
ActiveConfiguration          default
AdminState                   Online
AdminModeActive              False
BeaconOnStatus               False
OperationalState             Online
PrincipalSwitchRole           False
BoardTemp (1) - Degrees Celsius 31
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 Local          Rem Remote          Unique
Type      Type PortWWN         Type NodeWWN         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  McDATA 6-Port Fibre Channel Switch
                  Module for IBM eServer BladeCenter (TM)
Eth0NetworkAddress 10.20.92.246 (use 'set setup system' to update)
MACAddress         00:c0:dd:07:06:0a
WorldWideName     10:00:08:00:88:e0:00:0a
ChassisSerialNumber 0501000020
ActiveSWVersion    V5.2.0.9.0
ActiveTimestamp    Tue Feb  8 07:27:44 2005
DiagnosticsStatus  Passed
LicensedExternalPorts 6
LicensedInternalPorts 14
```

Show Config Command

Displays switch module, port, alarm threshold, security, and zoning for the current configuration.

Authority

None

Syntax

```
show config
  port [port_number]
  security
  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](#).

security

Displays the security database Autosave parameter value.

NOTE: This keyword is available only with the SANtegrity Enhanced PFE key. For additional information about McDATA Product Features Enabled, please contact your McDATA representative or visit the McDATA website at www.mcdata.com.

switch

Displays configuration parameters for the switch module.

threshold

Displays alarm threshold parameters for the switch module.

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
Configuration Name: default
-----
Port Number: 15
-----
AdminState           Online
LinkSpeed            Auto
PortType              GL
SymbolicName          Port15
ALFairness            False
DeviceScanEnabled    True
ForceOfflineRSCN     False
ARB_FF                False
InteropCredit         0
ExtCredit             0
FANEnabled            True
AutoPerfTuning        True
MSEnabled             True
NoClose               False
PDISCPingEnabled     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
DefaultDomainID      19 (0x13)
DomainIDLck          True
SymbolicName          FCSM6
R_A_TOV              10000
E_D_TOV              2000
PrincipalPriority     254
ConfigDescription     Default Config
ConfigLastSavedBy    USERID@OB-session5
ConfigLastSavedOn    day month date time year
InteropMode           McDATA Fabric Mode
```

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
-----
InteropAutoSave                True
DefaultVisibility              None
DefaultZone                    False
DiscardInactive                False
```

Show Log Command

Displays the contents of the log or the parameters used to create and display entries in the log. The log contains a maximum of 1200 entries. When the log reaches its entry capacity, subsequent entries overwrite the existing entries, beginning with the oldest.

Authority

None

Syntax

```
show log
  [number_of_events]
  component
  display [filter]
  level
  options
  port
  settings
```

Keywords

[number_of_events]

Specifies the number of the most recent events to display from the event log. [number_of_events] must be a positive integer.

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

SNMP

SNMP events.

Switch

Monitors switch management events.

Zoning

Monitors zoning conflict events.

display [filter]

Displays log events on the screen according to the component or severity level filter given by [filter]. [filter] can be one of the following:

Info

Displays all informative events.

Warning

Displays all warning events.

Critical

Displays all critical events.

Eport

Displays all events related to E_Ports.

Mgmtserver

Displays all events related to the management server.

Nameserver

Displays all events related to the name server.

Port [port_number]

Displays all events related to the port given by [port_number]. External ports are numbered 10–13; internal ports are numbered 0–9.

SNMP

Displays all events related to SNMP.

Switch

Displays all events related to switch management.

Zoning

Displays all events related to zoning.

level

Displays the event severity level logging setting and the display level setting.

options

Displays the options that are available for configuring event logging and automatic display to the screen. Refer to the for information about how to configure event logging and display level.

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 filter settings for component, severity level, port, and display level. 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 settings for log
-----
FilterComponent  NameServer MgmtServer Zoning Switch Blade Port
Eport Snmp
```

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

```
FCSM6: user1> show log level
Current settings for log
-----
FilterLevel      Info
DisplayLevel     Critical
```

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

```
FCSM6: user1> show log options
Allowed options for log
-----
FilterComponent
All, None, NameServer, MgmtServer, Zoning, Switch, Blade, Port, Eport, Snmp
FilterLevel      Critical, Warn, Info, None
DisplayLevel     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 for all ports. Type any character to stop the display.

inframe

Displays continuous performance data in frames/second received. 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.

Examples

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
  radius
  services
  snmp
  system
```

Keywords

mfg

Displays manufacturing information about the switch module.

radius

Displays RADIUS server information.

services

Displays switch service status information.

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           McDATA
  BuildDate           Unknown
  ChassisPartNumber   SB20-SDV
  ChassisSerialNumber 000015889
  CPUBoardSerialNumber 000015889
  LicensedPorts       20
  MACAddress          00:c0:dd:07:06:0a
  PlanarPartNumber    31106-02 A
  SwitchSymbolicName  FCSM6
  SwitchWWN           10:00:00:c0:dd:01:6e:55
  SystemDescription   McDATA 6-Port 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 Services command:

```
FCSM6: user1> show setup services
System Services
-----
TelnetEnabled           True
SSHEnabled              False
GUIMgmtEnabled         True
SSLMgmtEnabled         False
EmbeddedGUIEnabled     True
SNMPEnabled            True
NTPEnabled             True
CIMEnabled             True
FTPEntered            True
MgmtServerEnabled     True
```

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

```
FCSM6: user1> show setup radius

Radius Information
-----
DeviceAuthOrder  RadiusLocal
UserAuthOrder    RadiusLocal
TotalServers     1

Server: 1

ServerIPAddress  10.20.11.8
ServerUDPPort    1812
DeviceAuthServer False
UserAuthServer   True
AccountingServer False
Timeout          2
Retries          0
SignPackets      False
Secret           *****
```

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

```
FCSM6: user1> show setup snmp
SNMP Information
-----
SnmEnabled           True
Contact              <sysContact undefined>
Location             <sysLocation undefined>
Description           McDATA 6-Port Fibre Channel Switch
                    Module for IBM eServer BladeCenter (TM)
Trap1Address         10.0.0.254
Trap1Port            162
Trap1Severity        warning
Trap1Version         2
Trap1Enabled         False
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      True
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
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 switch module at convenient points and closes the Telnet session. Always power cycle the 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 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 1-57](#) for information about changing the port administrative state. While the test is running, the remaining ports on the switch 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) #> 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 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 module. This keyword is available to all account names without an Admin session.

add

Add a user account to the switch. You will be prompted for an account name, a password, authority, and an expiration date.

- A switch module can have a maximum of 15 user accounts.
- Account names are limited to 15 characters; passwords must be 8–20 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 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

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): user1> user add
      Press 'q' and the ENTER key to abort this command.
account name (1-15 chars)      : user1
account password (8-20 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): user1> 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): user1> 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 time year	10.20.68.108-1031	day month date
USERID@OB-session2 time year	10.20.68.108-1034	day month date
snmp@OB-session3 time year	Unknown	day month date
snmp@IB-session4 time year	Unknown	day month date
user1@OB-session5 time year	Unknown	day month date

Whoami Command

Displays the account name, session number, and switch module domain ID for the Telnet session.

Authority

None

Syntax

whoami

Examples

The following is an example of the Whoami command:

```
FCSM6: user1> 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 1-122](#) 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 2000 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
-----
wwn_b0241f
              zone_set_1

wwn_23bd31
              zone_set_1

wwn_221416
              zone_set_1

wwn_2215c3
              zone_set_1

wwn_0160ed
              zone_set_1

wwn_c001b0
              zone_set_1

wwn_401248
              zone_set_1

wwn_02402f
              zone_set_1

wwn_22412f
              zone_set_1
```

The following is an example of the Zone Members command:

```
FCSM6: user1> zone members wwn_b0241f

Current List of Members for Zone: wwn_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 1-122](#) 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 1-117](#) and the [“Zoneset Command” on page 1-120](#).

Authority

Admin session except for the Active, History, Limits, and List keywords. The Clear keyword also requires a zoning edit session.

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 requires a zoning edit session. 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 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 switch module zoning database limits, excluding the active zone set, which are described in [Table 1-29](#). This keyword does not require an Admin session.

Table 1-29. Zoning Database Limits

Limit	Description
MaxZoneSets	Maximum number of zone sets (256)
MaxZones	Maximum number of zones (2000)
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 (2000), 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 informs 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	[Zoning Name]
-----	-----	-----	-----
MaxZoneSets	256	6	
MaxZones	2000	17	
MaxAliases	2500	1	
MaxTotalMembers	10000	166f	
MaxZonesInZoneSets	2000	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
		24	Q_1Photon1
		8	Q_1_NewJBOD1
		13	Q_1_Photon_1
		21	Q_2_NewJBOD2
		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

    wwn_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
    wwn_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:c3

Configured Zoning Information
ZoneSet      Zone      ZoneMember
-----
wnn

    wwn_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
    wwn_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:
```


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

Online help is available for the SANsurfer Switch Manager 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.

Click the **Help** button in SANsurfer Switch Manager windows to display context-sensitive help.

Fabric Management Workstation

The requirements for fabric management workstations running SANsurfer Switch Manager are described in [Table 2-1](#):

Table 2-1. Management Workstation Requirements

Component	Description
Operating System	<ul style="list-style-type: none"> • Windows® 2000, 2003, and XP • Solaris™ 8, 9, and 10 • Linux® Red Hat® EL 3.x • S.u.S.E® Linux 9.0 Enterprise
Memory	256 MB or more
Disk Space	150 MB per installation
Processor	500 MHz or faster
Hardware	CD-ROM drive, RJ-45 Ethernet port
Internet Browser	Microsoft® Internet Explorer® 5.0 and later Netscape Navigator® 4.72 and later Mozilla™ 1.02 and later Java 2 Run Time Environment to support the McDATA SANbrowser

Telnet workstations require an operating system with a Telnet client.

McDATA SANbrowser

The switch module contains a web server interface known as McDATA SANbrowser. This server enables a web-based client to establish a web-interface session with the Fibre Channel switch module. One instance of the McDATA SANbrowser 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 McDATA SANbrowser enabled, but you can disable it using the EmbeddedGUIEnabled parameter of the Set Setup System command. Refer to [“Set Setup Command” on page 1-74](#) for more information.

The McDATA SANbrowser possesses the same capabilities and features as the workstation-based SANsurfer Switch Manager with the following exceptions:

- Management is limited to a single fabric
- Zoning Wizard is excluded
- Performance Viewer 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.

SANsurfer Switch Manager 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 SANsurfer Switch Manager application provides two basic windows: Topology and Faceplate. The Topology and Faceplate windows 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 2-1.

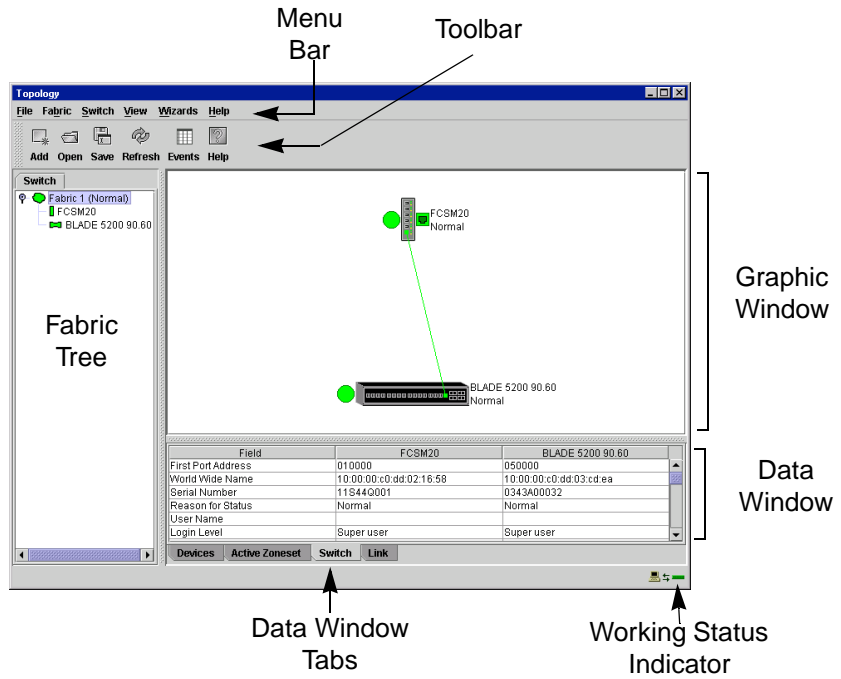


Figure 2-1. Topology Window

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 2-2. The Faceplate window for a 6-port Switch Module installed in a BladeCenter T unit is shown in Figure 2-2.

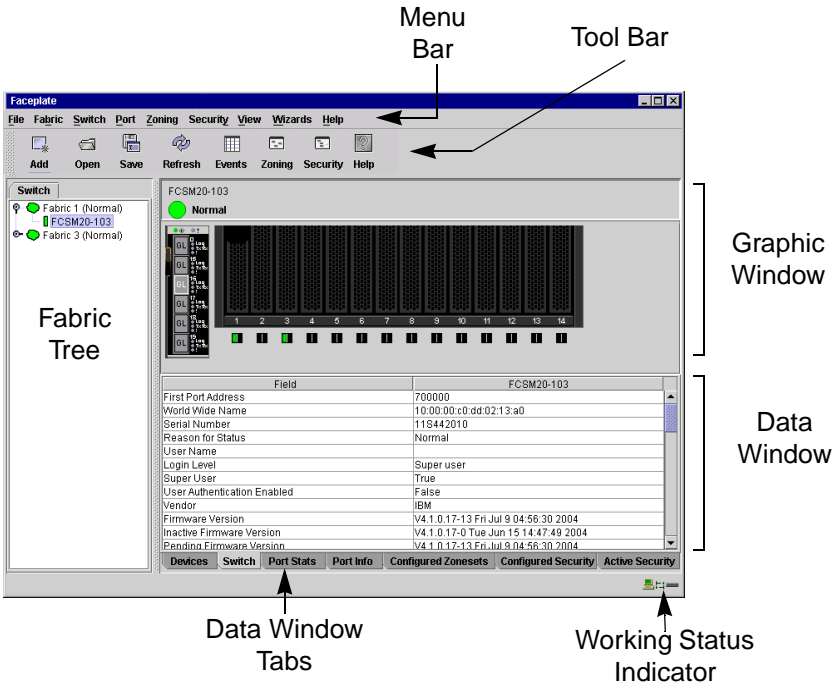


Figure 2-2. BladeCenter Faceplate Window

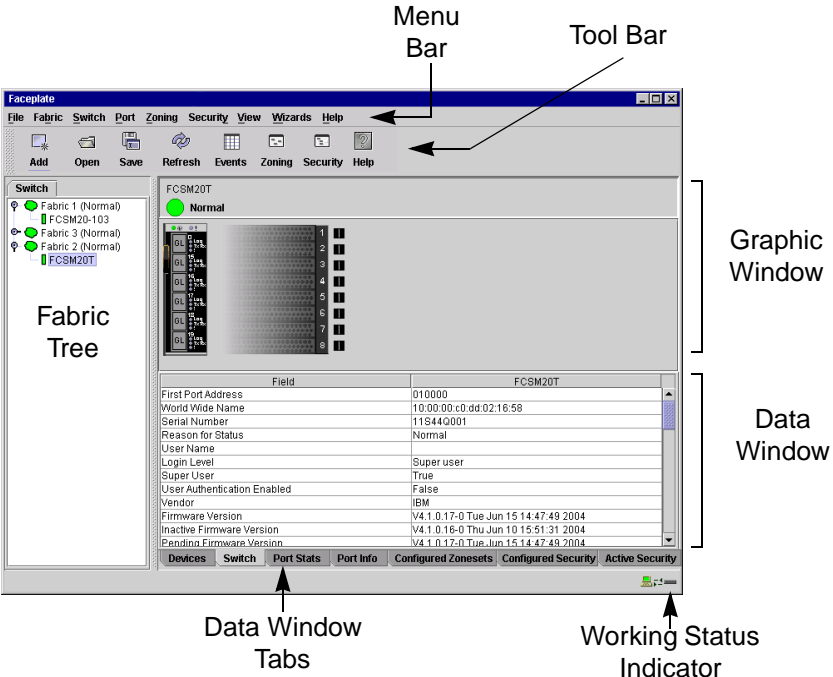


Figure 2-3. BladeCenter T Faceplate Window

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.

Topology Window Menu

The menu options available in the Topology window are shown in [Figure 2-4](#).

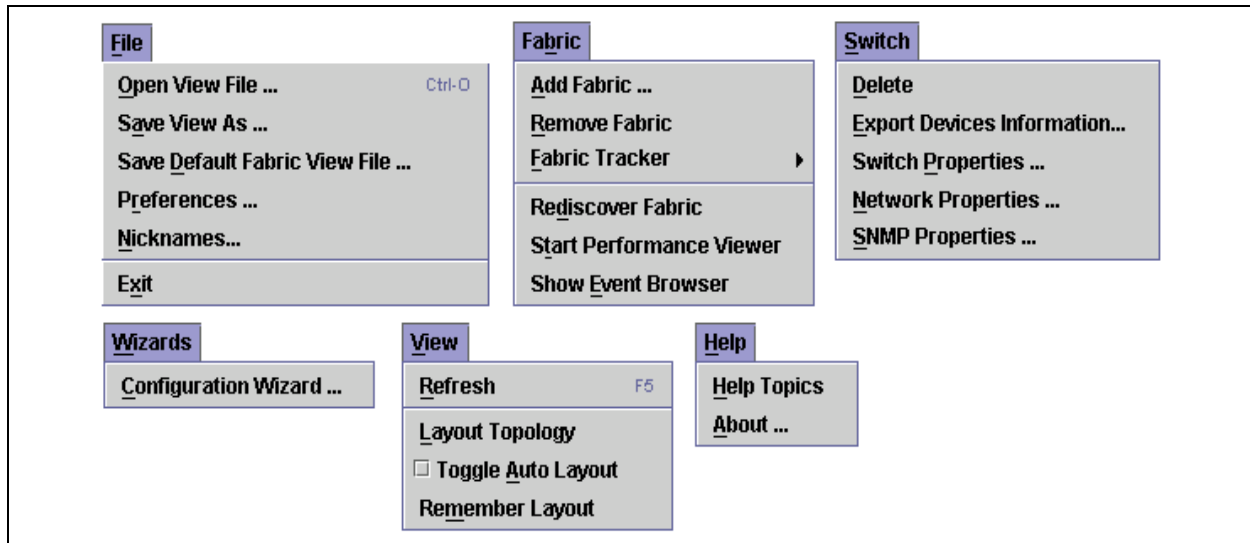


Figure 2-4. Topology Window Menu

Faceplate Window Menu

The menu options available in the Faceplate window are shown in [Figure 2-5](#).

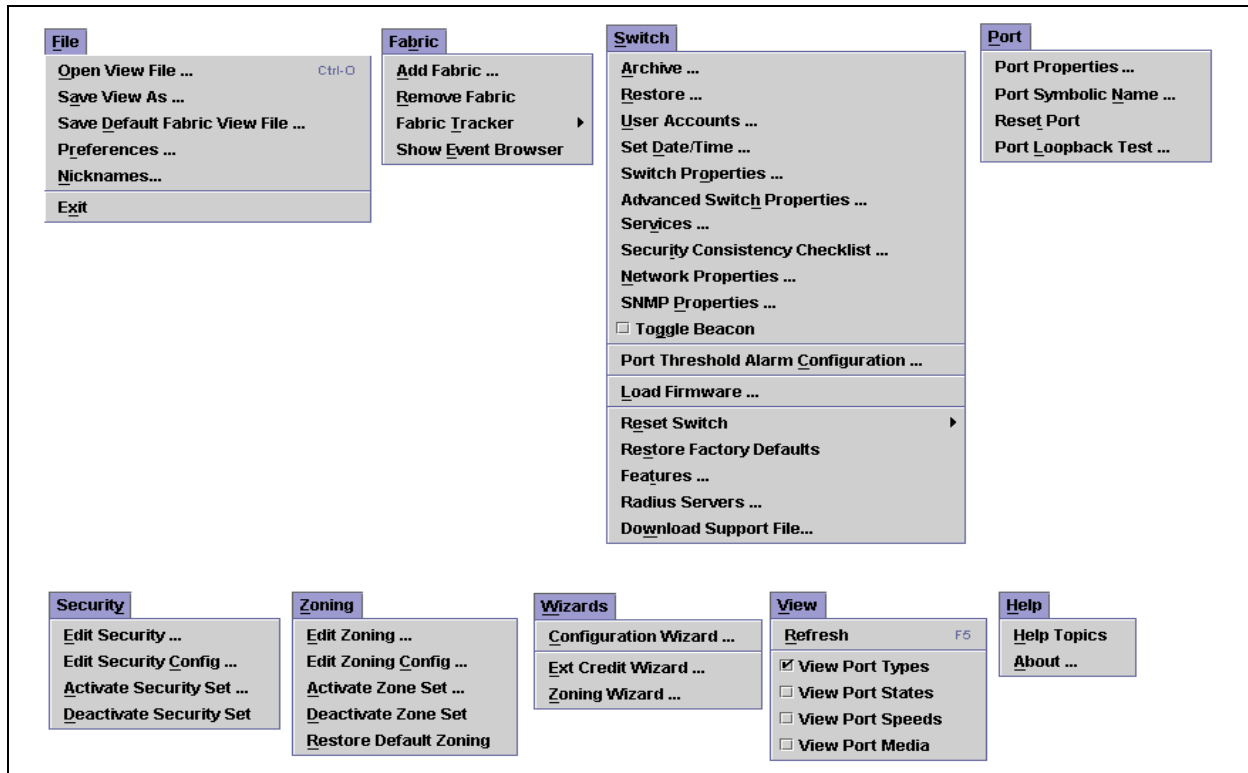


Figure 2-5. Faceplate Window Menu

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 2-15](#) for more information about these popup menus.









Topology Window Shortcut Keys

Shortcut key combinations, available in both the Topology and Faceplate windows, provide an alternative method of accessing menu options. The shortcut key combinations are not case-sensitive. For example, to close the application, press **Alt+F**, then press **X**.

Tool Bar

The tool bar consists of a row of graphical buttons that you can use to access SANsurfer Switch Manager functions as shown in [Table 2-2](#). 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 2-2. 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).
 Security	Edit Security	Opens the Edit Security window (Faceplate window only)
 Help	Help Topics	Opens the online help file.

Fabric Tree

The fabric tree lists the managed fabrics and their switches as shown in [Figure 2-6](#). 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.

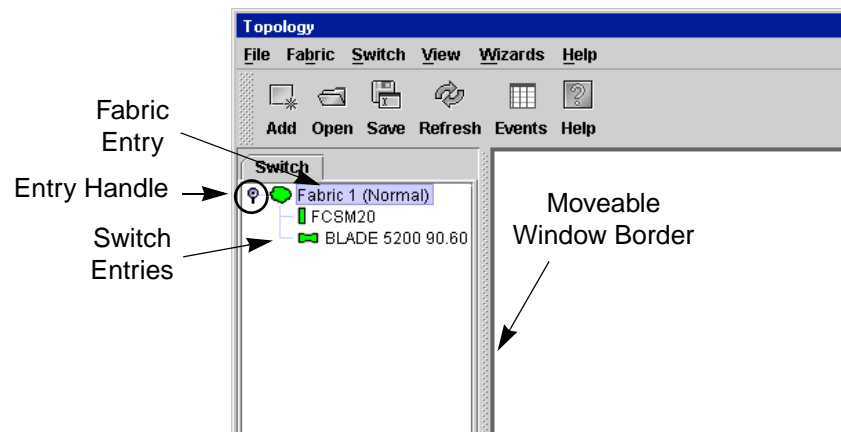


Figure 2-6. Fabric Tree

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.

Graphic Window

The graphic window shown in [Figure 2-1](#) 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.

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.

Working Status Indicator

The working status indicator, located in the lower right corner of the SANsurfer Switch Manager 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.

Using the Topology Window

The Topology window shown in [Figure 2-7](#) 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](#)

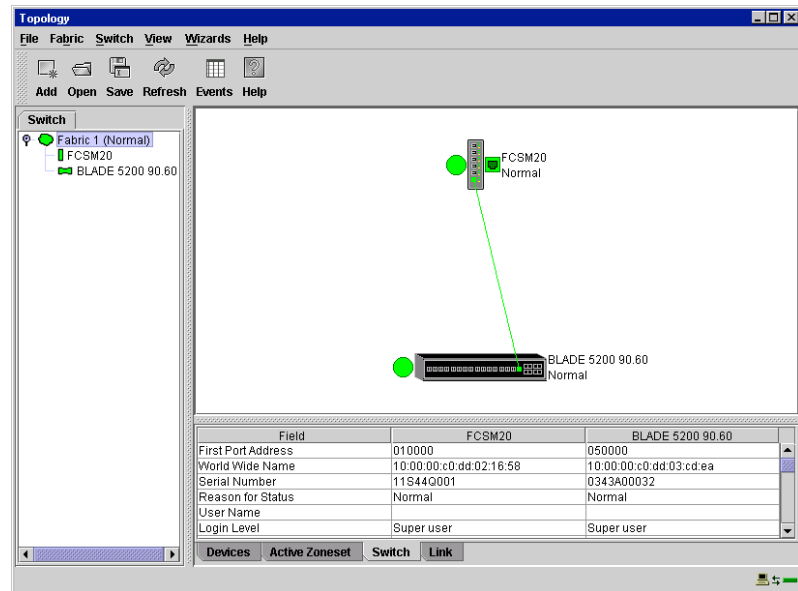


Figure 2-7. Topology Window

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 2-39](#) for more information about Topology window icons.

Table 2-3. 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

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 **Control** 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 2-4](#) for a list of switch module icons and vendors.

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 SANsurfer Switch Manager can arrange the icons when you select **Layout Topology**.

You can save a custom arrangement, or layout, and restore that layout during a SANsurfer Switch Manager 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**.

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.

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 2-73](#) 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 2-46](#) for more information about this data window. Refer to [“Zoning a Fabric” on page 2-50](#) 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 2-74](#) for more information.
- Link – displays information about the interswitch links. Refer to [“Link Data Window” on page 2-76](#) to for more information.

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 2-8](#) 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](#)

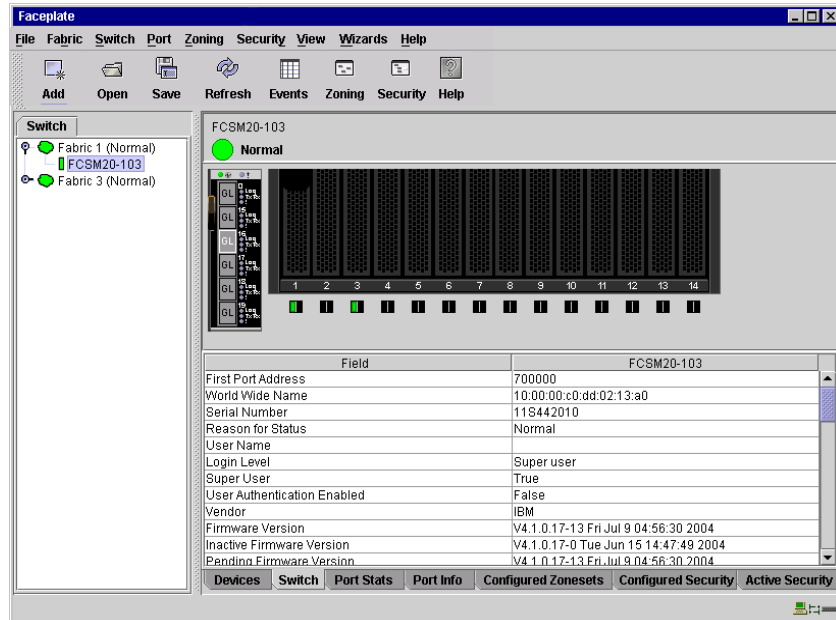


Figure 2-8. Faceplate Window

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 2-100](#) for more information about these displays.

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 SANsurfer Switch Manager 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.

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.

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.

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** tab to display all zone sets, zones, and zone membership in the zoning database.
- **Configured Security** – Click the **Configured Security** tab to display all security definitions currently saved in the database.
- **Active Security** – Click the **Active Security** tab to display the active security set.

Configuring the SANsurfer Switch Manager Environment

You can configure your SANsurfer Switch Manager environment through the use of fabric view files and SANsurfer Switch Manager preferences.

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 SANsurfer Switch Manager session. In addition to the SANsurfer Switch Manager 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.

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.

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.

Changing the Encryption Key

To change the encryption key for the SANsurfer Switch Manager 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.

Setting SANsurfer Switch Manager 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 SANsurfer Switch Manager 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 SANsurfer Switch Manager session and prompts you to load a fabric view file upon opening a SANsurfer Switch Manager session.
- Enable (default) or disable the use of the Initial Start window at the beginning of a SANsurfer Switch Manager session.
- Enable (default) or disable the Event Browser. Refer to [“Displaying the Event Browser” on page 2-42](#). If the Event Browser is enabled using the Preferences window as shown in [Figure 2-9](#), the next time SANsurfer Switch Manager is started, all events will be displayed. If the Event Browser is disabled when SANsurfer Switch Manager is started and later enabled, only those events from the time the Event Browser was enabled and forward will be displayed.

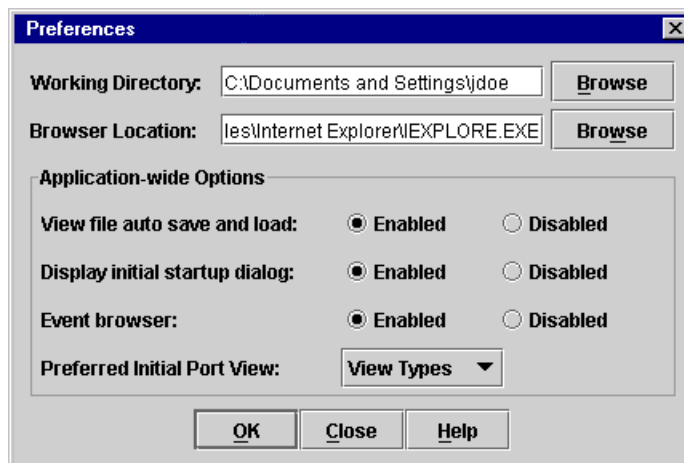


Figure 2-9. Preferences Window – SANsurfer Switch Manager

- 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 2-101](#)
 - [“Displaying Port Operational States” on page 2-101](#)
 - [“Displaying Port Speeds” on page 2-102](#)
 - [“Displaying Transceiver Media Status” on page 2-102](#)

To set preferences for your SANsurfer Switch Manager 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.

Managing Fabrics

This section describes the following tasks that manage fabrics:

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

RADIUS Servers

Remote Authentication Dial In User Service (RADIUS) provides a method to centralize the management of authentication passwords in larger networks. It has a client/server model, where the server is the password repository and third party authentication point and the clients are all of the managed devices. RADIUS can be configured for devices and/or user accounts. The RADIUS server windows are available only on a secure (SSL) fabric and on the entry switch (out of band switch).

RADIUS is designed to authenticate users and devices using a challenge/response protocol. Basic implementations consist of a central RADIUS server containing a database of authorized users as well as authentication information. A RADIUS client wishing to verify the authenticity of a user issues a challenge to the user and collects the response to the challenge. This information is forwarded to the RADIUS server for authentication and the server responds with the results, either an accept or reject. The RADIUS client does not need to be configured with any user authentication information, this all resides on the RADIUS server and can be managed centrally and separately from the clients. In addition, no passwords are exchanged between the RADIUS server and its clients. Authentication of requests from a RADIUS client to the server and responses from the server to a client can also be authenticated. This requires sharing a secret between the server and client. The accounting RADIUS supports the auditing of the users and switch services such as Telnet, FTP, and switch management applications.

Adding a RADIUS Server

When you add a RADIUS server, you provide a method to centralize the management of authentication passwords over a network.

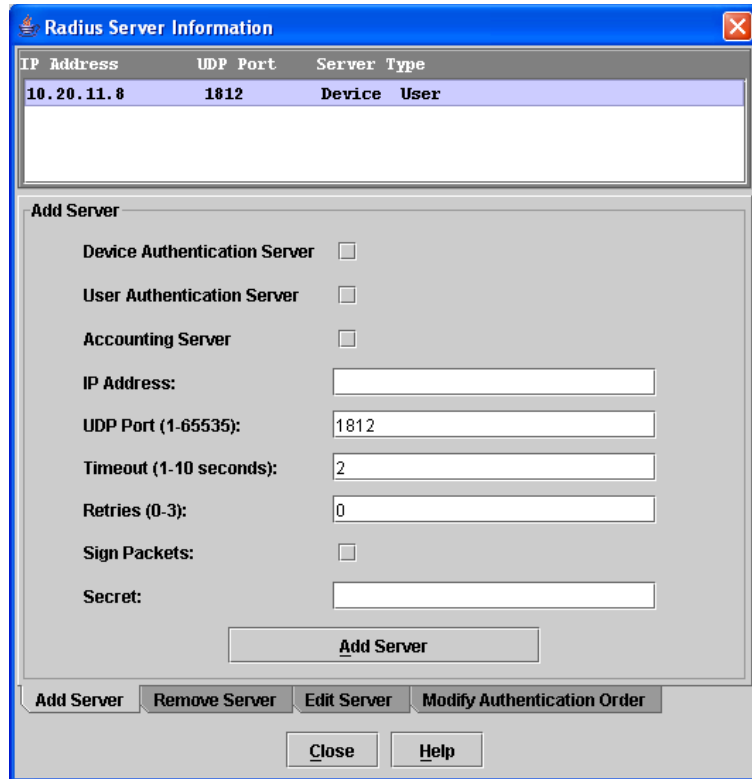


Figure 2-10. Add Server

To add a RADIUS server, do the following:

1. Open the Faceplate window, open the Switch menu, and select **Radius Servers....**
2. In the Radius Server Information window, shown in [Figure 2-10](#), click the **Add Server** tab.
3. Select the server type (Device, User, Account).

NOTE: Device authentication (Device checkbox) is available only with the SANtegrity Enhanced PFE key. For additional information about McDATA Product Features Enabled, please contact your McDATA representative or visit the McDATA website at www.mcddata.com.

4. In the IP Address field, enter the remote IP address of the server.
5. In the UDP Port field, enter the remote UDP port number of the Authentication RADIUS Server. The RADIUS Accounting Server UDP port will always be the value of Device/User Authentication Server UDP Port + 1.
6. In the Timeout field, enter the timeout value in seconds (minimum of 1 second, maximum of 30 seconds). This is the number of seconds the RADIUS client will wait for a response from the RADIUS server before retrying, or giving up on a request.

7. In the Retries field, enter the the number of retries. This is the maximum number of times the RADIUS client will retry a request sent to the primary RADIUS server.
8. Select the Sign Packet check box to enable the switch to include a digital signature (Message-Authenticator) in all RADIUS access request packets sent to the RADIUS server. A valid Message-Authenticator attribute will be required in all RADIUS server responses.
9. In the Secret field, enter the server secret. A secret is required for all RADIUS servers. The secret is used when generating and checking the Message-Authenticator attribute.
10. Click the **Add Server** button to add the server, and click the **Close** button to close the window.
11. Click the **Modify Authentication Order** tab, and verify that Device Authentication Order and User Authentication Order options are set to either **Radius** or **Radius Local** for RADIUS Authentication to be implemented.

Removing a RADIUS Server

When you remove a RADIUS server, you disable the management of authentication usernames and passwords over the network for that server.

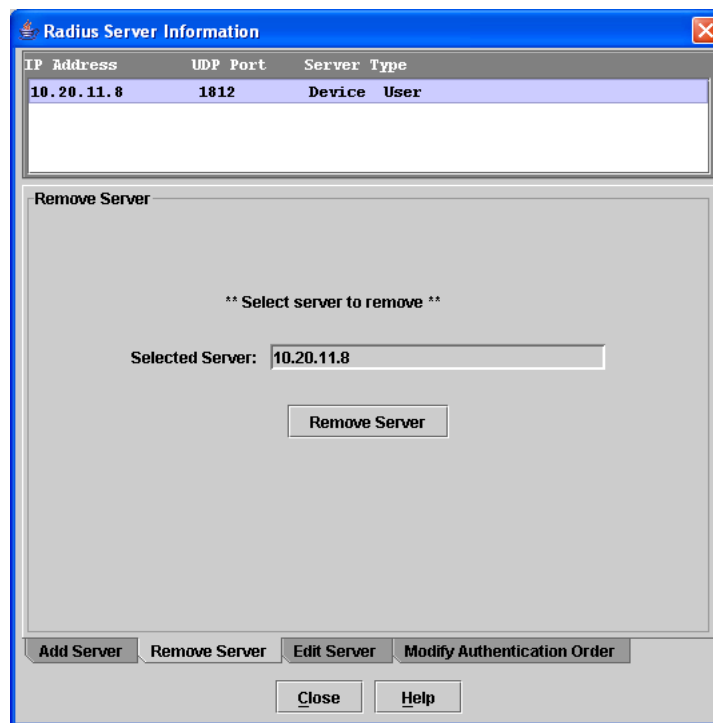


Figure 2-11. Remove Server

To remove a RADIUS server, do the following:

1. Open the Faceplate window, open the Switch menu, and select **Radius Servers....**
2. In the Radius Server Information window, shown in [Figure 2-11](#), click the **Remove Server** tab.

3. In server list at the top of the window, select the server to be removed.
4. Click the **Remove Server** button to remove the server, and click the **Close** button to close the window.

Editing RADIUS Server Information

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

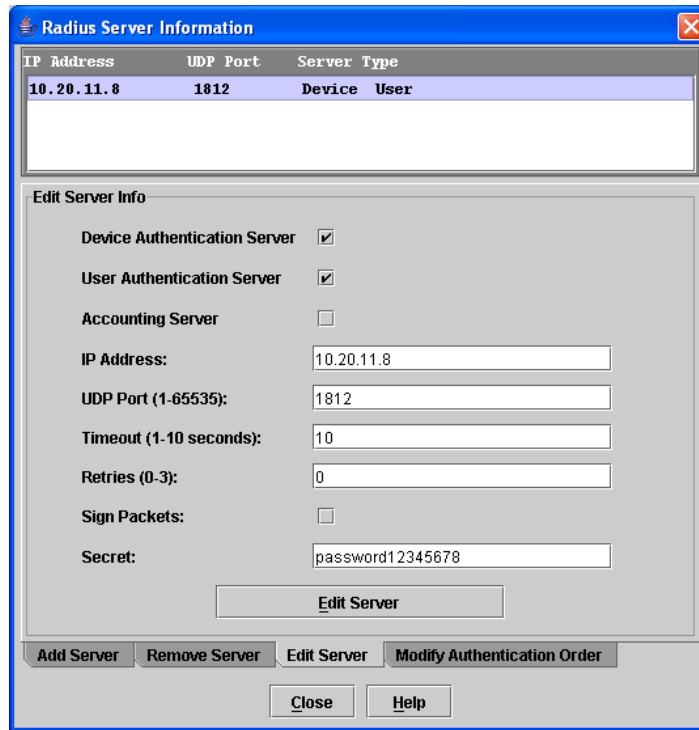


Figure 2-12. Edit Server Information

To edit information of a RADIUS server, do the following:

1. Open the Faceplate window, open the Switch menu, and select **Radius Servers...**
2. In the Radius Server Information window, shown in [Figure 2-12](#), click the **Edit Server** tab.
3. In server list at the top of the window, select the server to be edited.
4. Make changes to the IP Address, UDP Port, Timeout, Retries, and Secret fields.
5. Select or unselect the server type (Device, User, Account) and Sign Packet check boxes.

NOTE: Device authentication (Device checkbox) is available only with the SANtegrity Enhanced PFE key. For additional information about McDATA Product Features Enabled, please contact your McDATA representative or visit the McDATA website at www.mcdata.com.

6. Click the **Edit Server** button to save the changes, and click the **Close** button to close the window.

Modifying Authentication Order

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

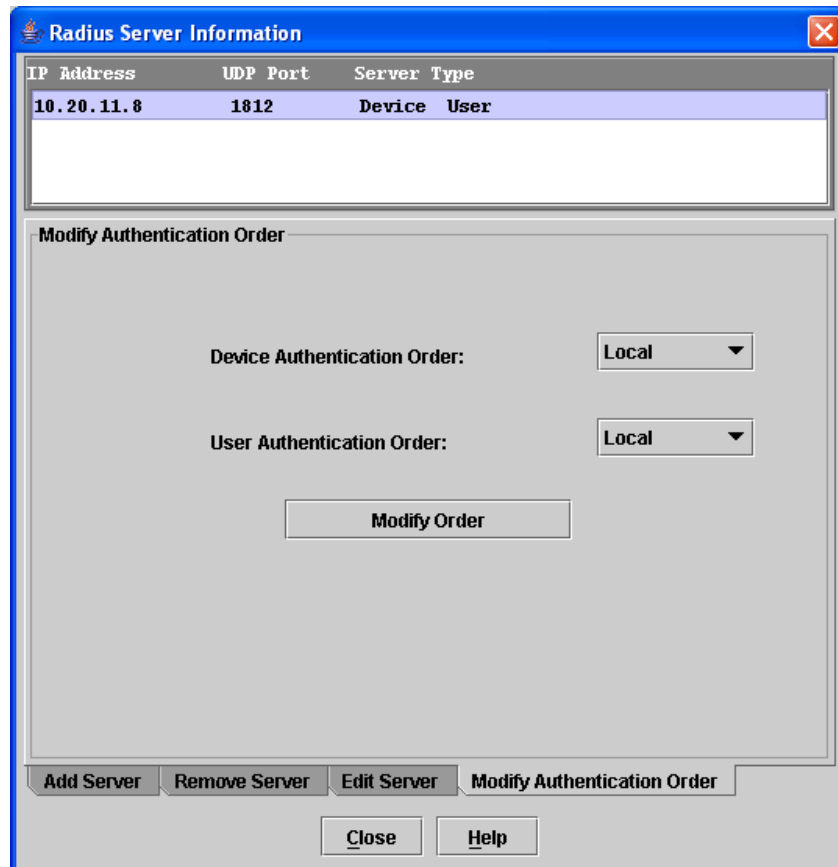


Figure 2-13. Modify Authentication Order - RADIUS Server Information

To modify the authentication order information of a RADIUS server, do the following:

1. Open the Faceplate window, open the Switch menu, and select **Radius Servers...**
2. In the Radius Server Information window, shown in [Figure 2-13](#), click the **Modify Authentication Order** tab.
3. In server list at the top of the window, select the server to be modified.
4. Make changes to the Device Authentication Order or User Authentication Order pull-down menus. Select **Local**, **Radius**, or **Radius Local**.

Click the **Modify Order** button to save the changes, and click the **Close** button to close the window.

Securing a Fabric

The components of Fibre Channel fabric security are:

- [Connection Security](#)
- [User Account Security](#)
- [Security Consistency Checklist](#)
- [Device Security](#)
- [Fabric Services](#)

Connection Security

Connection security provides an encrypted data path for switch management methods. The switch supports the Secure Shell (SSH) protocol for the command line interface and the Secure Socket Layer (SSL) protocol for management applications such as SANsurfer Switch Manager and Common Information Module (CIM).

The SSL handshake process between the workstation and the switch involves the exchanging of certificates. These certificates contain the public and private keys that define the encryption. The switch certificate is valid for one year beginning with its creation date and time. The workstation validates the switch certificate by comparing the workstation date and time to the switch certificate creation date and time. For this reason, it is important to synchronize the workstation and switch with the same date, time, and time zone. If a certificate has not been created by the user, the switch will automatically create one.

Consider your requirements for connection security: for the command line interface (SSH), management applications such as SANsurfer Switch Manager (SSL), or both. If SSL connection security is required, also consider using the Network Time Protocol (NTP) to synchronize workstations and switches.

User Account Security

User account security is the process by which your user account and password are authenticated with the list of valid user accounts and passwords. The switch validates your account and password when you attempt to add a fabric using SANsurfer Switch Manager or log in to a switch through Telnet. Your system administrator defines accounts, passwords, and authority levels that are stored on the switch.

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 SANsurfer Switch Manager in-band and out-of-band logins, Application Programming Interface (API) in-band and out-of-band logins, and Telnet logins.

The Admin account possesses Admin authority which grants full access to all tasks of the SANsurfer Switch Manager menu system. The switch validates your user account and SANsurfer Switch Manager 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 SANsurfer Switch Manager 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.

Security Consistency Checklist

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

Device Security

NOTE: Device security is available only with the McDATA SANtegrity Enhanced Product Features Enabled (PFE) key. Refer to “[Upgrading the Switch Using PFE Keys](#)” on page 2-97 for information about installing a PFE key. For additional McDATA PFE keys, please contact your McDATA representative or visit the website at www.mcddata.com.

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

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

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

Consider the devices, switches, and management agents and evaluate the need for authorization and authentication. Also consider whether the security database is to be distributed on the switches or centralized on a RADIUS server and how many servers to configure.

Managing device security involves the following tasks:

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

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

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

Edit Security

The Edit Security window shown in [Figure 2-14](#) opens after clicking the **Security** button on the toolbar or selecting Edit Security from the Security menu. The Security windows are available only on a secure (SSL) fabric and on the entry switch (out of band switch). The primary use of the Edit Security window is to edit the security configuration on the switch. You can also open and edit a security configuration saved to a file. Editing security files consists of renaming and removing security sets, groups, and members.

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

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

- ISL - default (E_Port authentication)
- MS (Management Server CT authentication)
- Port (F_Port authentication)

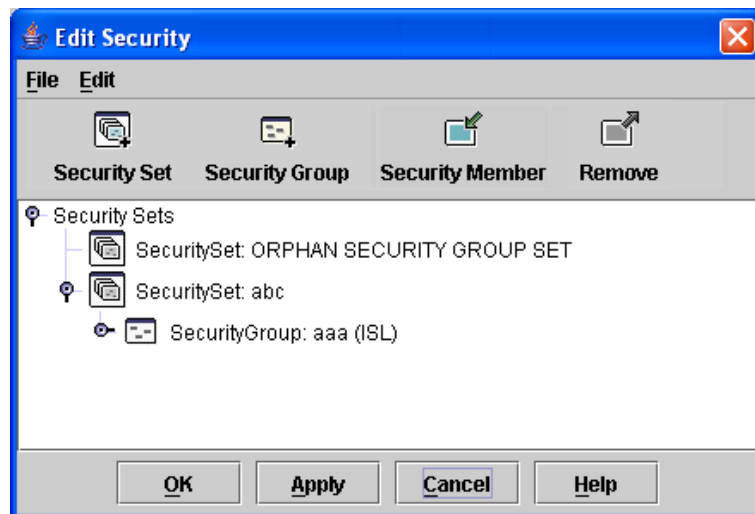


Figure 2-14. Edit Security Window

Use the File menu to:

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

Use the Edit menu to:

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

Creating a Security Set

There is a maximum of 4 security sets. To add a security set, do the following:

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

Create Security Group

Use the Create Security Group window shown in [Figure 2-15](#) to add a security group to a security set. The Create Security Group window is displayed after clicking the **Security Group** button on the toolbar, or after you right-click on a security set in the graphic window and select **Create a Security Group** from the popup menu.



Figure 2-15. Create Security Group Window

The naming conventions for all security groups are listed below.

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

Creating a Security Group

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

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

Create Security Group Member

Use the Create Security Group Member window shown in [Figure 2-16](#) to add a member to a security group. Choose options from the Group Member (or manually type in a hex value) and Authentication pull-down menus, and enter values in the Secret and Binding (ISL groups only) fields.

Figure 2-16. Create a Security Group Member Window

The conventions for ISL security group members are listed below:

- You can enter member world-wide name (WWN), which must be 16 hex characters, or 23 characters with valid WWN format `xx:xx:xx:xx:xx:xx:xx:xx`.
- The authentication choices are None and Chap.
- The Secret field is disabled if authentication is set to None. If authentication is Chap, the Secret field is enabled.
- The **Generate** button is only enabled when authentication is set to Chap.
- Valid binding entries are between 0 to 239.

The conventions for Port security group members are listed below:

- You can enter member world-wide name (WWN), which must be 16 hex characters, or 23 characters with valid WWN format `xx:xx:xx:xx:xx:xx:xx:xx`.
- The authentication choices are None and Chap.
- The Secret field is disabled if authentication is set to None. If authentication is Chap, the Secret field is enabled.
- The **Generate** button is only enabled when authentication is set to Chap.

The conventions for MS security group members are listed below:

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

Creating a Security Group Member

To add a member to a security group, do the following:

1. On the Faceplate window, click the **Security** button on the toolbar, or open the Security menu and select **Edit Security** to open the Edit Security window.
2. Choose one of the following methods to open the Create a Security Group Member window:
 - In the graphic window, click a security group and click the **Security Member** button in the toolbar.
 - Right-click on a security group and select **Create Members** from the popup menu.
3. Open the Group Member pull-down menu and select a Node World-Wide Name. The switch must be a member of any group in which authentication is used. You can also type in a hex value.
4. Open the Authentication pull-down menu, and select a type of protocol to be used for the authentication process for that member.
 - ISL authentication options are None (0 bytes), Chap (16 bytes)
 - MS (CT - Common Transport) authentication options are None (0 bytes), MD5 (16 bytes), SHA (20 bytes)
 - Port authentication options are None (0 bytes), Chap (16 bytes)
5. In the Secret area, enter an authentication "password" to be assigned that member. Or, you can click the **Generate** button to randomly generate a secret.
6. In the Binding field (ISL groups only), enter the domain ID (1-239) for the switch for the ISL group member. The WWN of the switch must be at the entered domain ID when attempting to enter the fabric, otherwise it will become isolated.
7. Click the **OK** button to save the changes.

Editing the Security Configuration on a Switch

To edit a security configuration on the switch, do the following:

1. On the Faceplate window, click the **Security** button on the toolbar, or open the Security menu and select **Edit Security** to open the Edit Security window. By default, the security configuration on the switch is displayed in the Edit Security window. To edit a security configuration saved to a file, open the File menu and select **Open File**, or press **Control+o** (letter o) to open the Open window. Browse for and select the security file, and click the **Open** button to display the security file in the Edit Security window.
2. Select the security item to edit in the graphic window, and choose one of the following:
 - **Rename a Security Set, or Group.** Open the Edit menu and select a Rename option. In the Rename window, enter a new name and click the **OK** button to save the changes.
 - **Edit Security Group Member.** Open the Edit menu and select a Edit Security Group Member option. In the Edit Security Group Member window, enter a new Group Member (WWN), choose an option in the Authentication pull-down menu, and click the **OK** button to save the changes.
 - **Remove a Security Set, Group, or Member.** Select the item to remove, open the Edit menu and select a Remove option. In the Remove window, click the **OK** button to remove that item from the security file and save the changes.
 - **Clear Security.** Select the Security Sets directory name, open the Edit menu and select **Clear Security**. In the Remove window, click the **OK** button to remove all security sets and save the changes. You can also right-click on the Security Sets (top level) directory name, and select **Clear Security** from the popup menu, and click the **OK** button to remove all security sets.
3. Click the **Apply** button to save the changes and keep the Edit Security window open. To save changes and close the Edit Security window in one step, click the **OK** button.
4. Click the **OK** button to close the Edit Security window.

Viewing Properties of a Security Set, Group, or Member

To view the properties of a security set, group, or member, do the following:

1. On the Faceplate window and click the **Security** button on the toolbar, or open the Security menu and select **Edit Security** to open the Edit Security window.
2. Choose one of the following:
 - Select a security set, group, or member, open the Edit menu and select **Properties**.
 - In the graphic window, right-click on the security item, and select **Properties** from the popup menu.
3. View the security information for the selected item in the Properties window.

Using the Security Config

Use the Security Config window shown in [Figure 2-17](#) to save the active security configuration on the switch to non-volatile or to temporary memory, and to require the domain ID of a switch be validated before attaching to the fabric.

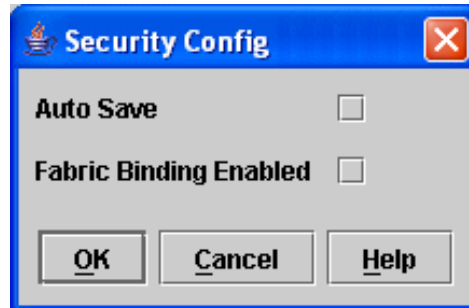


Figure 2-17. Security Config Window

To configure security on the switch, do the following:

1. On the Faceplate window, open the Security menu and select **Edit Security Config** to open the Security Config window.
2. Check the **Auto Save** check box to enable (default) or disable Auto Save mode. If enabled, the security configuration is saved to non-volatile memory on the switch. If disabled, the security file is saved only to temporary memory. The Auto Save feature is used when Fabric Binding is enabled. When Auto Save is disabled, any updates from remote switches will not be saved locally. If the local switch is reset, it may isolate.
3. Check the **Fabric Binding Enabled** check box to require the expected domain ID of a switch is verified before being allowed to attach to the fabric.

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

4. Click the **Apply** button to save the settings.
5. Click the **OK** button to close the Security Config window.

Archiving a Security Configuration to a File

To archive (save) a security configuration to a file, do the following:

1. On the Faceplate window, click the **Security** button on the toolbar, or open the Security menu and select **Edit Security** to open the Edit Security window.
2. Configure the security settings as desired.
3. Open the File menu and select **Save As**.
4. In the Save window, enter a name and location for the security file (.xml extension).
5. Click the **Save** button to save the security file.

Activating a Security Set

Only one security set can be active at one time. To activate a security set, do the following:

1. On the Faceplate window, open the Security menu and select **Activate Security Set** to open the Activate Security Set window.
2. In the Activate Security Set window, select a security set from the pull-down menu.
3. Click the **Activate** button to activate the security set.

Deactivating a Security Set

Only one security set can be active at one time. To deactivate an active security set, do the following:

1. In the Faceplate window, open the Security menu and select **Deactivate Security Set**.

In the Deactivate window, click the **Yes** button to confirm that you want to deactivate the active security set.

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 3-4](#) for more information. SNMP is enabled by default.

In-band management is the ability to manage switch modules across interswitch links using SANsurfer Switch Manager, 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 2-86](#) for more information.

Tracking Fabric Version Information

The Fabric Tracker option 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, SANsurfer Switch Manager version, switch active firmware version, device hardware, drivers, and firmware version from FDML.

The Snapshot Analyzer option 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.

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 2-18](#) 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 close 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.

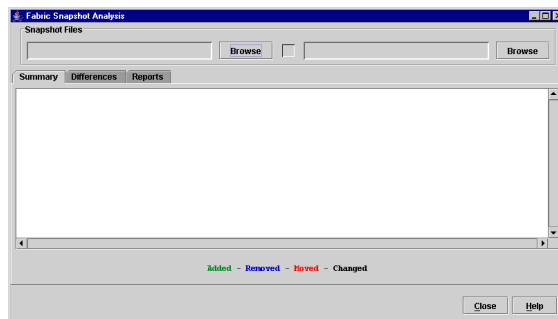


Figure 2-18. Fabric Version Snapshot Analysis Window

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.

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.

Managing the Fabric Database

A fabric database contains the set of fabrics that you have added during a SANsurfer Switch Manager 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](#)

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 2-19](#).

Figure 2-19. Add a New Fabric Window

2. Enter a fabric name (optional) and the IP address of the switch through which to manage the fabric.
3. Enter an account name and password. The factory account name and password are "admin" and "password". A password must have a minimum of 8 characters and no more than 20. The password is for the switch and is stored in the switch firmware. Refer to [“Managing User Accounts” on page 2-67](#) for information about creating user accounts.
4. Click the **Add Fabric** button.

A switch 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 SANsurfer Switch Manager inband and out-of-band logins, Application Programming Interface (API) inband and out-of-band logins, and Telnet logins. Additional logins will be refused.

If the entry switch has SSL (Secure Socket Layer) enabled, the switch will generate and display a Verify Certificate window that you must accept before gaining access to the fabric. Refer to [“Connection Security” on page 2-24](#) and [“System Services Window” on page 2-88](#) for more information on certificates and SSL.

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**.

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.

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 2-57.](#)

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**.

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 *McDATA 6-Port Fibre Channel Switch Module for IBM Eserver BladeCenter Installation Guide*.
2. Install the new replacement fibre channel switch module. For more information, see the *McDATA 6-Port 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**.
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 2-91.](#)
6. Click **OK** to write the configuration file to the switch module.

Deleting Switches and Links from the Topology Window

The SANsurfer Switch Manager 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 SANsurfer Switch Manager 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**.

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 2-45](#) and [“Switch Data Window” on page 2-74](#) for information about the Devices and Switch data windows.

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 2-4](#) 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 2-4](#). Switches that are not manageable through SANsurfer Switch Manager are displayed as third-party unmanageable switch icons.

Table 2-4. Topology Window Switch and Status Icons















Switch Icon	Description
	McDATA 6-Port Fibre Channel Switch Module for a BladeCenter unit
	McDATA 6-Port 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 SANsurfer Switch Manager. Use the management application that was shipped with this switch.
	Switch communication normal (green)
	Switch operational with errors (amber)
	Switch status critical–potential failure (red)
	Switch communication status unknown, unreachable, or unmanageable (blue)

Table 2-4. Topology Window Switch and Status Icons (Continued)

Switch Icon	Description
	Fabric management switch Ethernet connection normal (green)
	Fabric management switch Ethernet connection warning (amber)
	Fabric management switch Ethernet connection critical (red)

Displaying the Event Browser

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

Entries in the Event Browser shown in [Figure 2-20](#) are formatted by severity, time stamp, source, type, and description. The maximum number of entries allowed in the Event Browser is 10,000. The maximum number of entries allowed on a switch is 1200. Once the maximum is reached, the event list wraps and the oldest events are discarded and replaced with the new events. Event entries from the switch, use the switch time stamp, while event entries generated by the application 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 switch management application is running.

If the Event Browser is enabled using the Preferences dialog, the next time the switch management application is started, all events from the switch log will be displayed. If the Event Browser is disabled when switch management application 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 SANsurfer Switch Manager Preferences”](#) on page 2-17.

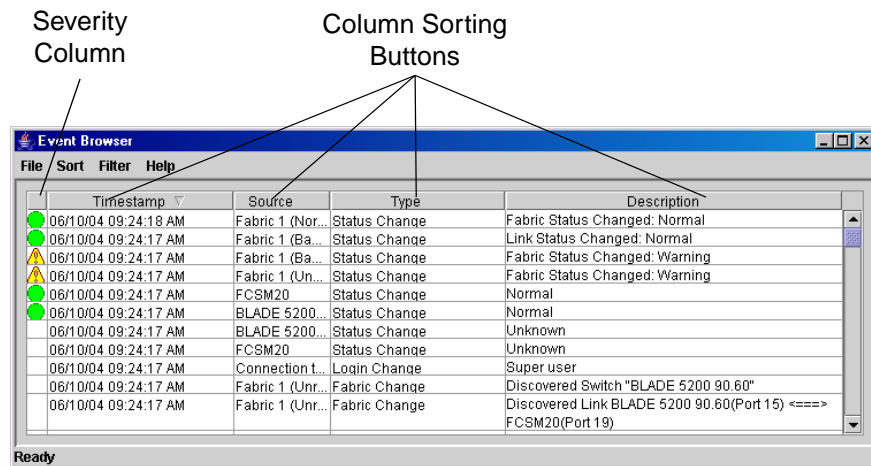





Figure 2-20. Events Browser

Severity is indicated in the severity column using icons as described in [Table 2-5](#).

Table 2-5. Severity Levels

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

NOTE: Events (Alarms, Critical, Warning, and Informative) generated by the application are not saved on the switch. They are permanently discarded when you close a SANsurfer Switch Manager session, but you can save these events to a file on the workstation before you close SANsurfer Switch Manager and read it later with a text editor or browser.

NOTE: Events generated by the switch are stored on switch, and will be retrieved when the application is restarted. Some alarms are configurable. Refer to "Configuring Port Threshold Alarms" on page 3-83.

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 2-21](#). 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, 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.

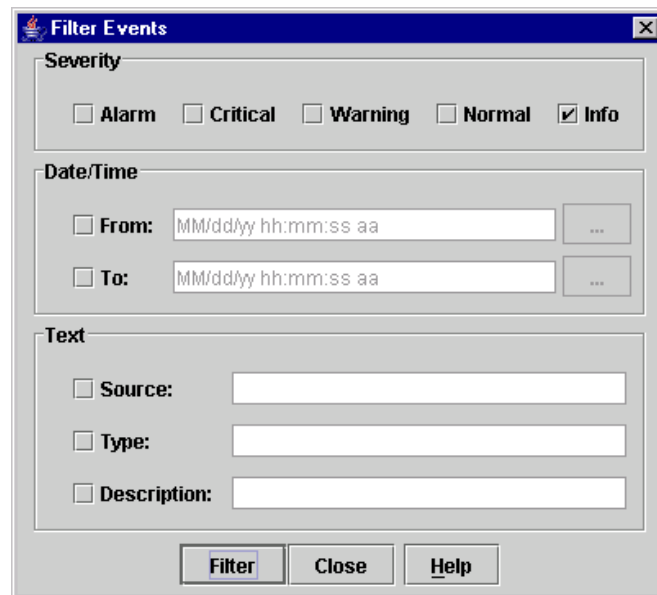


Figure 2-21. Filter Events Window

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 sorts of the same type alternate between ascending and descending order.

Saving the Event Browser to a File

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

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

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 2-6](#) describes the entries in the Devices data window. Refer to [“Exporting Device Information to a File” on page 2-47](#) for exporting device information.

Table 2-6. 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 2-48 for more information.
Details	Click the (i) to display additional detail about the device. Refer to “Displaying Detailed Device Information” on page 2-47 .
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 #	Row number reference for each listing in the Devices data window table.

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 2-77](#) for information about the zone set definitions on a particular switch. Refer to [“Zoning a Fabric” on page 2-50](#) for more information about zone sets and zones.

The Active Zoneset data window shown in [Figure 2-22](#) 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.

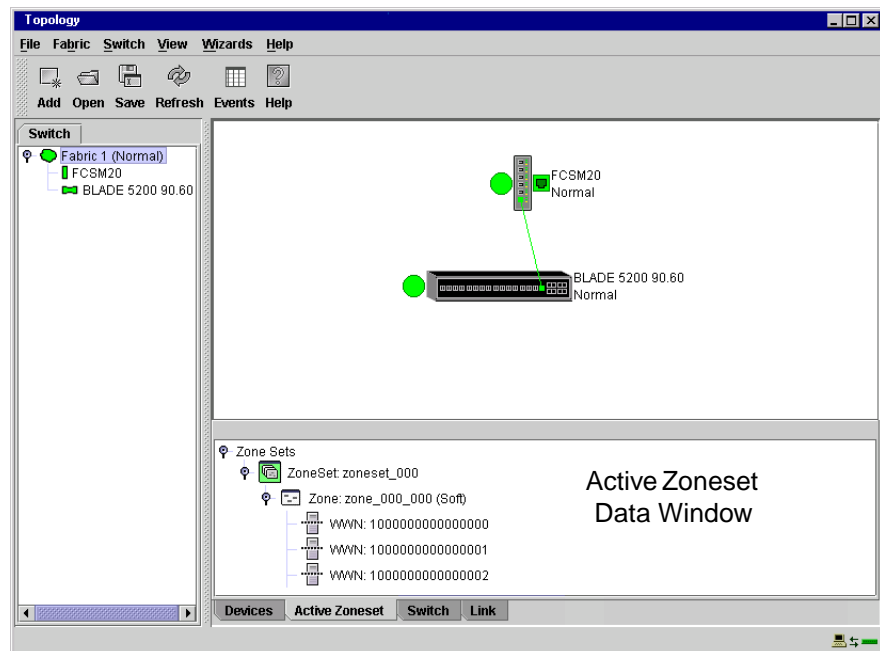


Figure 2-22. Active Zone Set Data Window

Working with Device Information and Nicknames

SANsurfer Switch Manager enables you to do the following tasks:

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

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 2-23](#).

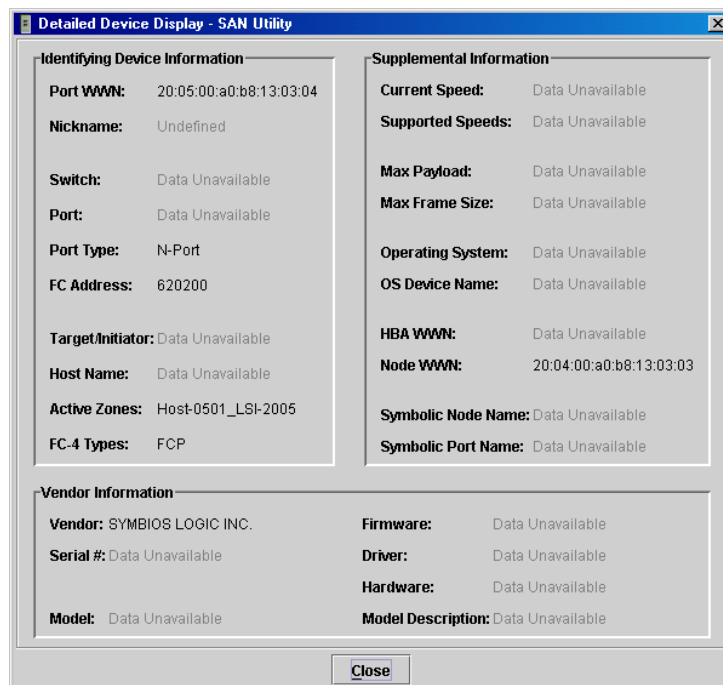


Figure 2-23. Detailed Devices Display Window

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.

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.

SANsurfer Switch Manager 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.

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 close 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 2-45](#).

Editing a Nickname

A nickname must start with a letter and can have up to 64 characters. Valid characters include alphanumeric characters [aA-zZ][0-9] and special symbols [\$ _ - ^]. You can access the Edit Nicknames window two ways. Choose one of the following methods to edit a nickname:

- In the Topology or Faceplate window, open the File menu and select **Nicknames** to open the Nicknames window. The device entries are listed in table format.
 - Click on a device entry in the table. Open the Edit menu and select **Edit Nickname** to open the Edit Nicknames window. Edit the nickname in the text field. Click the **OK** button to save the changes.
 - Double-click a cell in the **Nicknames** or **WWN** columns, and edit the nickname in the text field. Click the **OK** button to save the changes.

In the Topology or Faceplate window, click the **Devices** tab to display the Devices data window. Double-click a cell in the **Nickname** column to open the Edit Nickname window. Edit the nickname in the text field. Click the **OK** button to save the changes. Refer to [“Devices Data Window” on page 2-45](#) for more information.

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**.

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**.

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 SANsurfer Switch Manager. 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**.

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, Default Visibility, Default Zone, and Discard Inactive zoning configuration parameters using SANsurfer Switch Manager or the Set Config Zoning command. See [“Interop Auto Save” on page 2-57](#) for information about the Auto Save parameter, see [“Default Visibility” on page 2-57](#) for information about the Default Visibility parameter, and see [“Set Config Command” on page 1-59](#) for information about the Set Config Zoning command.

- [Zoning Concepts](#)
- [Using the Zoning Wizard](#)
- [Managing the Zoning Database](#)
- [Managing Zone Sets](#)
- [Managing Zones](#)
- [Managing Aliases](#)
- [Merging Fabrics and Zoning](#)

Zoning Concepts

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

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

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 (domain/port member only or it will revert back to a soft zone when activated)

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.

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.

Aliases

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

Zone Sets

A zone set is a named group of zones. A zone can be a member of more than one zone set. 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 2-77](#) for information about displaying the zoning database.

The orphan zone set is created by the application automatically to hold the zones which are not in any set. The orphan zone set cannot be removed and is not saved on the switch.

To apply zoning to a fabric, 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 2-46](#) for information about displaying the active zone set.

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.

The configuration parameters that affect the zoning database are Auto Save, Default Visibility, Default Zone, and Discard Inactive. 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 2-57](#) 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 2000.** 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 2000.** 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.

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.

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](#)

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 2-24](#). Changes can only be made to inactive zone sets, which are stored in flash (non-volatile) memory and retained after resetting a switch module.

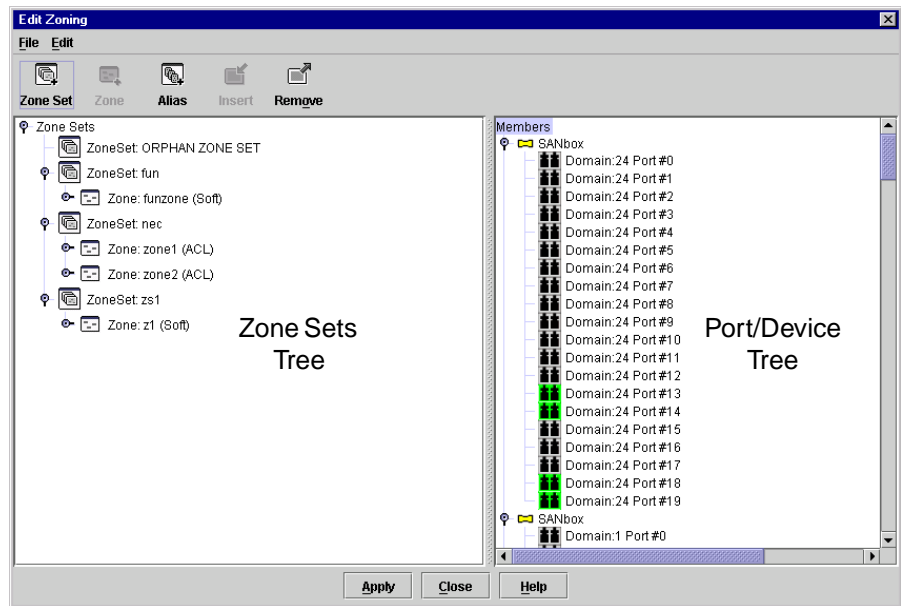


Figure 2-24. Edit Zoning Window

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 Interop Auto Save parameter is enabled on the Advanced 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.

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 SANsurfer Switch Manager 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.

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 2-7](#) describes the zoning tool bar operations.

Table 2-7. 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

Configuring the Zoning Database

Use the Zoning Config window to change the Auto Save, Default Visibility, Default Zone, and Discard Inactive configuration parameters. In the Faceplate window, open the Zoning menu and select **Edit Zoning Config** to open the Zoning Config window shown in [Figure 2-25](#). After making changes, click the **OK** button to put the new values into effect.

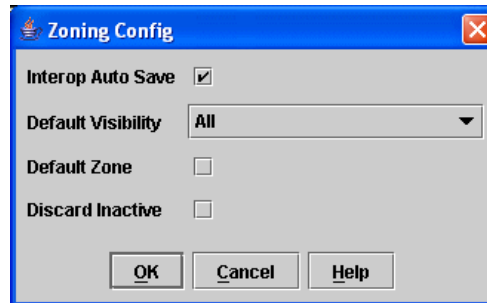


Figure 2-25. Zoning Config Window

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

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

Default Visibility The Default Visibility parameter is only available when the Interop Mode setting on the Advanced Switch Properties window is set to Standard. The Default Visibility parameter determines the level of communication that is permitted between 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 on the switch can communicate with all ports on switches that also have Default Visibility enabled. When Default Visibility is disabled (None) on a switch, none of the ports on that switch can communicate with any other switch in the fabric. The Default Visibility parameter permits or prohibits communication among ports/devices when there is no active zone set.

Default Zone The Default Zone parameter disables communication between ports and devices not defined in the active zoneset, or when there is no active zoneset. The Default Zone setting must be set the same on all switches in the fabric. The Default Zone setting is set automatically on all switches fabric if the Interop Mode setting on the Advanced Switch Properties window is set to McDATA Fabric Mode. If the Interop Mode setting on the Advanced Switch Properties window is set to Standard, you must ensure that all switches in the fabric have the same Default Zone setting.

Discard Inactive The Discard Inactive parameter automatically removes the previously active zone set when a zoneset is activated on a switch. The default setting is True.

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.

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**.

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.

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

Managing Zone Sets

Zoning a fabric involves creating a zone set, creating zones as zone set members, 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.

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 2-60.
5. Click the **Apply** button to save changes to the zoning database.

Activating and Deactivating a Zone Set

You must activate a zone set to apply its zoning definitions to the fabric. Only one zone set can be active at one time. When you activate a zone set, the switch 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 2-57](#) 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.

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.

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 it 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.

Removing a Zone Set

Removing a zone set affects the member zones in the following ways.

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

To delete a zone set from the database, 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.

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.

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 2-63](#) for more information. Refer to [“Zones” on page 2-51](#) 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 SANsurfer Switch Manager 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.

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. Click 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.

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.

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.

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.

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.

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.

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.

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.

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. Click 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.

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.

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 Interop Auto Save is turned on.

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 2-106](#) and the [“Show Command” on page 1-83](#) (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.

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 2-61](#) for information about adding and removing zone members. Refer to [“Resetting a Port” on page 2-112](#) for information about resetting a port.

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](#)
- [Resetting a Switch Module](#)
- [Configuring a Switch Module](#)
- [Archiving a Switch Module Configuration](#)
- [Restoring a Switch Module Configuration](#)
- [Restoring the Factory Default Configuration](#)
- [Installing Firmware](#)
- [Upgrading the Switch Using PFE Keys](#)
- [Downloading a Support File](#)

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 2-8. 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 SANsurfer Switch Manager. The USERID account can not be removed.

Users with Admin authority can view and modify the switch module and its configuration using SANsurfer Switch Manager. 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.

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

Creating User Accounts

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 2-26](#). A switch module can have a maximum of 15 user accounts.

Login	Admin Authority	Days to Expiration
images	false	never expires
USERID	true	never expires

Add Account

New Account Login:

Admin Authority Enabled

New Password:

Verify Password:

Account Expiration Date

Permanent account (no expiration date)

Account will expire in days (max of 2000 days)

Figure 2-26. 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.

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 2-27](#). Select the account (login) name from the list of accounts at the top of the window and click the **Remove Account** button.

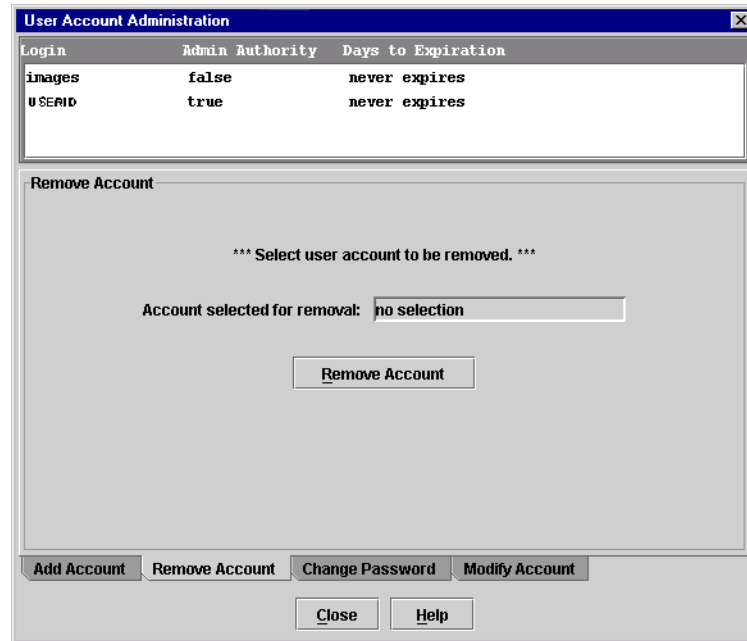


Figure 2-27. User Account Administration Window - Remove Account

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 2-28](#). 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.

Login	Admin Authority	Days to Expiration
images	false	never expires
USERID	true	never expires

Change Password

*** Select user account for password change. ***

Account Login:

Old Password:

New Password:

Verify Password:

Figure 2-28. User Account Administration Window - Change Password

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 2-29](#). 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.

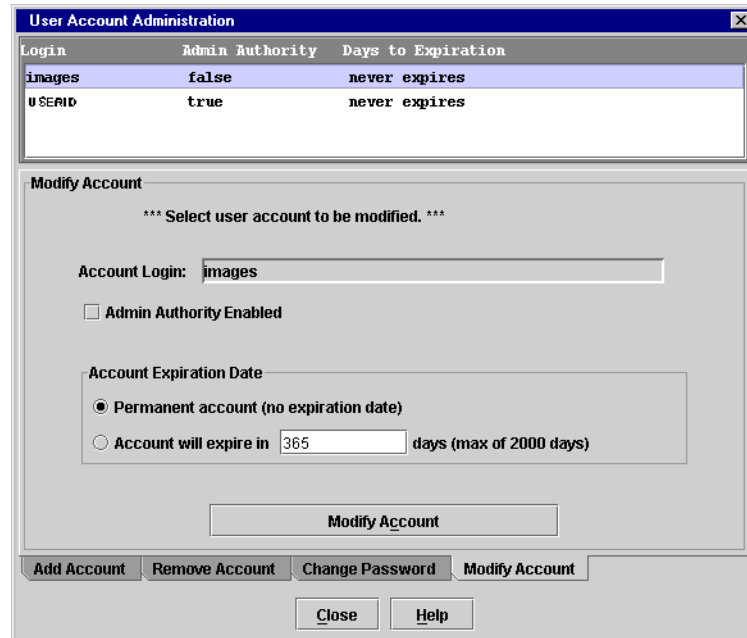


Figure 2-29. User Account Administration Window - Modify Account

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 2-30 shows the Faceplate window for the McDATA 6-Port Fibre Channel Switch Module.

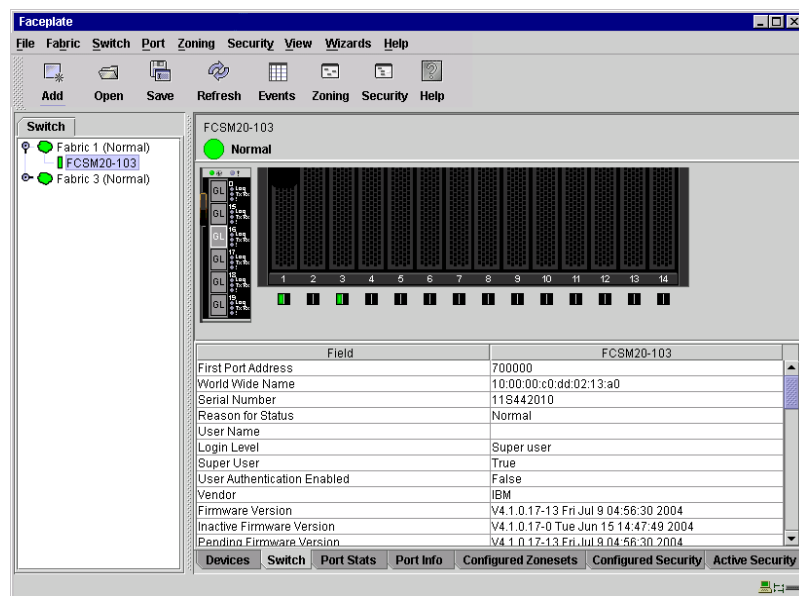


Figure 2-30. Faceplate Window - Switch Information

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.

Hardware Status

The Faceplate window shows the status of the switch module LEDs as shown in [Figure 2-31](#). 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.

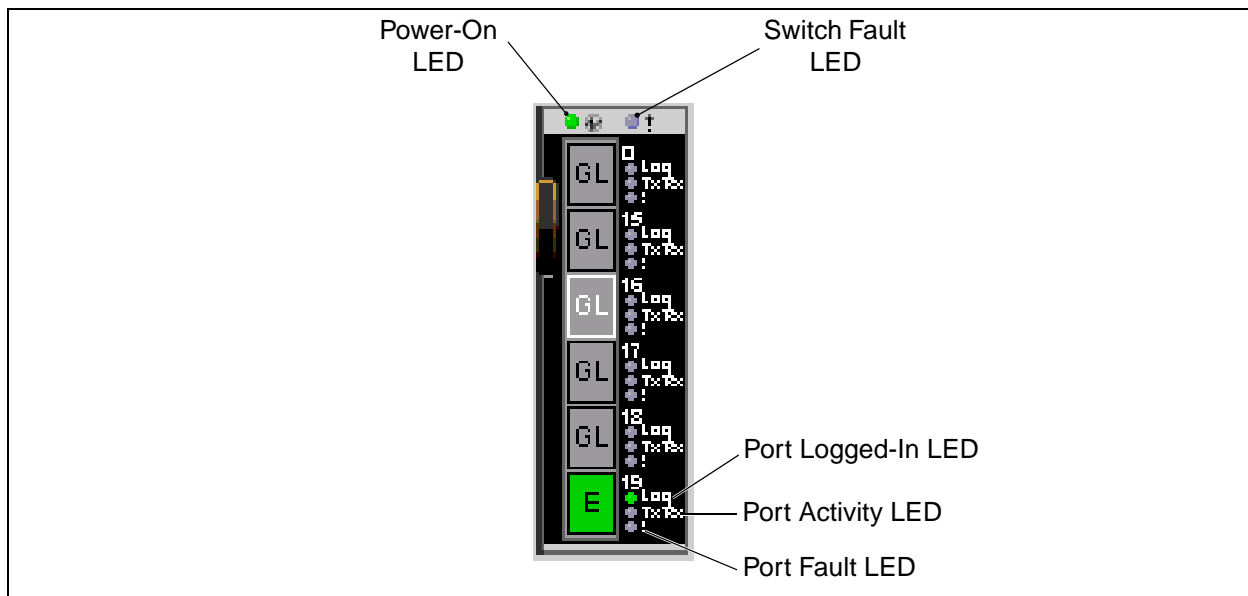


Figure 2-31. Hardware Status LEDs

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 2-45](#) for a description of the entries in the Devices data window.

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 2-82](#) 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 2-9](#) describes the Switch data window entries.

Table 2-9. 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
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

Table 2-9. Switch Data Window Entries (Continued)

Entry	Description
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.
Interop 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.
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.

Table 2-9. Switch Data Window Entries (Continued)

Entry	Description
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.
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.

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.

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 2-19](#) 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.

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 2-20](#) for a description of the Port Information data window entries.

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 2-32](#). 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.

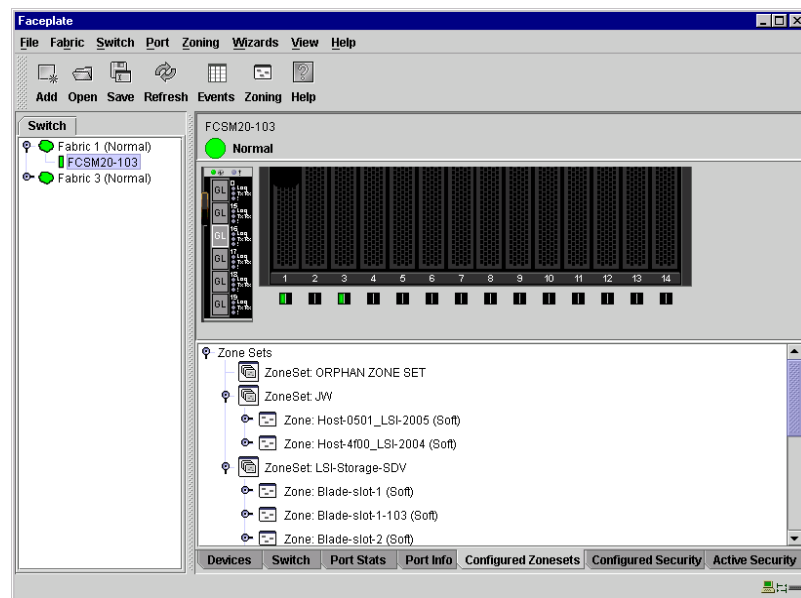


Figure 2-32. Configured Zonesets Data Window

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 2-33](#) prompts you to enable or disable all alarms, select an event, set triggers, set a sample window and enable or disable an individual alarm.

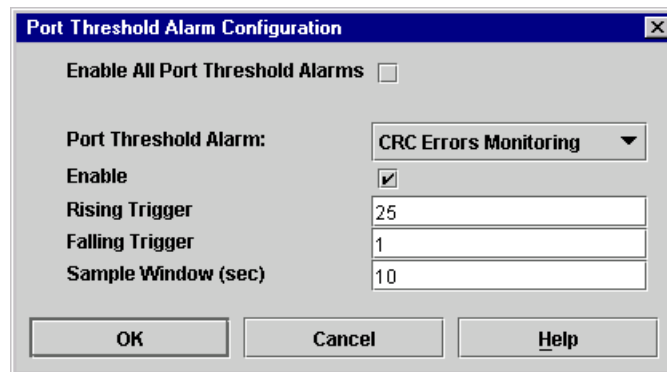


Figure 2-33. Port Threshold Alarm Configuration Window

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 2-34](#).
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.

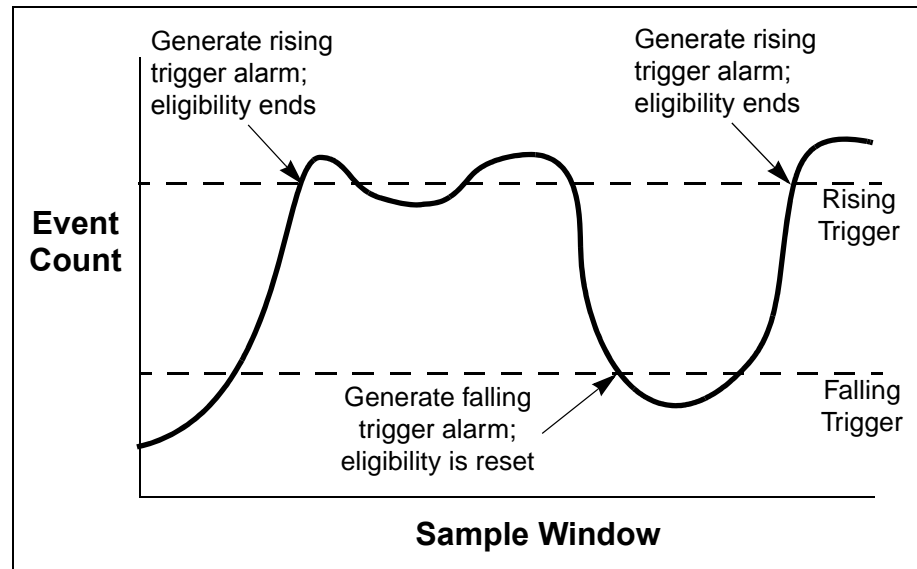


Figure 2-34. Port Threshold Alarm Example

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.

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**.

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 2-90](#) 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.

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 2-10](#) 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:

- SANsurfer Switch Manager 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 2-10. 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 SANsurfer Switch Manager, 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.

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.

Using the Configuration Wizard

SANsurfer Switch Manager 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.

Switch Properties

To open the Switch Properties window, either select a switch in the Topology window or open the Faceplate window for the switch you be configuring, and then open the Switch menu and select **Switch Properties**. You may also right-click a switch graphic in the Topology window or Faceplate window, and select **Switch Properties** from the popup menu.

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](#)
- [Broadcast Support](#)
- [In-band Management](#)
- [Fabric Device Management Interface](#)

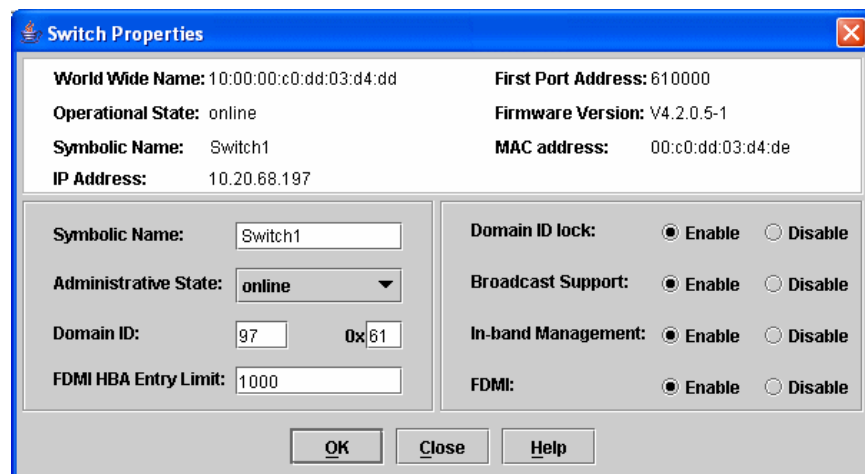


Figure 2-35. Switch Properties Window

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 (,).

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. SANsurfer Switch Manager 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 1-57](#).

[Table 2-11](#) describes the administrative state values.

Table 2-11. 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.

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 1-59](#) 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.

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. SANsurfer Switch Manager 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 2-45 for more information.

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.

In-band Management

In-band management is the ability to manage switch modules across interswitch links using SANsurfer Switch Manager, 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.

Advanced Switch Properties

Advanced Switch Properties window enables you to set the timeout values and Interop Mode settings. The Advanced Switch Properties window is available for only the entry switch, because an in-band switch can not be taken offline. The switch will automatically be taken offline temporarily and will be restored to its original state after the changes are completed. To open the Advanced Switch Properties window, open the Switch menu and select **Advanced Switch Properties**. After making changes, click the **OK** button to put the new values into effect.

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

- [Timeout Values](#)
- [Interop Mode for Zoning](#)

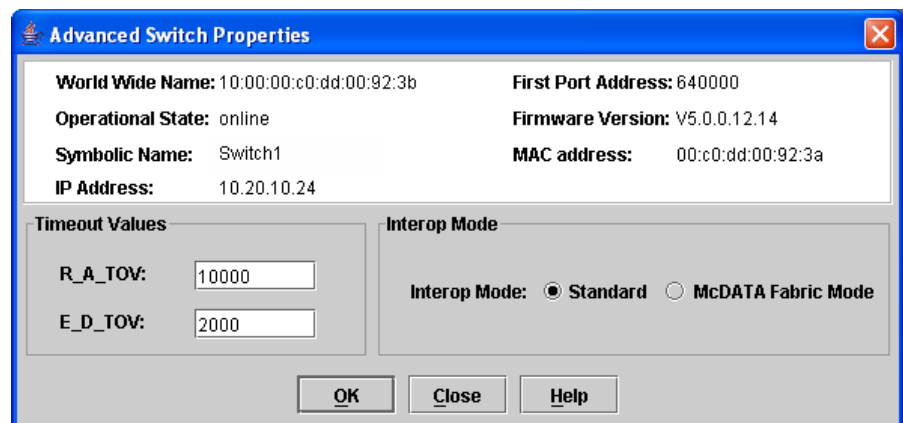


Figure 2-36. Advanced Switch Properties Window

Timeout Values

The switch module timeout values determine the timeout values for all external ports on the switch module. [Table 2-12](#) 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 2-12. Timeout Values

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

Interop Mode for Zoning

When a zone set is activated on an FC-SW-2 compliant switch, only the active zone set is propagated to all switches in the fabric. When a zone set is activated on a non-FC-SW-2 compliant switch, the active zone set and all inactive zone sets (the entire zoning database stored in permanent memory) are propagated to all switches in the fabric. Use the Standard option for FC-SW-2 compliant switches to propagate only the active zone set to all switches in the fabric. Use the McDATA Fabric Mode parameter for non-FC-SW-2 compliant switches. The default setting is McDATA Fabric Mode.

NOTE: The Interop Mode setting must be the same on all switches in the fabric, otherwise the interswitch links will not connect.

System Services Window

The System Services window provides a central location for you to enable or disable any of the external user services such as Simple Network Management Protocol (SNMP), Secure Sockets Layer (SSL), Secure SHell (SSH), embedded switch management application, command line interface, Network Time Protocol (NTP), and Common Information Model (CIM). To display the System Services window, open the Switch menu and select **Services**.

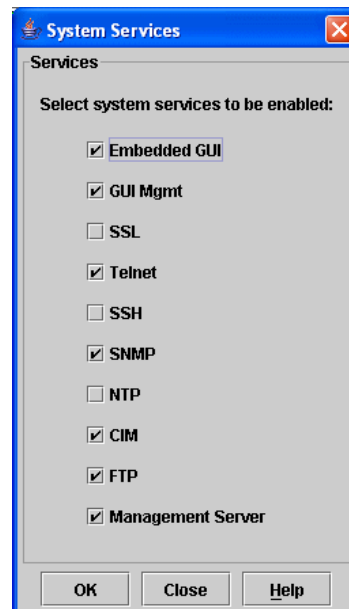


Figure 2-37. System Services window

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

- **Embedded GUI** - Embedded Graphical User Interface. Allows users to point a browser at the switch and run the embedded switch management application on that switch as McDATA SANbrowser.
- **GUI Mgmt** - Allows out-of-band management of the switch from the switch management application (GUI). If disabled, the switch can not be specified as the entry switch for a fabric in the GUI, but can still be managed through an in-band connection.
- **SSL** - Secure Sockets Layer. Provides secure encrypted communications between the switch management application (GUI) and the switch. SSL must be enabled for configuration of security and RADIUS servers with the switch management application (GUI). SSL certificates are generated on the switch with the switch date/time and validated with the workstation's date/time. If the Switch and workstation date/time are not in sync, invalid certificates will be generated and prevent an SSL connection from being established between the switch and switch management application (GUI). To disable SSL when using a user authentication RADIUS server, the RADIUS authentication order must first be set to **Local**.

- **Telnet** - Command line interface. Allows users to manage the switch through a Telnet command line interface session. Disabling Telnet access to the switch is not recommended.
- **SSH** - Secure SHell. Provides secure encrypted Telnet command line interface sessions with the switch. Note that you will have to have an SSH client running on your workstation in order to manage your switch with Telnet command line interface when SSH is enabled.
- **SNMP** - Simple Network Management Protocol. Allows management of the switch through third-party applications that use SNMP.
- **NTP** - Network Time Protocol. Allows the switch to obtain its time and date settings from an NTP server. Configuring all of your switches and your workstations to utilize NTP will keep their date/time settings in sync and will prevent difficulties with SSL certificates and event logs.
- **CIM** - Common Information Model. Allows management of the switch through third-party applications that use CIM.
- **FTP** - File Transfer Protocol. Allows file transfers to the switch via FTP. FTP is required for out-of-band firmware uploads which will complete faster than in-band Firmware uploads.
- **Management Server** - Allows management of the switch through third-party applications that use GS-3 Management Server.

Network Properties

Use the Network Properties window shown in [Figure 2-38](#) 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**.

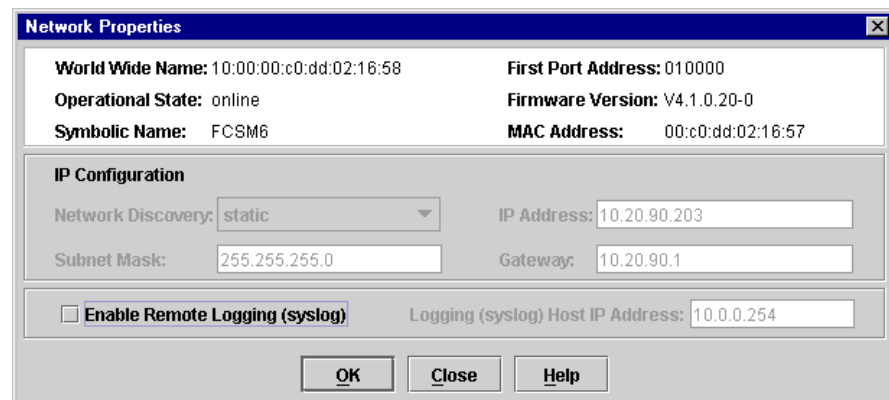


Figure 2-38. Network Properties Window

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 2-13](#) cannot be changed using SANsurfer Switch Manager. Make changes to the IP configuration parameters through the BladeCenter management module instead.

Table 2-13. IP Configuration Parameters

Parameter	Description
Network Discovery	Static - Uses the IP configuration parameters entered in the Network 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.

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`).

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 2-80](#).

Archiving a Switch Module Configuration

Archiving a switch module saves the current switch configuration parameters to an .XML archive file containing the configuration parameters. Basically any data received by the SANsurfer Switch Manager is archived. However, passwords are not archived with the user account information. The switch module can later be restored using the saved switch configuration file. Archived parameters include switch properties and statistics, IP configuration, SNMP configuration, port properties and statistics, alarm configuration, and zoning configuration. Refer to [“Backing up and Restoring Switch Module Configurations” on page 1-4](#) 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. You can use the archive later to restore the switch module. Refer to [“Restoring a Switch Module Configuration” on page 2-92](#) 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.

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 McDATA 6-Port Fibre Channel Switch Module switch only with an archive from a McDATA 6-Port Fibre Channel Switch Module. Refer to [“Archiving a Switch Module Configuration” on page 2-91](#) 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 2-39](#). The Restore window offers a **Full Restore** and a **Selective Restore** tab.

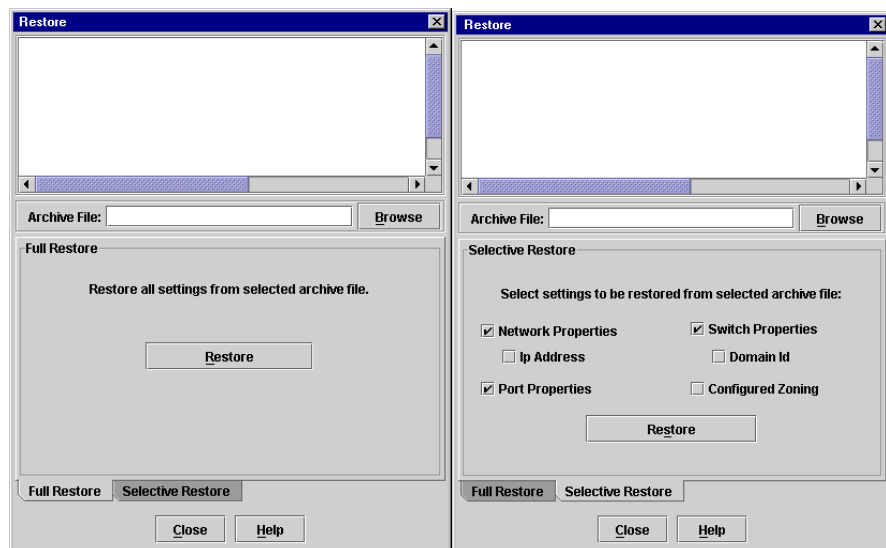


Figure 2-39. Restore Windows – Full and Selective

3. Enter the archive file name or browse for the file. This archive file must be one that was produced by the SANsurfer Switch Manager Archive function. Configuration backup files created with the Config Backup command are not compatible with the SANsurfer Switch Manager 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 2-89](#).
 - **IP Address:** Restores switch IP address in addition to the other network properties. Refer to [“Network Properties” on page 2-89](#).
 - **Switch Properties:** Restores all settings presented in the Switch properties window except the domain ID. Refer to [“Switch Properties” on page 2-83](#).
 - **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 2-108](#).
 - **Configured Zoning:** Restores all zone sets, zones, and aliases in the switch’s zoning database.
 - **Configured Security:** Restores all security sets in the switch database.
 - **Radius Server:** Restores all RADIUS Server information defined in the switch database.
5. If you select the Configured Zoning or Full Restore option and the file contains zone sets, a window prompts you to activate one of those zone sets. Click the **Yes** button, and select a zone set from the drop-down menu in the Select Zone Set to be Activated window.
6. Click the **OK** button and view the results in the top pane of the Restore window.

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 2-14](#) 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 2-14. 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
Interop Mode	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
Device Scan Enabled	True
Remote Logging	False
Remote Logging Host Ip Address	10.0.0.254

Table 2-14. Factory Default Configuration Settings (Continued)

Setting	Value
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

Installing Firmware

Installing firmware involves loading, unpacking, and activating the firmware image on the switch. SANsurfer Switch Manager 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:

- SANsurfer Switch Manager 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.

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

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. SANsurfer Switch Manager 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.

Upgrading the Switch Using PFE Keys

A Product Features Enabled (PFE) key is a password that you can purchase from your switch distributor or authorized reseller to upgrade your switch. PFE keys vary according to the features you purchase and come with instructions.

NOTE: The SANtegrity Enhanced® PFE key is required to configure and activate device security. Refer to “[Device Security](#)” on page 2-26. For additional information about McDATA Product Features Enabled, please contact your McDATA representative or visit the McDATA website at www.mcddata.com.

To display the Feature Licenses dialog, open the Switch menu and select **Features**.

NOTE: Upgrading a switch using PFE keys through an in-band switch is not recommended because traffic is disrupted. However, SANsurfer Switch Manager does not prevent the user from doing so.

To upgrade the switch, do the following:

1. If the upgrade PFE key instructions indicate that the procedure is disruptive, isolate the switch from the fabric.
2. Add a fabric with the IP address of the switch you want to upgrade.
3. Open the faceplate display for the switch you want to upgrade.
4. Open the Switch Menu and select **Features** to open the Feature Licenses dialog.
5. In the Feature Licenses dialog, click the **Add** button to open the Add License Key dialog shown in [Figure 2-40](#).

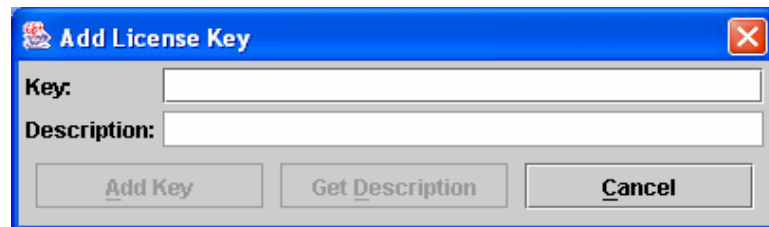


Figure 2-40. Add License Key Dialog

6. In the Add License Key dialog, enter the PFE key in the Key field.
7. Click the **Description** button to display the upgrade description.
8. Click the **Add Key** button to upgrade the switch. Allow a minute or two for the upgrade to complete.

Downloading a Support File

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

To create a support file, do the following:

1. On the Faceplate window, open the Switch menu, and select **Download Support File**.
2. In the Download Support File window, click the **Browse** button to define a location for the support file or type the path in the text field.
3. Click the **Start** button to begin the process of creating and downloading the support file to your workstation. Observe the status in the Status area.
4. After the support file is saved to your workstation, click the **Close** button to close the Download Support File window.

Managing Ports

This section describes the following tasks that manage ports and devices:

- [Displaying Port Information](#)
- [Configuring Ports](#)
- [Resetting a Port](#)

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 2-41](#). The Port Information data window for a 6-port Switch Module in BladeCenter T unit is shown in [Figure 2-42](#).

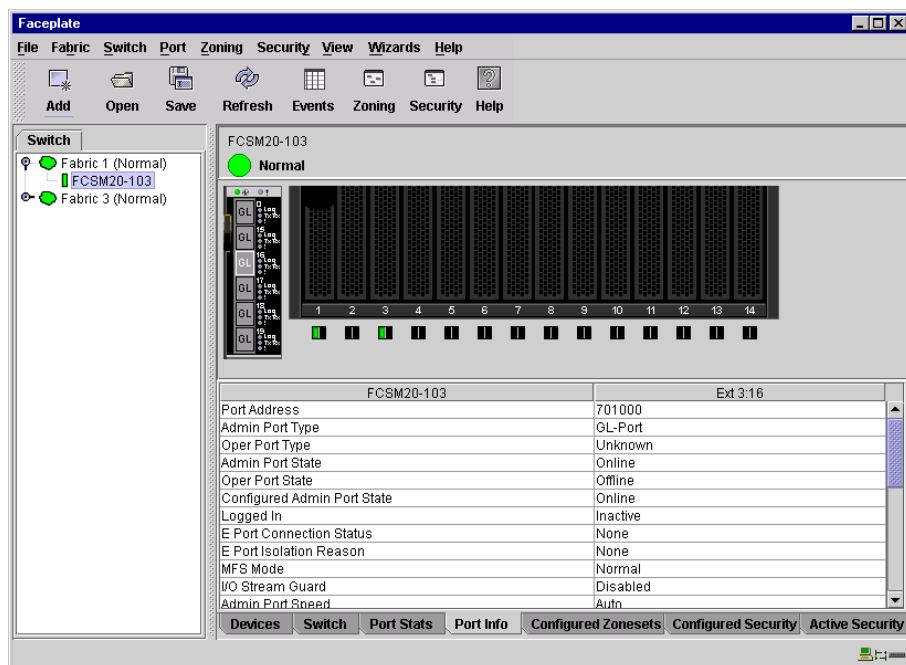


Figure 2-41. BladeCenter Faceplate Window – Port Information

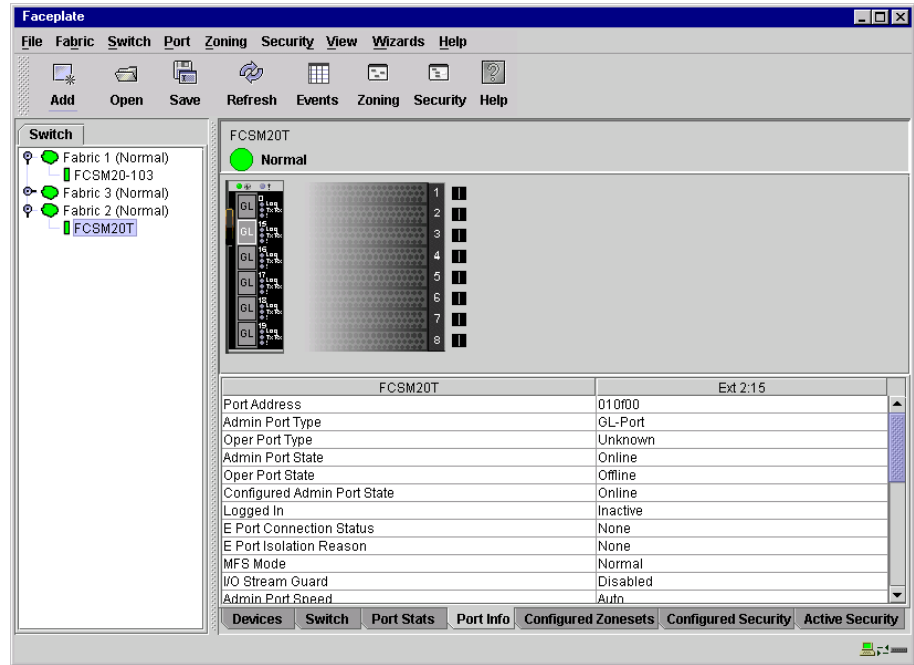


Figure 2-42. BladeCenter T Faceplate Window – Port Information

Monitoring Port Status

The Faceplate window provides the following port related information:

- SNMP configuration (see [“Switch Module Monitoring Using SNMP”](#) on page 3-4)
- 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.

Displaying Port Types

To display port type status, from the Faceplate window, open the View menu, and select **View Port Types**. [Table 2-15](#) lists the possible port types and their descriptions.

Table 2-15. 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.

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 2-16](#) lists the available operational states. The port operational state refers to actual port state and not the administrative state you assigned.

Table 2-16. 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 2-106 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.

Displaying Port Speeds

To display the speed of each port in the Faceplate window, open the View menu and select **View Port Speeds**. [Table 2-17](#) lists the available port speeds.



Table 2-17. Port Speeds

State	Description
Au	Auto-detect
1-Gbps	1-Gbps transmission speed
2-Gbps	2-Gbps transmission speed

Displaying Transceiver Media Status

To display transceiver media status, open the View menu and select **View Port Media**. [Table 2-18](#) lists and describes the port media states.

Table 2-18. Port Transceiver Media View

Media Icon	Description
	Optical SFP module, online (Green)
	Optical SFP module, offline (Gray)
None	Empty port, no transceiver installed

Port Graphing and Performance Viewer Application

You can use the Performance Viewer application to view port performance as graphs. The Performance Viewer window displays data communication rates and total errors for selected ports as shown in [Figure 3-4](#). You can graph communication data rates using either frames per second or KB per second. For more information about port graphing, see [“Using the Performance Viewer Application”](#) on page 3-7.

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 2-19](#) 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 2-19. 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.
AI 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.

Table 2-19. Port Statistics Data Window Entries (Continued)

Entry	Description
Class 3 Words In	Number of class 3 words received by this port.
Class 3 Words Out	Number of class 3 words transmitted by this port.
Decode Errors	Number of invalid transmission words detected during decoding. Decoding is from the 10-bit characters and special K characters.
Ep Connects	Number of E_Port logins.
FBusy	Number of class 2 and class 3 fabric busy (F_BSY) frames generated by this port in response to incoming frames. This usually indicates a busy condition on the fabric or N_port that is preventing delivery of this frame.
Flow Errors	Number of times a frame is received and all the 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.
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.

Table 2-19. Port Statistics Data Window Entries (Continued)

Entry	Description
Rx Link Resets	Number of link reset primitives received from an attached device.
Rx Offline Sequences	Number of offline sequence primitives received by the port.
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.

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 2-20. 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.
Administrative Port Speed	The speed requested by the user.
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.

Table 2-20. Port Information Data Window Entries (Continued)

Entry	Description
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

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 2-43](#). To open the Port Properties window, select one or more ports, open the Port menu and select **Port Properties**.

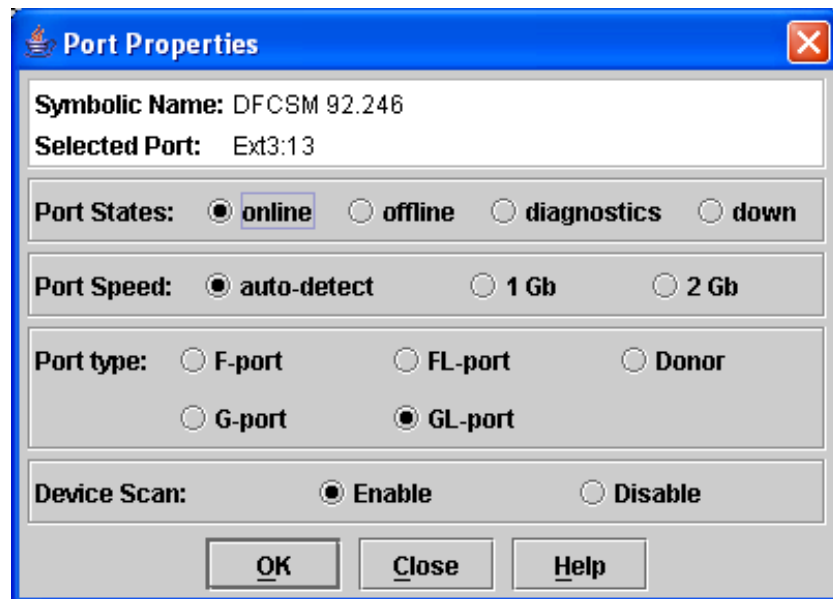


Figure 2-43. External Port Properties Window

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 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 2-44](#). To open the Port Properties window, select one or more internal ports open the Port menu and select **Port Properties**.

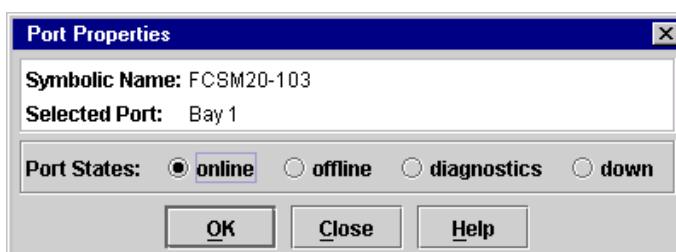


Figure 2-44. Internal Properties Window

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 SANsurfer Switch Manager 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. SANsurfer Switch Manager always makes changes to the configured administrative state.

The current administrative state is the state that is applied to the port for temporary purposes and is not preserved across switch module resets. The current administrative state is set using the Set Port command. Refer to the [“Set Port Command” on page 1-72](#).

[Table 2-21](#) 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 2-21. 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.

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 2-22](#) 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 2-22. 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.

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 2-23](#) 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 2-23. 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.

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.

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.

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 3-2](#).

This chapter contains information about the following topics:

- [LED Diagnostics](#)
- [Testing Ports](#)
- [Switch Module Monitoring Using SNMP](#)
- [Using the Performance Viewer Application](#)

LED Diagnostics

The McDATA 6-Port 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 3-1](#) shows the location of these LEDs on the switch module. For more information about switch module LEDs, see the *McDATA 6-Port Fibre Channel Switch Module for IBM Eserver BladeCenter Installation Guide*.

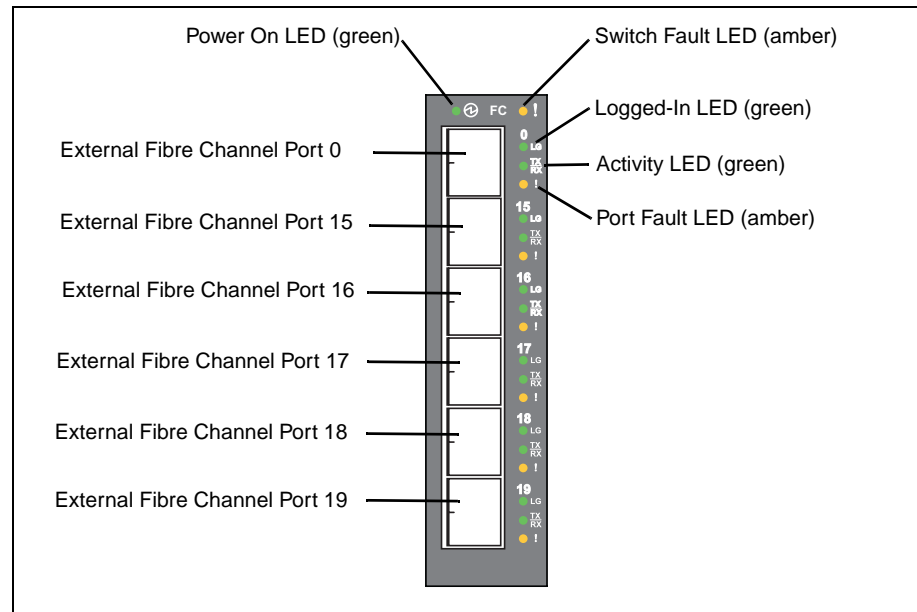


Figure 3-1. Switch Module LEDs

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 3-2](#).

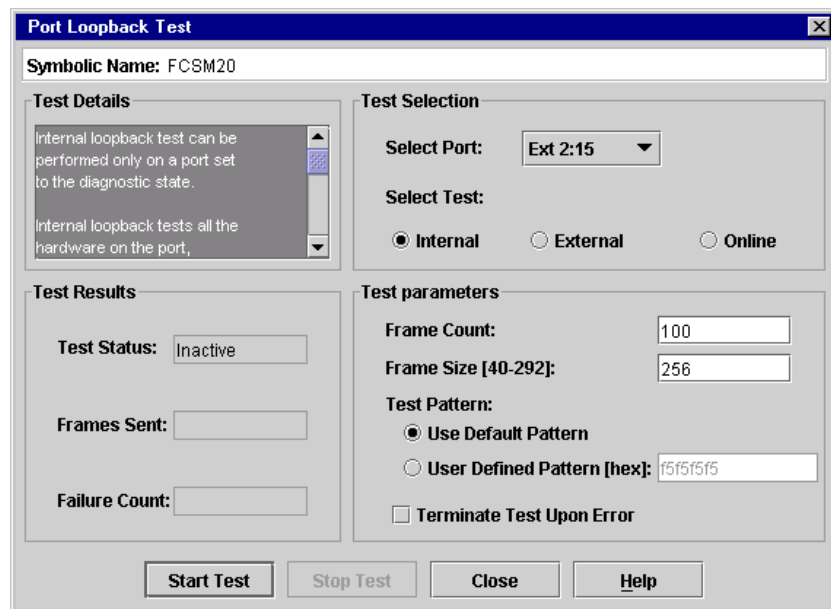


Figure 3-2. Port Loopback Test Window

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, SANsurfer Switch Manager will prompt you to confirm that the port state needs to be changed to the diagnostic state. Click the **OK** button and SANsurfer Switch Manager 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.

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 3-3](#) 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.

The screenshot shows the 'Snmp Properties' dialog box with the following fields and options:

- World Wide Name:** 10:00:00:c0:dd:00:92:21
- Operational State:** online
- Symbolic Name:** unknown
- First Port Address:** a40000
- Firmware Version:** V4.1.0.0-25
- MAC Address:** 00:c0:dd:00:92:20

SNMP Configuration

- SNMP Enabled
- SNMP Proxy
- Contact:** Contact2
- Location:** Location 2
- Read Community:** [Empty]
- Authentication Trap:** True
- Trap Community:** [Empty]
- Write Community:** [Empty]

SNMP Trap Configuration

- Trap 1 Enabled
- Trap Version:** V2
- Trap Severity:** Mark
- Trap Address:** 11.1.1.1
- Trap Port:** 11

Buttons: OK, Close, Help

Figure 3-3. SNMP Properties Window

SNMP Configuration

The SNMP configuration defines how authentication traps are managed. [Table 3-1](#) describes the SNMP configuration parameters. The illegal characters for the user-defined fields are the pound sign (#), semi-colon (;), and comma (,).

Table 3-1. 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".

SNMP Trap Configuration

The SNMP trap configuration defines how traps are set. Choose from the tabs **Trap1 – Trap 5** to configure each trap. [Table 3-2](#) describes the SNMP configuration parameters.

Table 3-2. 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 window 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.

Using the Performance Viewer Application

Performance Viewer application displays port performance using graphs. Performance Viewer plots data communication rates and total errors for selected ports as shown in [Figure 3-4](#). When graphing data communication rates, you can choose either frames/second or KB/second.

On Solaris platforms, if you launch the Performance Viewer application from the SANSurfer Switch Manager application and Performance Viewer can not connect to the fabric, (for example, if you have reached the maximum number of SANSurfer Switch Manager sessions on the entry switch), then Performance Viewer opens with a blue fabric icon displayed in the fabric tree.

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).

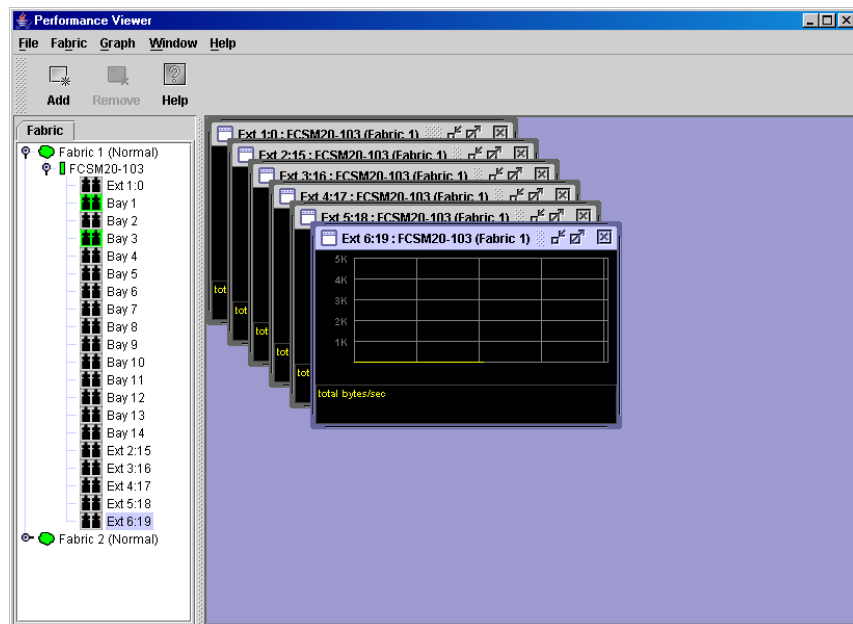


Figure 3-4. Fabric View Graphs

This section describes how to do the following:

- [Starting Performance Viewer](#)
- [Exiting Performance Viewer](#)
- [Saving and Opening Performance View Files](#)
- [Changing the Default Performance View File Encryption Key](#)
- [Setting Performance Viewer Preferences](#)
- [Setting the Polling Frequency](#)
- [Displaying Graphs](#)
- [Printing Graphs](#)
- [Saving Graph Statistics to a File](#)

Starting Performance Viewer

To start Performance Viewer from within SANsurfer Switch Manager, open the Topology window and select **Start Performance Viewer** from the Fabric menu. Open the fabric in the Performance Viewer Topology window.

When starting the Performance Viewer application from the SANsurfer Switch Manager application on Linux and Solaris platforms, the fabric currently displayed in the SANsurfer Switch Manager topology display opens automatically in the Performance Viewer topology display. On Windows platforms, you will need to manually open the fabric in the Performance Viewer Topology window.

NOTE: On the Solaris platforms, if you launch the Performance Viewer application from the SANsurfer Switch Manager application and Performance Viewer can not connect to the fabric, (for example, if you have reached the maximum number of SANsurfer Switch Manager sessions on the entry switch), then Performance Viewer opens with a blue fabric icon displayed in the fabric tree. The reason for status displayed after the fabric name in the fabric tree will indicate the reason for failure to connect.

Exiting Performance Viewer

To exit a Performance Viewer 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 Performance Viewer session. If you have not yet defined an encryption key, the Save Default Performance View File window, shown in [Figure 3-5](#), 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 3-10](#) for information about defining and changing this encryption key.

In the Save Default Performance View File window, 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 Performance Viewer 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 Performance Viewer Preferences” on page 3-10](#) for more information.



Figure 3-5. Save Default Performance Viewer File Window

In your next Performance Viewer session, the Load Default View File window shown in [Figure 3-6](#) 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 Performance Viewer with no fabric displayed.

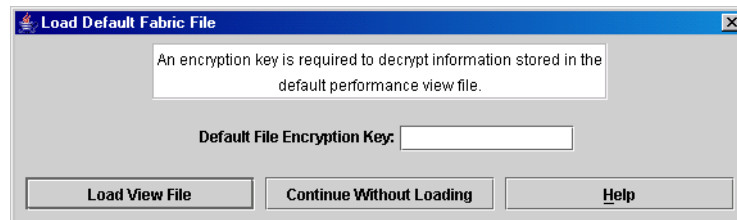


Figure 3-6. Load Default View File Window

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 window.
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 window.
2. Enter a name for the fabric file or click the **Browse** button to select an existing file.

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 window.
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.

Setting Performance Viewer Preferences

To set preferences, open the File menu and select **Preferences** to open the Preferences window shown in [Figure 3-7](#). 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, Performance Viewer prompts you to save and load the default fabric file between sessions. Refer to [“Exiting Performance Viewer” on page 3-8](#) for more information on the default performance view file.
- Enable or disable the Display Dialog When Making Non-secure Connections checkbox. If enabled, the Non-secure Connections Check window is displayed when you attempt to open a non-secure fabric. You then have the option of opening a non-secure fabric. If disabled, you cannot open a fabric with a non-secure connection).

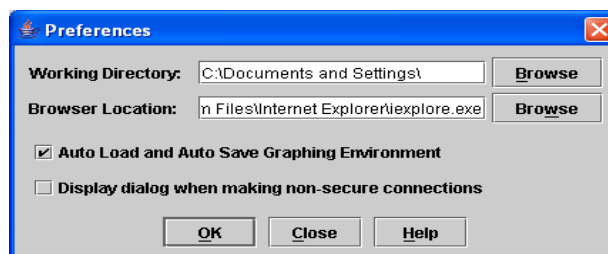


Figure 3-7. Preferences – Performance Viewer

Setting the Polling Frequency

Performance Viewer 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 window.
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.

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 window. Include an account name and a password if required.
2. Set the graphing options and polling frequency. By default, Performance Viewer plots total bytes transmitted and received at a polling frequency of once per second. Refer to [“Customizing Graphs” on page 3-12](#) 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 3-11](#) 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.

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.

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 window 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 window shown in [Figure 3-8](#).

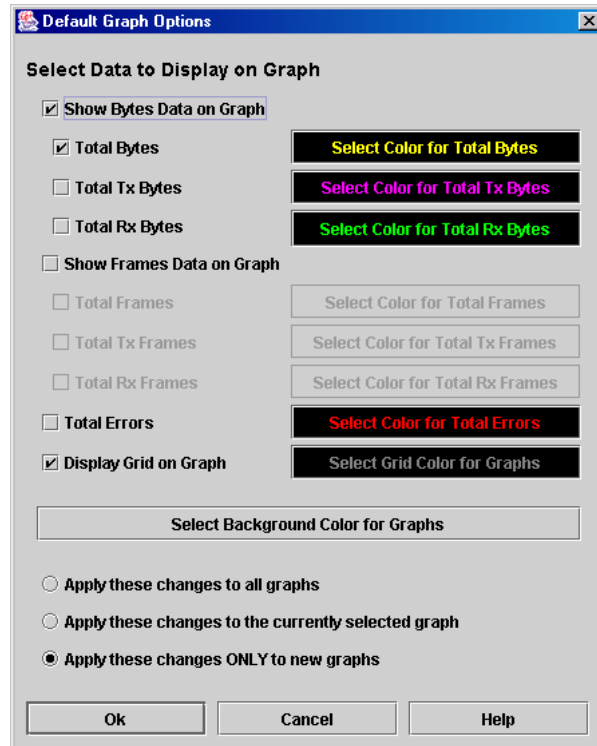


Figure 3-8. Default Graph Options Window

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 window, 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 windows 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 window, 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 window, click the **OK** button to save the color scheme changes and close the window.

Setting Global Graph Type

The Set Global Graph Type option enables you to view port activity using two types of graphs:

- Line Graph - plots continuous port activity in horizontal line format.
- Bar Graph - the last polling value received by the application in bar graph format.

To set the global graph type, open the Graph menu and select **Line Bar** or **Bar Graph**.

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.

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.

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 window, enter a path name for the file. By default, the file is saved in the working directory.
4. Click the **Save** button.

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 SANsurfer Switch Manager 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.

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	SANsurfer Switch Manager 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

Table A-1. Port Mapping For Server Units (Continued)

Switch Module Physical Port Connection	SANsurfer Switch Manager and CLI Logical Port Number	SNMP Port Numbering	Configurable
Server bay 12 ²	12	13	No
Server bay 13 ²	13	14	No
Server bay 14 ²	14	15	No
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.

A

access control list zone 2-51, 2-63
 account name display 1-113, 1-116
 active zone set 2-46, 2-52, 2-87
 Active Zoneset data window 2-46
 Activity LED 2-73
 Admin
 account name 1-6
 authority 1-6
 Admin command 1-7
 Admin session timeout 1-79
 administrative state
 configured 2-84, 2-109
 current 2-84, 2-109
 port 1-73, 2-109
 switch 1-58, 2-84
 Advanced Switch Properties 2-86
 alarm
 configuration 1-63, 2-78
 configuration defaults 1-47
 configuration display 1-96
 description 1-71
 log 1-57, 1-83
 alias
 add members 1-8, 2-64
 copy 1-8
 create 1-8, 2-64
 delete 1-8
 delete members 1-9
 description 2-52
 display list 1-8
 display members 1-8
 remove 2-65
 rename 1-9
 Alias command 1-8
 Arbitrated Loop Physical Address 1-72
 archive configuration 2-91
 authentication 1-26
 device 2-19
 trap 3-5
 user 2-19
 authority 1-6

auto save

 default fabric view file 2-17
 graphing options 3-10
 zoning configuration 2-57

B

beacon 1-57
 binding 1-25, 1-28
 broadcast 1-84, 2-85
 browser 1-79
 internet 2-2, 2-17, 3-10
 service 1-76

C

certificate 1-18, 2-24
 CHAP authentication 1-26
 chassis status 1-84
 checklist 2-25
 CIM command 1-10
 CIMListener command 1-11
 CIMSubscription command 1-13
 command line interface (CLI) 1-1
 command syntax 1-5
 commands 1-6
 Common Information Model
 configure 1-10
 display listener 1-84
 display subscription 1-84
 listener 1-11
 service 1-76, 2-89
 subscription 1-13
 Config command 1-15
 configuration
 activate 1-15
 archive 2-91
 backup 1-15
 copy 1-15
 delete 1-15
 edit 1-15
 list 1-15
 reset 1-44

- restore 1-16, 2-92
- save 1-16
- wizard 2-82
- configured administrative state 2-84
- connection
 - Secure Socket Layer 1-18
 - security 1-75, 1-76, 2-24
- contact 3-5
- CRC error 2-78
- Create command 1-18
- current administrative state 2-84

D

- data window
 - Active Zoneset 2-46
 - Configured Zonesets 2-77
 - description 2-10, 2-13, 2-15
 - Devices 2-45, 2-73
 - port information 2-106
 - port statistics 2-103
 - switch 2-74
- database
 - fabric 2-36
 - zoning 2-54
- date 2-80
- Date command 1-21
- Decode error 2-78
- default
 - configuration 2-94
 - visibility 2-60
 - zoning 2-58
- default fabric view file
 - auto save 2-17
 - SANsurfer Switch Manager 2-17
- defaults
 - alarm configuration 1-47
 - port configuration 1-46
 - RADIUS configuration 1-49
 - security configuration 1-50
 - services configuration 1-49
 - Simple Network Management Protocol
 - configuration 1-48
 - switch module configuration 1-45
 - system configuration 1-50
 - zoning configuration 1-47
- device
 - authentication 2-19
 - security 2-26
- device information
 - export to file 2-47
 - scan 2-111
- device port nickname
 - create 2-48
 - delete 2-49
 - description 2-48
 - edit 2-48
 - export to file 2-49
 - import 2-49

- Devices data window 2-45, 2-73
- disk space 2-2
- domain ID
 - binding 1-25, 1-28
 - description 2-84
 - display 1-84
 - lock 2-84
- donor port 1-84, 2-101, 2-111

E

- E_Port isolation 2-65, 2-84
- embedded GUI service 2-88
- encryption key 3-10
- Error Detect Timeout 2-87
- event browser
 - display 2-42
 - filter 2-44
 - preference 2-17
 - save to file 2-45
 - sort 2-44
- event logging
 - by component 1-69, 1-99
 - by port 1-71, 1-100
 - by severity level 1-100
 - display 1-99
 - restore defaults 1-71
 - save settings 1-71
 - settings 1-100
 - severity level 1-70, 2-43
 - start 1-71
 - stop 1-71
- external test 1-109, 3-2

F

- F_Port 2-101, 2-111
- fabric
 - add 2-36
 - add a switch 2-37
 - database 2-36
 - delete 2-37
 - discovery interval 2-17
 - displaying information 2-39
 - loop port 2-101, 2-111
 - management 2-19
 - management workstation 2-2
 - merge 2-65
 - port 2-101, 2-111
 - rediscovery 2-37
 - services 2-34
 - status 2-39
 - tree 2-9
 - zoning 2-50
- Fabric Device Management Interface 1-84, 2-85
- fabric tracker 2-35
- fabric view file
 - open 2-16
 - save 2-16
- Faceplate window

- data window 2-15
- description 2-14
- menus 2-7
- factory defaults 1-44, 2-94
- Fault LED 2-73
- FC-4 descriptor 2-111
- FC-SW-2 compliance 2-87
- Feature command 1-22
- File Transfer Protocol
 - example 1-37
 - service 1-76, 2-89
- firmware
 - image file 1-36, 2-96
 - install with CLI 1-23
 - install with SANsurfer Switch Manager 2-96
 - list image files 1-36
 - non-disruptive activation 1-34, 2-96
 - remove image files 1-36
 - retrieve image file 1-36
 - unpack image 1-36
 - version 1-90
- Firmware Install command 1-23
- FL_Port 2-101, 2-111

G

- gateway address 1-79, 2-90
- generic port 2-101, 2-111
- graph type 3-13
- graphic window 2-10
- group
 - add member 1-25, 2-31
 - copy 1-27
 - create 1-27, 2-29
 - display 2-32
 - display member 2-32
 - edit member attributes 1-28, 2-32
 - list 1-28
 - list members 1-29
 - Management Server 1-27
 - remove 2-32
 - remove member 1-29, 2-32
 - rename 1-29, 2-32
 - type 1-27, 1-29
- Group command 1-24
- GUI management service 2-88

H

- hard reset 2-81
- Hardreset command 1-31
- hardware status 2-73
- help 2-1
- Help command 1-32
- History command 1-33
- host bus adapter 1-84
- hot reset 2-81
- Hotreset command 1-34

I

- Image command 1-36
- in-band management 2-86
- indication service listener 1-11
- Initial Start Window 2-17
- internal port test 1-109
- internal test 3-2
- internet browser 2-2
- IP
 - address 1-79, 2-90
 - configuration 2-90
- ISL group 1-27
- ISL monitoring 2-78

L

- layout 2-12
- link
 - delete 2-38
 - selecting 2-12
 - status 2-11
- Link control frame preference routing 1-61
- Link data window 2-76
- link state database 1-84
- Lip command 1-39
- listener
 - add 1-11
 - Common Information Model 1-84
 - create 1-11
 - delete 1-11
- log
 - archive 1-69
 - clear 1-69
 - display 1-70, 1-100
 - event 1-69, 1-99
 - local 1-79
 - power-on self test 1-88
 - remote 1-79
- logged in users 1-90
- Logged-In LED 2-73
- login limit 2-25, 2-37
- loop port
 - bypass 1-72
 - enable 1-72
 - fabric 2-101, 2-111
 - initialization 1-39
- loopback test 3-2
- loss of signal monitoring 2-78

M

- Management Server
 - group 1-27
 - service 1-76, 2-89
- management workstation 2-3
- manufacturer information 1-105
- mask address 1-79
- McDATA SANbrowser 1-76, 1-79
 - description 2-3

- service 2-88
- status 2-76
- MD5 authentication 1-26
- media status 2-102
- memory
 - activity 1-84
 - workstation 2-2
- menu structure 2-6
- Multi-Frame Sequence bundling 1-61

N

- name server
 - display 1-85
 - zone 2-51
- network
 - configuration reset 1-45
 - discovery 1-79, 2-90
 - gateway address 1-79
 - interfaces 1-84
 - IP address 1-79
 - mask 1-79
 - properties 2-89
- Network Time Protocol
 - client 1-79, 2-80
 - interaction with Date command 1-21
 - server 2-80
 - server address 1-79
 - service 1-76, 2-89
- nickname
 - create 2-48
 - delete 2-49
 - description 2-48
 - edit 2-48
 - export to file 2-49
 - import 2-49
- node-to-node test 3-3
- non-disruptive activation 1-34

O

- online
 - help 2-1
 - test 3-3
- operating systems 2-2
- orphan zone set 2-52

P

- page break 1-58
- Passwd command 1-40
- password
 - change 1-40
 - default fabric view file 2-16
 - switch 1-40
 - user account 2-70
- performance
 - graphs 3-11
 - tuning 1-60
- performance view file

- auto save 3-10
- encryption key 3-8, 3-10
- open 3-10
- save 3-9
- Performance Viewer 2-3
 - arrange graphs 3-11
 - customize graphs 3-12
 - display graphs 3-11
 - preferences 3-10
 - print a graph 3-14
 - rescale a graph 3-13
 - save graph to a file 3-14
 - start 3-8
- PFE - See Product Features Enable
- Ping command 1-41
- port
 - Activity LED 2-73
 - administrative state 1-73, 2-109
 - configuration 1-59, 2-108
 - configuration defaults 1-46
 - configuration display 1-96
 - counters 1-72
 - displaying information 2-99
 - external test 1-109
 - Fault LED 2-73
 - group 1-27
 - initialize 1-44
 - Logged-In LED 2-73
 - loopback test 1-109
 - mode 2-101
 - online test 1-109
 - operational information 1-85
 - operational state 2-101
 - performance 1-85, 1-102, 3-7
 - performance tuning 1-60
 - reset 2-112
 - selecting 2-15
 - speed 1-72, 2-102, 2-110
 - status 2-14
 - symbolic name 2-112
 - test 3-2
 - view 2-14, 2-18
- Port Information data window 2-76, 2-106
- Port Statistics data window 2-76, 2-103
- port/device tree 2-55
- Power On LED 2-73
- power on self test log 1-88
- preferences
 - Performance Viewer 3-10
 - SANsurfer Switch Manager 2-17
- principal switch 2-84
- processor 2-2
- Product Features Enable key 1-22, 2-97
- properties
 - network 2-89
 - port 2-109
 - SNMP 3-4
 - switch 2-83
- Ps command 1-42

Q

Quit command 1-43

R

RADIUS server

- add 2-20
- authentication order 2-23
- configuration 1-74
- configuration defaults 1-49
- configuration display 1-105
- edit configuration 2-22
- remove 2-21
- reset 1-44

read community 3-5

refresh 2-39, 2-72

remote log

- enable 1-79
- host address 1-79

remote logging 2-90

reset

- with POST 2-81
- without POST 2-81

Reset command 1-44

Resource Allocation Timeout 2-87

restore configuration 2-92

S

SANsurfer Switch Manager

- description 2-1
- Performance Viewer 2-3
- preferences 2-17, 3-10

scan device 2-111

secret 1-26

Secure Shell

- description 2-24
- service 1-75, 2-89

Secure Socket Layer

- certificate 1-18
- description 2-24
- service 1-76, 2-88
- switch time 1-21

security

- certificate 2-24
- configuration 1-61, 2-33
- configuration defaults 1-50
- configuration display 1-96
- connection 2-24
- consistency checklist 2-25
- database 1-44
- device 2-26
- user account 2-25

Security command 1-52

security database

- clear 1-52, 2-32
- display 1-53
- display history 1-52
- limits 1-53

security edit session

- cancel 1-52
- initiate 1-52
- revert changes 1-53
- save changes 1-53

security set

- activate 1-55, 2-34
- add member group 1-55
- copy 1-55
- create 1-55, 2-28
- deactivate 1-55, 2-34
- delete 1-56
- delete member group 1-56
- display 1-56, 2-32
- display active 1-52, 1-55
- display members 1-56
- remove 2-32
- rename 1-56, 2-32

Securityset command 1-55

SerDes level test 3-2

service listener 1-11

services 2-88

services configuration defaults 1-49

Set command 1-57

Set Config command 1-59

Set Log command 1-69

Set Port command 1-72

Set Setup command 1-74

severity levels 2-43

SFP level test 3-2

SHA-1 authentication 1-26

Show command 1-83

Show Config command 1-96

Show Log command 1-99

Show Perf command 1-102

Show Setup command 1-105

Shutdown command 1-108

Simple Network Management Protocol

- configuration 1-77, 3-5
- configuration display 1-105
- defaults 1-48
- properties 3-4
- proxy 3-5
- reset 1-44
- service 1-76, 2-89
- trap configuration 3-6

snapshot

- comparison 2-35
- export to a file 2-36
- save 2-35

SNMP enabled 3-5

soft zone 2-51, 2-63

status icon color 2-9

steering 1-88

subnet mask address 2-90

subscription

- create 1-13
- delete 1-13
- display 1-84

- support file 1-18, 2-98
- Switch data window 2-74
- Switch Fault LED 2-73
- switch module
 - add 2-37
 - administrative state 1-58, 2-84
 - configuration 1-62, 2-82
 - configuration defaults 1-45
 - configuration display 1-96
 - delete 2-38
 - displaying information 2-72
 - Fault LED 2-73
 - hard reset 1-31, 2-81
 - hot reset 2-81
 - icons 2-39
 - location 3-5
 - log 1-79
 - management service 1-76, 2-88
 - manufacturer information 1-105
 - operational information 1-89
 - paging 2-79
 - properties 2-83
 - replace 2-38
 - reset 1-112, 2-80
 - reset without POST 1-45, 2-81
 - restore factory defaults 2-94
 - selecting 2-12
 - services 1-44, 1-75, 1-105
 - status 2-11
 - symbolic name 2-83
 - upgrade 2-97
- symbolic name
 - port 2-112
 - switch 2-83
- syslog 2-90
- system configuration
 - change 1-79
 - defaults 1-50
 - display 1-105
- system services 2-88

T

- Telnet
 - interface 1-1
 - service 1-75, 2-89
 - session timeout 1-79
- Test command 1-109
- testing ports 3-2
- time 1-21
 - synchronization 2-80
 - zone 1-58
- timeout
 - Admin session 1-79
 - Telnet session 1-79
- timeout values 2-87
- tool bar
 - standard 2-8
 - zoning 2-56

- Topology window
 - arrange icons 2-12
 - data windows 2-13
 - menus 2-6
 - usage 2-11
- transceiver status 2-102
- transmission speed 2-110
- trap
 - authentication 3-5
 - community 3-5
 - configuration 3-6
 - SNMP version 3-6

U

- upgrade 1-22
- Uptime command 1-112
- user account
 - add 1-113
 - create 2-68
 - default 2-67
 - delete 1-113
 - display 1-113
 - edit 1-113
 - list 1-113
 - logged in 1-90
 - modify 2-71
 - password 2-70
 - remove 2-69
 - security 2-25
- User command 1-113

V

- version snapshot 2-35
- Virtual Interface preference routing 1-61

W

- web server 2-3
- Whoami command 1-116
- wizard zoning 2-3
- working
 - directory 2-17, 3-10
 - status indicator 2-10
- workstation 2-2
- write community 3-5

Z

- zone
 - access control list 2-51
 - add member port 1-117, 2-62
 - copy 1-117, 2-60
 - create 1-117, 2-61
 - definition 2-51
 - delete 1-117
 - delete member port 1-118
 - list 1-117
 - list members 1-117

- name server 2-51
- remove 2-60, 2-63
- remove all 2-63
- remove member port 2-63
- rename 1-118, 2-62
- soft 2-51
- type 1-118, 2-63
- Zone command 1-117
- zone merge
 - description 2-65
 - failure 2-65
 - failure recovery 2-65
- zone set
 - activate 1-120, 2-60
 - active 1-122, 2-46, 2-52
 - add member zone 1-120
 - copy 1-120
 - create 1-120, 2-59
 - deactivate 1-45, 1-120, 2-60
 - definition 2-52
 - delete 1-120
 - delete member zone 1-121, 2-60
 - display 1-120
 - display active 1-120
 - display members 1-121
 - display zones 1-118
 - management 2-59
 - orphan 2-52
 - remove 2-60
 - rename 1-121, 2-62
 - tree 2-55
- Zoneset command 1-120
- zoning
 - configuration 1-64, 2-57
 - configuration defaults 1-47
 - configuration display 1-96
 - database 1-45, 2-52, 2-54, 2-87
 - default 2-58
 - edit 1-122
 - history 1-122
 - limits 1-123
 - list definitions 1-123
 - remove all 2-59
 - revert changes 1-123
 - save edits 1-123
 - wizard 2-53
- Zoning command 1-122
- zoning wizard 2-3

