IBM 3534 SAN Fibre Channel Managed Hub

User's Guide

The IBM License Agreement for Machine Code is included in this book. Carefully read the agreement. By using this product you agree to abide by the terms of this agreement and applicable Copyright Laws.

GC26-7391-02

IBM 3534 SAN Fibre Channel Managed Hub User’s Guide

GC26-7391-02

Note:

Before using this information and the product it supports, read the information in “Safety and environmental notices” on page xv and “Notices” on page 383.

Third Edition (June 2001)

This edition replaces GC26-7391-01.

Publications are not stocked at the address given below. If you want additional IBM publications, ask your IBM representative or write the IBM branch office serving your locality.

A form for your comments is provided at the back of this publication. If the form has been removed, address your comments to:

International Business Machines Corporation
RCF Processing Department
Dept. G26/Bldg. 050-2
5600 Cottle Road
San Jose, CA 95193-0001
U.S.A.
FAX: 1-800-426-6209

You can also send your coments electronically to:

starpubs@us.ibm.com

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Contents

Figures xi

Tables xiii

Safety and environmental notices xv

Translated safety notices xv
Safety inspection xv
  Remove ac power xv
  External machine checks xv
Battery notice xvi
Product recycling xvi
Laser safety xvi
General restrictions xvi
Usage restrictions xvii

About this book xix

Who should use this book xix
Where to start xix
Related publications xx
Web sites xx

Chapter 1. Introduction 1

Overview of the 3534 Managed Hub 1
  Performance 2
  Manageability 2
System components 2
  GBICs 2
  Fibre-optic cable connections 5
  Serial port connection 6
  Serial cabling and emissions requirements 7
  Ethernet connection 7
  Front panel LED status indicators 8
  3534 Managed Hub power on (ready) indicator 9
Overview of diagnostics 9
  Verifying power-on self-test (POST) 9
  Running diagnostics 10

Chapter 2. Installing the 3534 Managed Hub 13

Preinstallation checklist 13
Setting the IP address 14
  Setting the 3534 Managed Hub name 15
  Setting the IP address using the serial port 16

Setting the IP address using the Ethernet port 22
Verifying 3534 Managed Hub installation .24
Downloading firmware 24
Downloading firmware from a UNIX host 25
Downloading firmware from a Windows host 26

Chapter 3. IBM StorWatch Managed Hub Specialist 27
Overview of the StorWatch Specialist 27
Launching the StorWatch Specialist 28
StorWatch Specialist views 28
Fabric view 29
Fabric Topology view 31
Name Server Table view 33
Zone Administration interface 34
StorWatch Switch view 41
Port Statistics view 44
Performance view 47
Administrative interface 48
Telnet interface 58

Chapter 4. Feature code upgrades 59
IBM 3534 Entry Fabric Switch feature code upgrade 59
Fabric Watch feature code upgrade 60
Threshold behavior models 61
Installing Fabric Watch 63
Installing Fabric Watch through Telnet 63
Installing Fabric Watch using the IBM StorWatch Specialist . .64
Using Fabric Watch 64
Classes 65
Threshold naming conventions 68
Events 69
Alarms 70
Configuring thresholds and alarms 71
Telnet commands overview 72
Telnet commands 73
Fabric Watch view (optional software) 77
Hub view 82
Getting help 82
Getting software updates 83

Chapter 5. Zoning 85
Overview 85
Increased SAN control 86
Functions of zoning 87
Uses for zoning 87
Zoning concepts 88
Zone definition 88
Zoning components 88

Zone members 88
Zone aliases 89
Zone configurations 89
Example of zone configuration 90
Using zoning 91
Zoning setup and administration 92
Zone management 92
Enforcing a zone 92
Adding multiple items 92
Multiswitch fabrics 93
Zoning commands 95
Zone alias commands 96
Zone configuration commands 98
Zone commands 99
Configuration management commands 101

Chapter 6. QuickLoop 103
Features 103
User interfaces 103
QuickLoop configurations 104
QuickLoop commands 106
qlPartner 106
qlShow 107
Using the StorWatch Specialist 108
Fault isolation 109
Hub level 109
Port level 109

Chapter 7. QuickLoop Zoning 111
Using QuickLoop zones 112
QuickLoop zoning advantages 112
QuickLoop zones 112
Configuring QuickLoop zones 113
QuickLoop zones using ports 114
Arbitrated loop physical address (AL_PA) zoning 116
Creating zones 116

Chapter 8. Managing the 3534 Managed Hub with SNMP . . . 119
SNMP transports 121
MIB-II support 121
Fabric element MIB support 121
Vendor-unique MIB 122
Generic traps 122
Enterprise specific traps 123
Agent configuration 123
Available MIB and trap files 124
syslog daemon 124
syslogd support 125

Error message format 125
Message classification 126
Switch configuration 127
syslogd configuration 128

Appendix A. Error messages 129
Fan error message 129
Port error messages 129
Thermometer error message 130

Appendix B. Commands 131
agtcfgDefault 132
agtcfgSet 135
agtcfgShow 138
aliasShow 141
backspace 143
bcastShow 144
camTest 146
centralMemoryTest 147
cmemRetentionTest 149
cmiTest 151
configDefault 153
configDownload 155
configShow 158
configUpload 160
configure 163
crossPortTest 170
date 175
diagClearError 177
diagDisablePost 179
diagEnablePost 181
diagHelp 183
diagShow 184
dlsReset 186
dlsSet 187
dlsShow 189
errDump 190
errShow 191
fabricShow 196
fanShow 198
fastboot 199
firmwareDownload 200
fspfShow 202
fwClassInit 204
fwConfigReload 205
fwConfigure 206
fwShow 209
gbicShow 211
h 213

help 215
i 216
ifModeSet 218
ifModeShow 220
ifShow 221
interfaceShow 223
iodReset 228
iodSet 229
iodShow 230
ipAddrSet 231
ipAddrShow 233
licenseAdd 235
licenseHelp 236
licenseRemove 237
licenseShow 238
linkCost 239
login 241
logout 242
loopdiagClear 243
loopdiagDone 244
LSDbShow 245
mcastShow 248
msConfigure 250
msPlatShow 252
msPlCapabilityShow 254
msPlClearDB 256
msPIMgmtActivate 257
msPIMgmtDeactivate 259
nbrStatsClear 261
nbrStateShow 264
nsAllShow 266
nsShow 268
parityCheck 270
passwd 272
portCfgEport 274
portCfgGport 276
portCfgLport 278
portCfgLongDistance 280
portcfgMcastLoopback 282
portDisable 284
portEnable 285
portErrShow 286
portLogClear 288
portLogDump 290
portLogShow 292
portLoopbackTest 297
portPerfShow 300
portRegTest 301
portRouteShow 303
portShow 305

portStatsShow 308
psShow 311
qlPartner 312
qloopEnable 314
qloopShow 316
quietMode 318
ramTest 319
reboot 322
routeHelp 323
setGbicMode 324
setSplbMode 325
spinSilk 327
sramRetentionTest 332
supportShow 334
switchBeacon 336
switchDisable 338
switchEnable 339
switchName 341
switchShow 343
switchStatusPolicySet 346
switchStatusPolicyShow 348
switchStatusShow 350
syslogdIpAdd 352
syslogdIpRemove 353
syslogdIpShow 354
tempShow 355
topologyShow 356
trackChangesSet 359
uptime 361
uRouteConfig 363
uRouteRemove 365
uRouteShow 366
version 368
zoneAdd 370
zoneCreate 372
zoneDelete 374
zoneRemove 375
zoneShow 377

Appendix C. Veritas DMP settings in the fabric environment 379
Introduction 379
Analysis 379
Resolution and workaround 379
Veritas Dynamic MultiPathing (DMP) 379
Host bus adapter settings 380
Solaris sd driver parameter settings 380

Notices 383
Trademarks 384

Electronic emission notices 384
Federal Communications Commission (FCC) statement . . . 384
Industry Canada compliance statement 385
European community compliance statement 385
Germany compliance statement 385
Japanese Voluntary Control Council for Interference (VCCI) class 1 statement 386
Taiwan Class A compliance statement 387
IBM license agreement for machine code 387
Statement of limited warranty 388
Production status 388
IBM warranty for machines 388
Warranty service 389
Extent of warranty 390
Limitation of liability 390

Glossary 393

Index 397

Figures

1. IBM 3534 SAN Fibre Channel Managed Hub faceplate 1
2. SWL fiber-optic GBIC (part number and labeling varies) 3
3. LWL fiber-optic GBIC module (part number and labeling varies) 4
4. GBIC port 4
5. Front end of the GBIC 4
6. Dual SC fiber-optic plug connector 5
7. Serial port connections 6
8. Serial Port connections 16
9. Connection Description window 17
10. Connect To window 18
11. COM1 Properties window: Port Settings tab 19
12. Settings - Emulation window 20
13. HyperTerminal session 21
14. Ethernet port connections 22
15. Fabric view 30
16. Fabric Topology view 32
17. Name Server Table view 33
18. Zone Alias Settings view 36
19. Zone Settings view 38
20. Zone Config Settings view 40
21. Switch view 42
22. Port Statistics view 44
23. Performance view 47
24. Switch Admin view 49
25. User Admin view 51
26. Firmware Upgrade view 52
27. Reboot Switch view 53
28. SNMP Admin view 54
29. License Admin view 56
30. QuickLoop Admin view 57
31. Telnet Session in Use dialog box 58
32. Example of range threshold: temperature (Celsius) 61
33. Example of rising and falling threshold: error rate 62
34. Threshold tab in the Fabric Watch view 78
35. Boundaries Config tab in the Fabric Watch view 79
36. Alarm Config tab in Fabric Watch view 81
37. A fabric with three zones 86
38. Example of zone configuration 91
39. QuickLoop configuration showing a single switch 105
40. QuickLoop configuration showing two switches 106
41. QuickLoop configuration view 108
42. Port-based zoning 115
43. Zone Administration view 118
44. MIB tree 120

Tables

1. Cabling connections 5
2. Cabling pinouts 7
3. Front panel LED status indicators 8
4. Power-on self-tests 9
5. Offline and online tests 10
6. Customer preinstallation checklist 13
7. Fabric Watch classes and areas 66
8. Valid class name abbreviations 68
9. Fabric Watch Telnet commands 72
10. Zoning commands 95
11. Zoning rules 112
12. syslog message classification 127
13. Arbitrated loop settings 164
14. Switch fabric settings 164
15. System service settings 166
16. Virtual channel settings 167
17. Diagnostic error numbers 192
18. Error message description 273
19. Description of the portlogShow fields 292
20. Descriptions of the reasons for the last start of the switch 361

Safety and environmental notices

Safety notices are printed throughout this book. Danger notices warn you of conditions or procedures that can result in death or severe personal injury. Attention notices indicate the possibility of damage to a program, device, system, or data.

Translated safety notices

The translation of the safety notices found in this book are contained in a separate book. See *IBM External Devices Safety Information* for a translation of the Danger notices.

Translated notices are easy to locate in the safety information manual as they are in numeric order. Look for the ID number (72XXD201) in the following example.

DANGER

An electrical outlet that is not correctly wired could place hazardous voltage on metal parts of the system or the products that attach to the system. It is the customer’s responsibility to ensure that the outlet is correctly wired and grounded to prevent an electrical shock. (72XXD201)

Safety inspection

Perform the following safety checks to identify unsafe conditions. Be cautious of potential safety hazards that are not covered in the safety checks. If unsafe conditions are present, determine how serious the hazards are and whether you should continue before correcting the problem.

Remove ac power

Perform the following steps to remove ac power.

1. Perform a controlled system shutdown.
2. Disconnect the power cord from the power source.

External machine checks

Attention: IBM authorizes only trained service personnel to open this machine. It is designed to be serviced at the factory.

Perform the following external machine checks.

1. Verify that all external covers are present and not damaged.
2. Ensure that all latches and hinges are in correct operating condition.
3. If the 3534 Managed Hub is not installed in a rack cabinet, check for loose or broken feet.
4. Check the power cord for damage.
5. Check the external signal cable for damage.
6. Check the cover for sharp edges, damage, or alterations that expose the internal parts of the device.
7. Correct any problems that you find.

Battery notice

A lithium battery can cause fire, explosion, or a severe burn. Do not recharge, disassemble, heat above 100°C (212°F), solder directly to the cell, incinerate, or expose the cell contents to water. Keep away from children. Replace only with the part number specified for your system. Use of another battery can present a risk of fire or explosion. The battery connector is polarized; do not attempt to reverse the polarity. Dispose of the battery according to local regulations.

Product recycling

This unit contains recyclable materials. Recycle these materials where processing sites are available and according to local regulations. In some areas, IBM provides a product take-back program that ensures proper handling of the product. Contact your IBM representative for more information.

Laser safety

This unit might contain a single-mode or multimode transceiver, which are class 1 laser products. The transceivers comply with IEC 825-1 and FDA 21 CFR 1040.10 and 1040.11. The transceiver must be operated under the recommended operating conditions.

General restrictions

The classification is valid only if the module is operated within the specified temperature and voltage limits. The system using the module must provide power supply protection. The +3.3 V/+5 V system power source must cease to operate if there is an overload at the power source.

The operating temperature of the module must be in the temperature range given in the recommended operating limits. These limits guarantee laser safety.

Usage restrictions

The optical ports of the modules must be terminated with an optical connector or with a dust plug.

About this book

The *IBM 3534 SAN Fibre Channel Managed Hub User's Guide* provides information on the following:

- Overview of the IBM 3534 Fibre Channel Managed Hub
- Installing the IBM 3534 Fibre Channel Managed Hub
- Using the IBM 3534 SAN Fibre Channel Managed Hub StorWatch™ Specialist
- Upgrades and feature description
- Managing and monitoring a hub using zoning
- Managing a hub remotely

Who should use this book

This book is intended for customers and for network and system administrators whose responsibility includes administration and management of a storage area network.

Before using this book, you must know how to service, analyze, isolate, report, and resolve problems for the 3534 Managed Hub hardware. You must also know how to safely work with electrical components.

Note: Throughout this book, the term *switch* applies to both switches and hubs unless otherwise noted.

Note: Throughout this book, the IBM StorWatch SAN Fibre Channel Managed Hub Specialist is referred to as the StorWatch Specialist.

Where to start

When performing any service action on the 3534 Managed Hub, be sure to follow the directions in the *IBM 3534 SAN Fibre Channel Managed Hub Installation and Service Guide*. This ensures that you use the correct service, turn on, and turn off procedures for the 3534 Managed Hub. Failure to follow these instructions can cause damage to the 3534 Managed Hub.

Related publications

Additional information related to the 3534 Managed Hub can be found in the following publications:

- *IBM 3534 SAN Fibre Channel Managed Hub Installation and Service Guide,* SY27-7616
- *IBM External Devices Safety Information*, SA26-7003
- *Electrical Safety for IBM Customer Engineers,* S229-8124
- *IBM SAN Fibre Channel Switch 2109 Model S08 Installation and Service Guide, SC26-7350*
- Fibre Channel Standards, see "Web sites".

Web sites

For additional information about storage products, see the Web site at:

www.ibm.com/storage/fchub/

For detailed information about the fibre-channel standards, see the Fibre Channel Association Web site at:

www.fibrechannel.com/

Chapter 1. Introduction

Note: Throughout this book, the term *switch* applies to both switches and hubs unless otherwise noted.

The IBM 3534 SAN Fibre Channel Managed Hub is an 8-port fibre-channel hub that consists of a system board with connectors for supporting up to eight ports. This includes seven fixed shortwave optic ports, one gigabit interface converter (GBIC) port, and an operating system for building and managing a switched loop architecture.

Figure 1 shows the faceplate of the 3534 Managed Hub. Ports are numbered sequentially from the left port, starting with zero. The 3534 Managed Hub faceplate includes a silk-screen imprint of the port numbers.

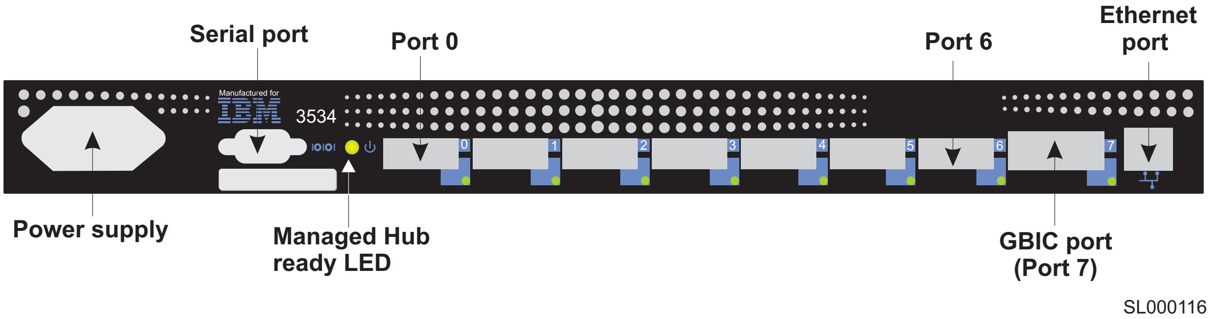


Figure 1. IBM 3534 SAN Fibre Channel Managed Hub faceplate

Overview of the 3534 Managed Hub

The 3534 Managed Hub is a high-performance fibre-channel managed hub that has the following characteristics:

Simple The 3534 Managed Hub is easy to set up and configure. After power-on self-test (POST), you need only add the internet protocol (IP) address of the 3534 Managed Hub. The remainder of the setup for the 3534 Managed Hub is automated.

Flexible GBIC modules and fixed optic ports support fiber transmission media.

Reliable The 3534 Managed Hub uses highly integrated, reliable, multifunction application specific integrated circuit (ASIC) devices.

High performance
The 3534 Managed Hub uses a low-latency, high-performance design that requires no central processing unit (CPU) data path interaction, resulting in a data transfer latency of less than 2 µs from any port to any port at peak fibre-channel bandwidth of 100 MBps when there is no port contention.

Extendable

The 3534 Managed Hub can be connected to another 3534 Managed Hub to expand the loop capabilities to 14 ports. It can also be connected with a single port into a storage area network (SAN) fabric as a loop extension.

Performance

A minimum aggregate routing capacity of 4 000 000 frames per second is specified for class 2, class 3, and class F frames. Nonblocking throughput of up to 800 MBps (0.8 GBps) is provided.

Manageability

The 3534 Managed Hub can be managed using the serial port or the 10BASE-T or 100BASE-T Ethernet port. Management interfaces include Telnet or Web-based management using the StorWatch Specialist.

System components

The system board is enclosed in an air-cooled chassis, which can be either mounted in a standard rack or used as a stand-alone unit. The chassis includes a power supply, a fan tray, an RJ-45 Ethernet connection for 3534 Managed Hub setup and management, and a serial port. The serial port is used for recovering factory settings only and initial configuration of the IP address for the 3534 Managed Hub if the default address is not known.

GBICs

Important: Do not look into the end of a fibre-optic cable or into a fibre optic receptacle. This unit contains a class 1 laser.

The 3534 Managed Hub accommodates one GBIC module. All interfaces have status lights that are visible from the front panel, giving a quick, visual check of the port status and activity.

The GBIC modules that are supported are the short wavelength (SWL) and long wavelength (LWL) fiber-optic versions.

SWL fiber-optic GBIC module

The SWL fiber-optic GBIC module, with the SC connector color-coded black, is based on SWL lasers supporting 1.0625 GBps link speeds. This GBIC module supports 50-µm multimode fiber-optic cables, with cables up to 500 m (1640 ft) in length. The GBIC module is shipped with a protective plug in place, which remains in place if no fiber-optic cable is connected to the port. Figure 2 shows an SWL GBIC module.

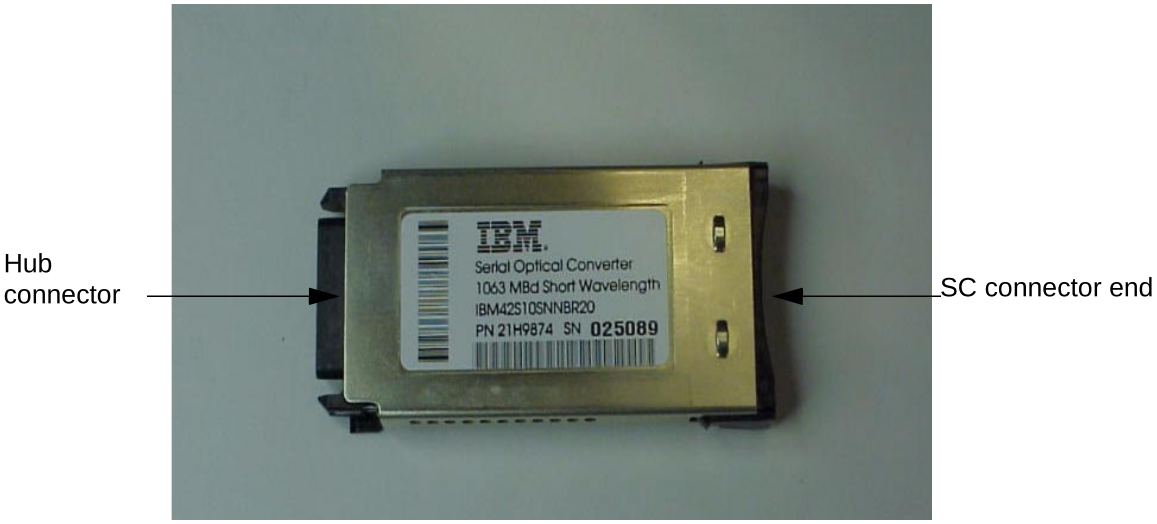


Figure 2. SWL fiber-optic GBIC (part number and labeling varies)

The SWL fibre optic GBIC module uses a class 1 laser, which complies with the 21 CFR, subpart J as of the date of manufacture.

LWL fiber-optic GBIC module

The LWL fiber-optic GBIC module, with SC connector color-coded blue, is based on long wavelength 1300 nm lasers supporting 1.0625 GBps link speeds. This GBIC module supports 9-µm, single-mode fiber-optic cable. Cables up to 10 km (6.2 mi) in length, with a maximum of five splices, can be used. The GBIC module is shipped with a protective plug in place. The protective plug should remain in place if no fiber-optic cable is connected to the port. Figure 3 shows an LWL fiber-optic GBIC module.

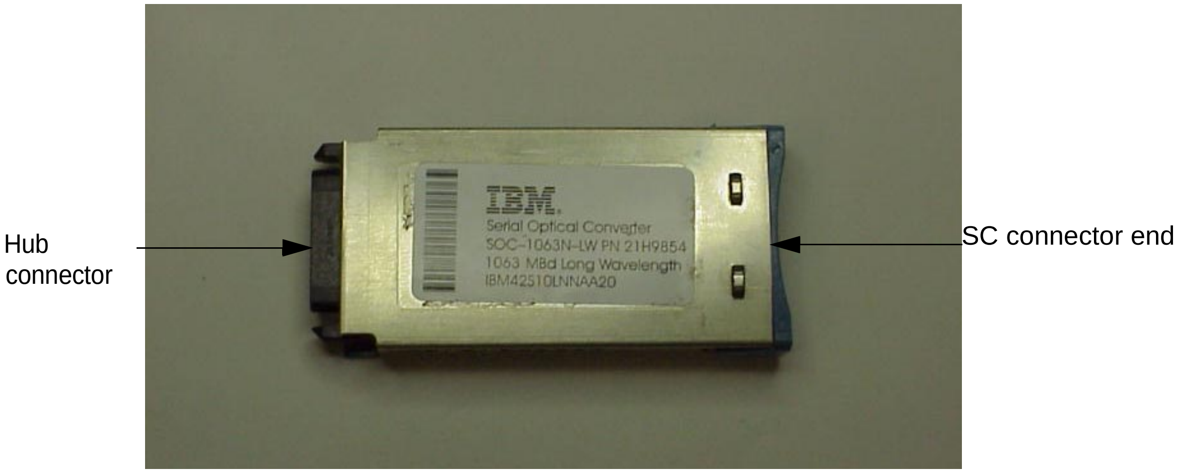


Figure 3. LWL fiber-optic GBIC module (part number and labeling varies)

Installing GBICs

The 3534 Managed Hub comes with seven fiber-optic ports (ports 0 - 6) and one GBIC port (port 7). See Figure 4.

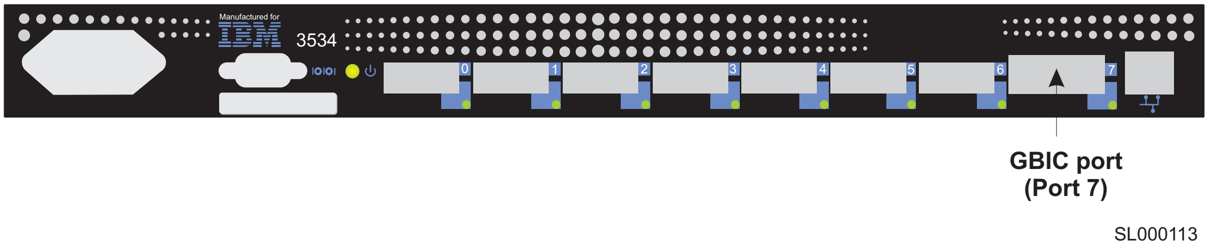


Figure 4. GBIC port

Figure 5 shows the front end of the GBIC, with the dust protection rubber plug removed. The plug should be left inserted in the GBIC until a fibre-channel cable is inserted. The other end of the GBIC is inserted into the 3534 Managed Hub. The GBICs are keyed and only seat if they are inserted correctly.

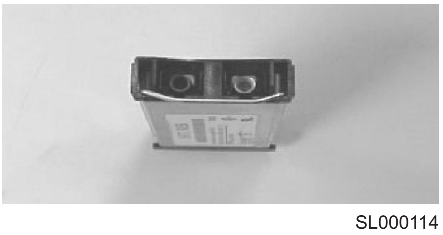


Figure 5. Front end of the GBIC

Fibre-optic cable connections

All network cable connections are made to the front panel of the 3534 Managed Hub. All recommended cabling supports the 1.0625 GBps transfer rate of the 3534 Managed Hub, as shown in Table 1.

Table 1. Cabling connections

Cable type	Cable specifications	Maximum cable length	GBIC module optical wavelength
SWL fiber-optic	• Duplex SC plug connectors • Multimode fiber • 50 µm core diameter • 125 µm cladding diameter duplex cable	500 m (1641 ft)	780 - 860 µm without open fiber control (non-OFC)
LWL fiber-optic	• Duplex SC plug connectors • Single mode fiber • 9 µm core diameter • 125 µm cladding diameter duplex cable	10 km (32 808 ft)	1270 - 1350 µm without open fiber control (non-OFC)

Attention: To prevent damage to the housing or to prevent scratching the fiber-optic end, use extreme care when removing or installing connectors. To prevent contamination, always install protective covers on unused or disconnected components.

Attention: When removing the protective plug from the GBIC or the fiber-optic ports, do not force the fiber-optic plug into the GBIC or the fiber-optic ports module. This can damage the connector, the GBIC, and the fiber-optic ports. Make sure the fiber surface is clean and free of dust or debris before inserting the connector into the GBIC or fiber-optic ports.

Fiber cable connections are made to the front panel using the 3534 Managed Hub standard dual SC plug connectors, as shown in Figure 6.

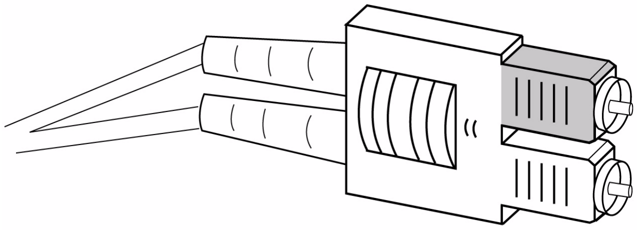


Figure 6. Dual SC fiber-optic plug connector

The connectors are keyed and must be inserted into the connector on the GBIC module with the correct alignment. In most cases, one of the two connector plugs is a different color to aid in proper connector alignment.

Serial port connection

Attention: For dust and ESD protection, the 3534 Managed Hub includes a cover for the serial port. When not in use, keep the serial port covered.

The 3534 Managed Hub includes a serial port that is used to set the IP address when setting up or reinitializing a 3534 Managed Hub or when running diagnostics. It is not used during normal operation. Figure 7 shows the serial port connections. The settings are:

- 8-bit
- No parity
- One stop-bit
- 9600 baud
- Flow control = none
- Emulation = auto detect

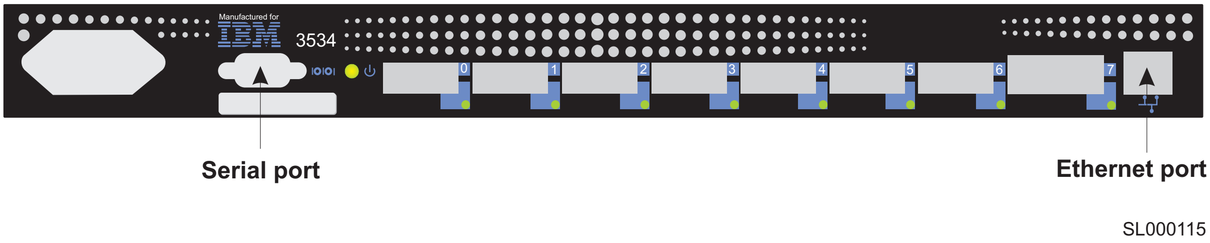


Figure 7. Serial port connections

Note: The serial port and Telnet connection are mutually exclusive; there can be only one serial port session active at a time. Telnet takes priority, so the serial port is terminated when a Telnet connection is made. The serial port connection is restored after the Telnet session is completed, but you must log in again. A password is required to log in to the serial port session because password checking is skipped only at initial startup.

Serial cabling and emissions requirements

The 3534 Managed Hub uses a standard serial cable with a male 9-pin D-subminiature connector. Only pins 2, 3, and 5 are required and are supported. Table 2 shows the cabling pinouts.

Table 2. Cabling pinouts

Pin	Signal	Description
1		
2	TxData	Transmit data
3	RxData	Receive data
4		
5	GND	Logic ground
6		
7		
8		
9		

Ethernet connection

Connecting the 3534 Managed Hub to an existing 10BASE-T or 100BASE-T Ethernet local area network (LAN) through the front panel Ethernet port provides the following:

- Gives access to the internal SNMP agent of the 3534 Managed Hub
- Permits remote Telnet and Web access for remote monitoring and testing
- Permits the setting or changing of the IP address

Note: The connection is only for Telnet, single network management protocol (SNMP) agent, and the Web-based server access. No fabric connection is used through this connection.

Front panel LED status indicators

The color and flash speed of each LED port, as described in Table 3, indicates the individual port status.

Table 3. Front panel LED status indicators

Front panel LEDs	Status
No light showing	No light or signal carrier (no module, no cable) for media interface LEDs.
Steady yellow	Receiving light or signal carrier, but the attached device is not yet online.
Slow yellow (See note 1)	Disabled (the result of diagnostics or the **portDisable** command).
Fast yellow (See note 2)	Error, fault with the port.
Steady green	Online (connected with device over cable).
Slow green (See note 1)	Online, but segmented (loopback cable or incompatible hub).
Fastgreen (See note 2)	Internal loopback (diagnostic).
Flickering green	Online and frames are flowing through the port.
Green and yellow	The port is bypassed.
Note 1: Slow: blinks at 2-second intervals **Note 2**: Fast: blinks at one-half second intervals	

Each 3534 Managed Hub port includes an LED indicator. If port 7 does not have a GBIC installed, the LED is off. If a problem has been detected with the port, the LED indicators provide some indication of the type of problem. Faults and problems are indicated by a yellow port indicator.

When a GBIC is installed (port 7 only) and a cable is connected to a properly functioning fibre-channel device, the LED indicator is steady green. If a slow green blink is observed, it indicates the port is detecting light but cannot make a proper fabric connection. This could indicate any of the following conditions:

- A loopback cable is installed.
- The fabric is segmented (an E_port connection to another switch cannot be completed).
- The 3534 Managed Hub has been connected to an incompatible switch or hub.

When frame traffic is being transferred on a port, the LED flickers fast green showing that the port is active and is transferring data.

3534 Managed Hub power on (ready) indicator

After the POST diagnostics have completed, this LED indicates that system board diagnostics have completed successfully.

Overview of diagnostics

The 3534 Managed Hub is designed for maintenance-free operation. When there is a suspected failure, the 3534 Managed Hub has self-diagnostic capabilities to help isolate any equipment or fabric failures.

The 3534 Managed Hub supports POST and diagnostic tests. The diagnostic tests are run by Telnet commands and are used to determine the status of the 3534 Managed Hub and to isolate problems.

For more information about diagnostic testing commands and procedures, see the *IBM 3534 Fibre-Channel Managed Hub Installation and Service Guide*.

Verifying power-on self-test (POST)

Table 4 lists the diagnostic tests that are automatically run during a POST.

Table 4. Power-on self-tests

Test	**Brief description**
Memory test	Checks the CPU random access memory (RAM).
Port register test	Checks the ASIC registers and static random access memory (SRAMs).
Central memory test	Checks the system board SRAMs.
CMI conn test	Checks the CMI bus between ASICs.
CAM test	Checks the content addressable memory (CAM).
Port loopback test	Checks all of the hardware of the 3534 Managed Hub to ensure that the frames are transmitted, looped back, and received.

After the 3534 Managed Hub completes the POST, the LED returns to a steady state from the blinking states that are described in Table 3 on page 8.

A yellow LED indicates that the port failed one of the POSTs.

After the 3534 Managed Hub completes the POST, any error conditions can be displayed through Telnet.

The 3534 Managed Hub ready LED can be used to verify a successful POST approximately 2 minutes after the hub is started.

Running diagnostics

For detailed information about running diagnostics, see the *3534 Fibre-Channel Managed Hub Installation and Service Guide*.

The following tests are available from the Telnet connection on the 3534 Managed Hub. The test name is followed by the command used to run the test.

- Hub offline (**switchDisable**)
- Memory test (**ramTest**)
- Port register test (**portRegTest**)
- Central memory test (**centralMemoryTest**)
- CMI conn test (**cmiTest**)
- CAM test (**camTest**)
- Port loopback test (**portLoopbackTest**)
- Cross port test (**crossPortTest**)
- Spin silk test (**spinSilk**)
- SRAM data retention test (**sramRetentionTest**)
- CMem data retention test (**cmemRetentionTest**)
- Hub online (**switchEnable**)

See Table 5 to determine which tests are run offline or online.

Attention: Offline tests are disruptive to 3534 Managed Hub operations. Do not run these tests unless you are sure that the 3534 Managed Hub operation can be disrupted.

Table 5. Offline and online tests

Offline tests	**Offline and online tests**
portRegTest	ramTest
centralMemoryTest	crossPortTest
cmiTest	
camTest	
portLoopbackTest	
spinSilk	
sramRetentionTest	

Table 5. Offline and online tests

Offline tests	**Offline and online tests**
cmemRetentionTest	

Chapter 2. Installing the 3534 Managed Hub

Note: Installation of the 3534 Managed Hub is the customer's responsibility.

This section describes the installation of the 3534 Managed Hub.

Preinstallation checklist

Complete the items in the preinstallation checklist (see Table 6) before installing the 3534 Managed Hub. Completing this checklist ensures a successful installation of the product. Some steps might need to be adapted for your host network.

Table 6. Customer preinstallation checklist

Step	Customer action or decision	Comments and references
1	• Desktop installation • Rack-mount installation	Determine whether the 3534 Managed Hub is to be installed on a desktop or is to be rack mounted.
2	Ensure that the required host platform operating system (OS) service pack is installed. For example: Microsoft® Windows NT® service pack 4. 0 (or later) and required hot fixes.	For a current list of supported platforms, required host platform code updates, and information about how to obtain them, see the Web site at: www.ibm.com/storage/fchub/ or contact IBM technical support.
3	Ensure that the required fibre-channel host bus adapter (HBA), basic input and output system (BIOS), and device driver are installed.	For a list of supported HBAs and the required BIOS and device driver, see the Web site at: www.ibm.com/storage/fchub/
4	Ensure that the disk or tape systems to be installed are compatible. Ensure that the device driver is installed or updated.	This is usually performed by a service representative during target device installation. For a list of supported systems and the required BIOS and device driver, see the Web site at: www.ibm.com/storage/fchub/
5	Ensure that all host fibre-channel cables have been: • Ordered with the product or have been preinstalled and checked. • Labeled with the host system identifier and the 3534 Managed Hub identifier.	Refer to the HBA specification provided with your HBA to determine the required cables, host system identifier, and 3534 Managed Hub identifier. For example, label the intended port or zone location.

Table 6. Customer preinstallation checklist (continued)

Step	Customer action or decision	Comments and references
6	Decide on the 3534 Managed Hub network parameters. Ethernet port configuration decisions: **Attention:** Save this configuration for future reference. • Static IP address _____________ • Netmask (if required) _____________ If the 3534 Managed Hub is not on the same TCP/IP subnet as the server (see note), assign the default network gateway address or route table entries.	**Attention:** Using incorrect network parameters can cause problems on the Ethernet network. Obtain the 3534 Managed Hub network parameters from your network administrator.
7	Set the 3534 Managed Hub name using the Telnet command **switchName**.	The 3534 Managed Hub name must resolve to the internet protocol (IP) address on the host system that uses the StorWatch Specialist. Do so even when using the IP address with your Web browser to connect to the 3534 Managed Hub. Your network administrator adds the IP address of the 3534 Managed Hub to the domain name server (DNS) or network information service (NIS). Alternately, you can perform local name resolution using a hosts file. Failure to do this results in poor performance when using a Web browser to manage the 3534 Managed Hub.
8	Attach the Ethernet cable from the server (see note) to the network hub.	None
9	Attach the Ethernet cable from the network where the 3534 Managed Hub will be installed.	None
Note: The term *server* (as used here) refers to the computer used for the StorWatch Specialist.		

Setting the IP address

The IP address can be set through the serial port or the Ethernet port. Where possible, setting the IP address through the serial port is the preferred method.

The 3534 Managed Hub is shipped from the factory with a default IP address (10.77.77.77) preinstalled. This IP address is printed on the label on the top front edge of the 3534 Managed Hub. This address is used for the external Ethernet connection.

The customer sets a new IP address in the 3534 Managed Hub during installation. This address must be approved by the system administrator

If you can, use this default address to attach to your LAN to establish a network connection to the 3534 Managed Hub. You can change this IP address later using a Telnet command or by using the StorWatch Specialist from any server having access to the same LAN. This is the easiest way to set the IP address. You need to ask your system administrator if the default address can be used.

If using the default IP address is not possible, the IP address has to be set using the serial port or the Ethernet port. Set the IP address using the information provided by the system administrator from the preinstallation checklist (see Table 6 on page 13).

Setting the 3534 Managed Hub name

Use the **switchName** command to set the name of the 3534 Managed Hub. The new name must be enclosed in double quotes as shown in the following example. The command syntax is:

```
switchName “new_name_of_hub”
```

```
switchDomain> switchName “sw3”
Updating flash...
```

If you plan to use StorWatch Specialist to connect to the 3534 Managed Hub through a Web browser, you must first set the 3534 Managed Hub name. This name must resolve to the IP address assigned by your network administrator on the client system to connect to the 3534 Managed Hub through the StorWatch Specialist. Failure to do this results in poor performance when using a Web browser to manage the 3534 Managed Hub.

Use the **switchName** command with the NewName operand to assign a new switch name. Certain restrictions apply to a length and format of the 3534 Managed Hub name. Switch names can be up to 19 characters long, must begin with an alpha character, and can consist of alpha, numeric, and underscore characters.

Note: This command is only available to users with administrator authority.

Setting the IP address using the serial port

Note: Opening a HyperTerminal session varies depending on which version of Windows® you are using. This procedure is based on the use of a laptop computer running Windows 98.

Attention: Do not use a null modem cable. Be sure that you use the serial cable that was shipped with the 3534 Managed Hub to connect to the serial port on the 3534 Managed Hub, or another female-female cable that has straight-through connections for the signal lines.

Perform the following steps to set or change the IP address using the serial port:

1. Using the serial cable that came with the 3534 Managed Hub, connect your service terminal (PC or laptop) to the serial port before plugging the 3534 Managed Hub into the electrical outlet. See Figure 8 for serial port location.

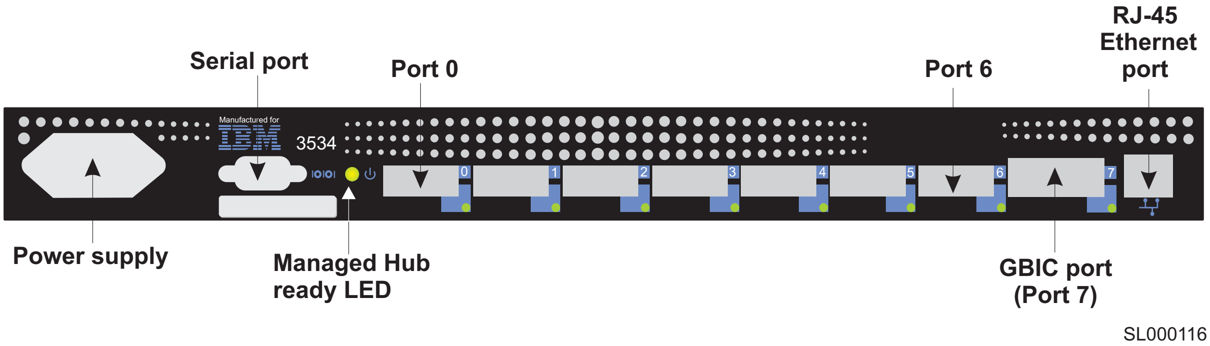
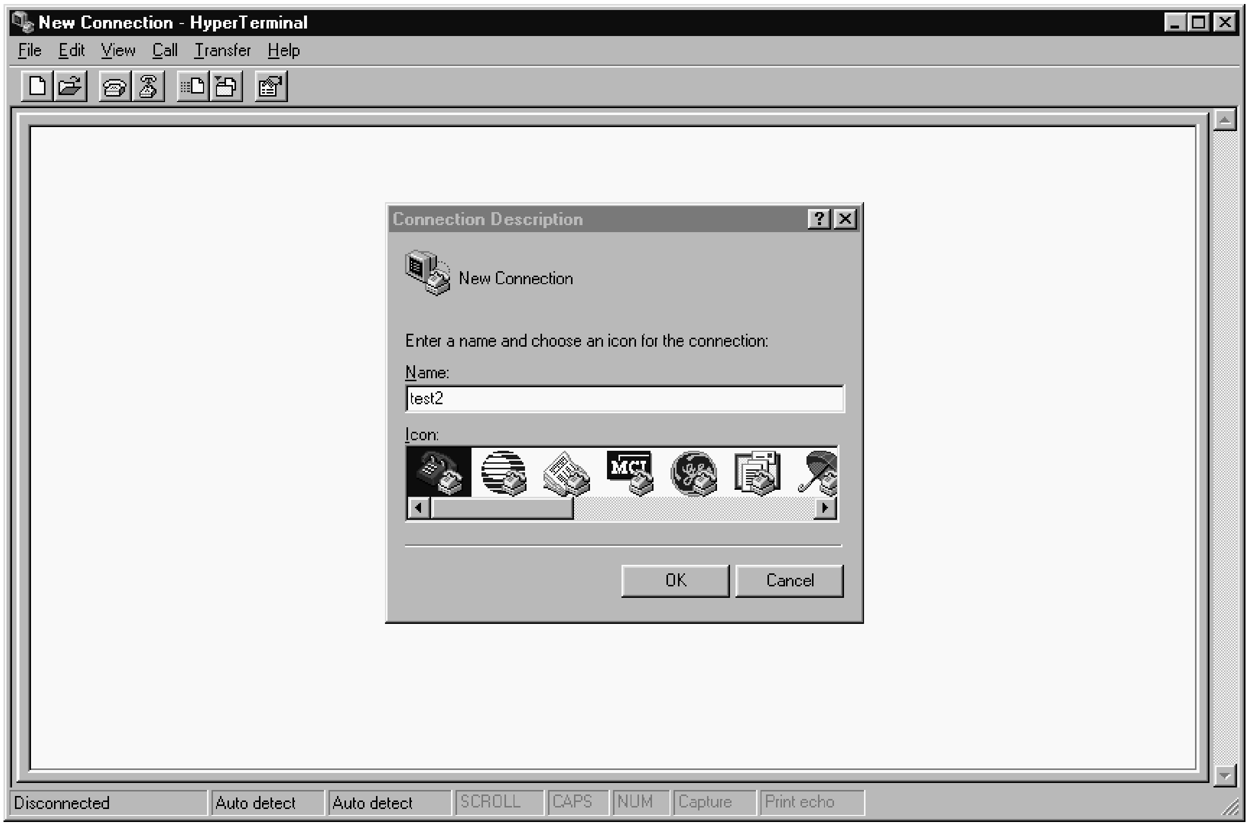


Figure 8. Serial Port connections

2. Click **Start —> Programs —> Accessories**.
3. Open a HyperTerminal session and configure it as follows:
    a. In the Connection Description window, type the name you want to use for your new session, select any icon from the **Icon** field shown in Figure 9, and click **OK**.



New Connection

Enter a name and choose an icon for the connection:

Name:

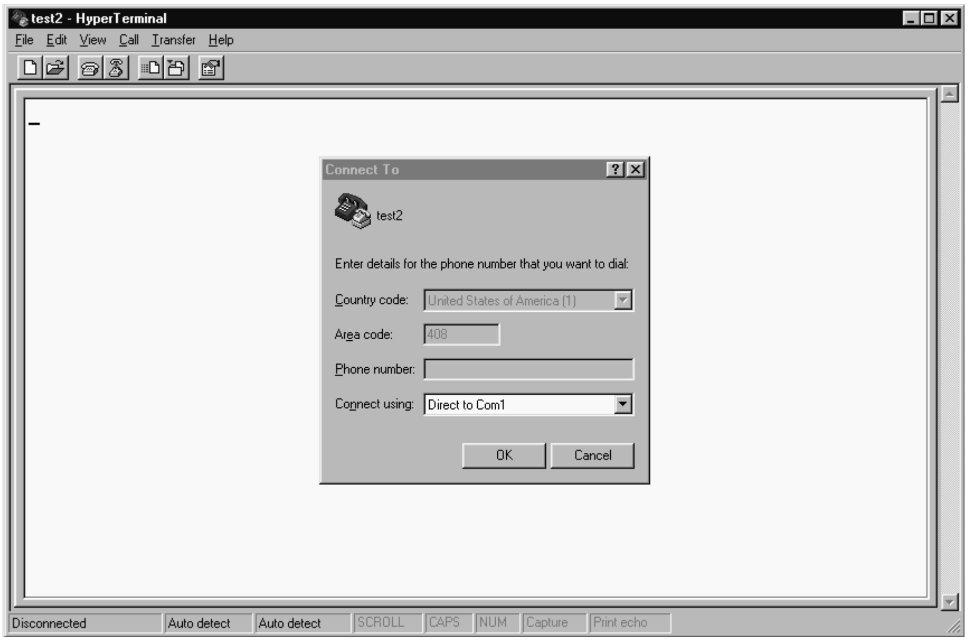
test2

Icon:

SL000117

Figure 9. Connection Description window

b. The Connect To window is displayed, as shown in Figure 10. In this window, change the **Connect using** field from the default to `Direct to Com1` and click **OK.**



test2

Enter details for the phone number that you want to dial:

Country code: United States of America (1)

Area code: 408

Phone number:

Connect using: Direct to Com1

Disconnected | Auto detect | Auto detect

SL000118

Figure 10. Connect To window

c. The COM1 Properties window is displayed as shown in Figure 11. Type the following parameters in the **Port Settings** tab:

   Bits per second: `9600`

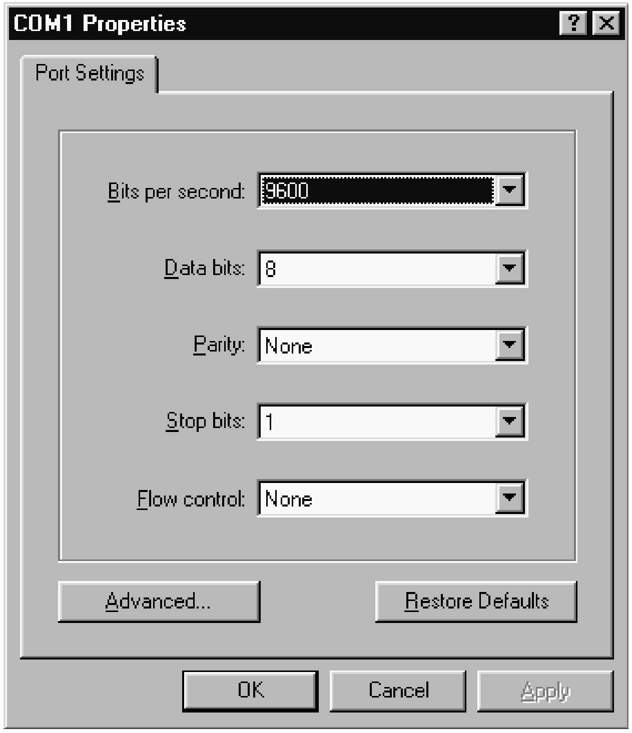
   Data bits: `8`

   Parity: `None`

   Stop bits: `1`

   Flow control: `None`

d. Click **OK**.



COM1 Properties

Port Settings

Bits per second: 9600

Data bits: 8

Parity: None

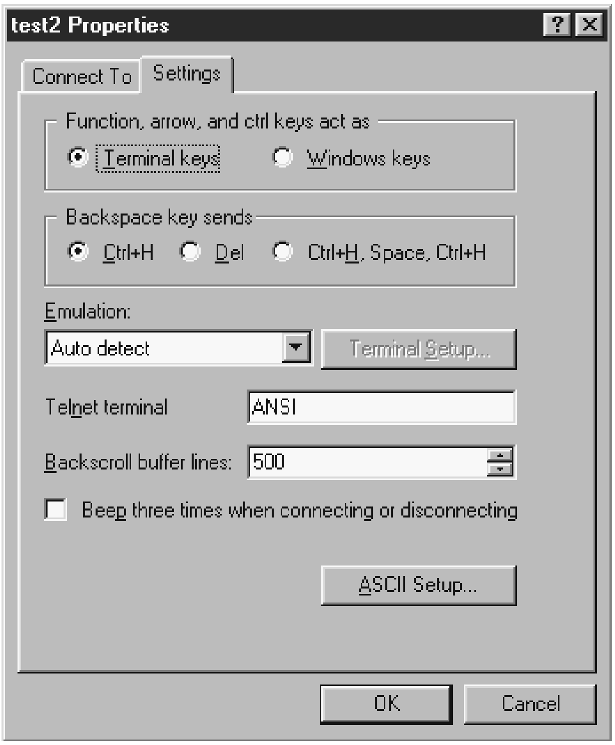
Stop bits: 1

Flow control: None

SL000119

Figure 11. COM1 Properties window: Port Settings tab

e. Click **File —> Properties**. The Properties window is displayed. Click the **Settings** tab, set the **Emulation** field to `auto detect`, as shown in Figure 12, then click **OK**.



Function, arrow, and ctrl keys act as

● Terminal keys ○ Windows keys

Backspace key sends

● Ctrl+H ○ Del ○ Ctrl+H, Space, Ctrl+H

Emulation: Auto detect

Telnet terminal ANSI

Backscroll buffer lines: 500

□ Beep three times when connecting or disconnecting

SL000120

Figure 12. Settings - Emulation window

DANGER

An electrical outlet that is not correctly wired could place hazardous voltage on metal parts of the system or the products that attach to the system. It is the customer’s responsibility to ensure that the outlet is correctly wired and grounded to prevent an electrical shock. (72XXD201)

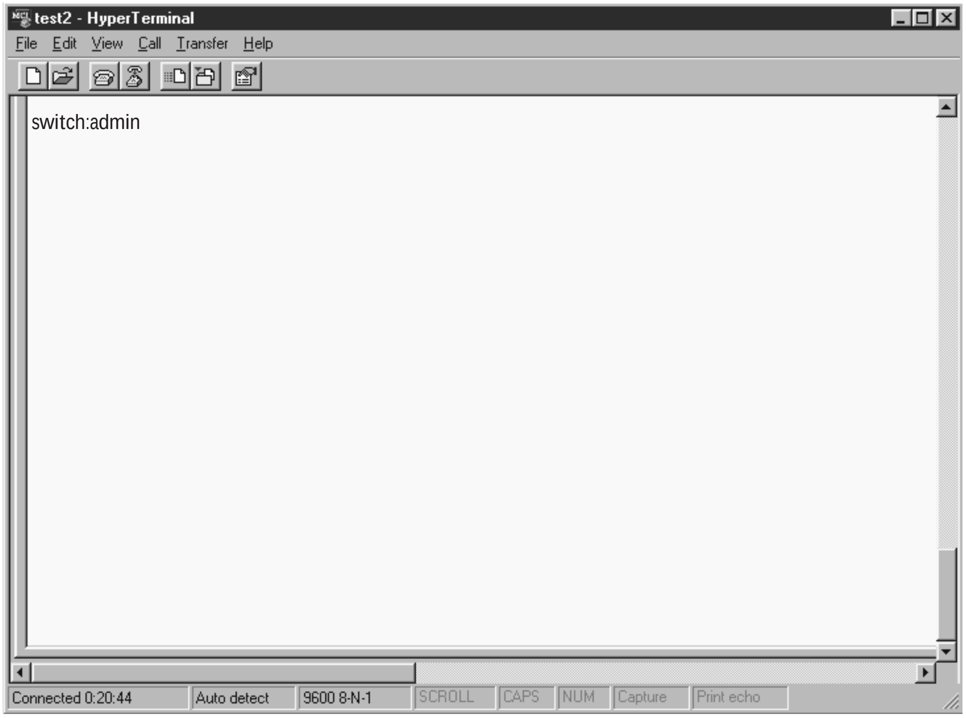
4. Start up the 3534 Managed Hub by inserting the power cord into an electrical outlet and waiting about 2 minutes for diagnostics to complete. Make sure that the power cord is fully seated into the front of the unit and that the green ready LED is on.

5. Press Enter on your service terminal (PC or laptop).

   The 3534 Managed Hub responds:

   ```
   Admin>
   ```

   The HyperTerminal session is now running, as shown in Figure 13 on page 21.



```
switch:admin
```

Figure 13. HyperTerminal session

For each prompt, type in the information as shown and press Enter at the end of each response.

a. Admin> `ipaddrSet`

   This is the command to set the IP address.

b. Ethernet IP address `[`Current ipaddress or None`]:` `new IP address`.

   This is the new address from the system administrator.

c. Ethernet Subnetmask `[`Current subnet mask or None`]`: new `Subnetmask` or press Enter.

   This is the new Subnetmask from the system administrator.

d. Fibre-channel IP address [None]`:` press Enter.

e. Fibre-channel Subnetmask [None]: press Enter.

f. Gateway address [Current Gateway address or None]: new Gateway address or press Enter.

   This is the new Gateway address from the system administrator.

g. Admin> `logout`

   This ends the Serial port session.

6. You have completed the installation of the 3534 Managed Hub. Remove the cable from the serial port connector. To check the

fibre-channel ports of the 3534 Managed Hub before turning the 3534 Managed Hub over to the system administrator, see “Verifying 3534 Managed Hub installation” on page 24.

Setting the IP address using the Ethernet port

Before attempting to set the IP address using the Ethernet port, the system administrator must provide a host on the same subnet as the 3534 Managed Hub. Set a secondary address to 10.77.77.1 (or a similar unassigned and available address other than the address of the 3534 Managed Hub) with a mask of 255.255.255.0.

If you cannot use this method, go to "Setting the IP address using the serial port" on page 16.

Perform the following steps to set the IP address using the Ethernet port:

1. Attach the LAN to the front panel of the 3534 Managed Hub by plugging an existing Ethernet 10BASE-T or 100BASE-T LAN cable to the RJ-45 connector on the front of the 3534 Managed Hub. See Figure 13 on page 21 for the RJ-45 Ethernet port location.

DANGER

An electrical outlet that is not correctly wired could place hazardous voltage on metal parts of the system or the products that attach to the system. It is the customer’s responsibility to ensure that the outlet is correctly wired and grounded to prevent an electrical shock. (72XXD201)

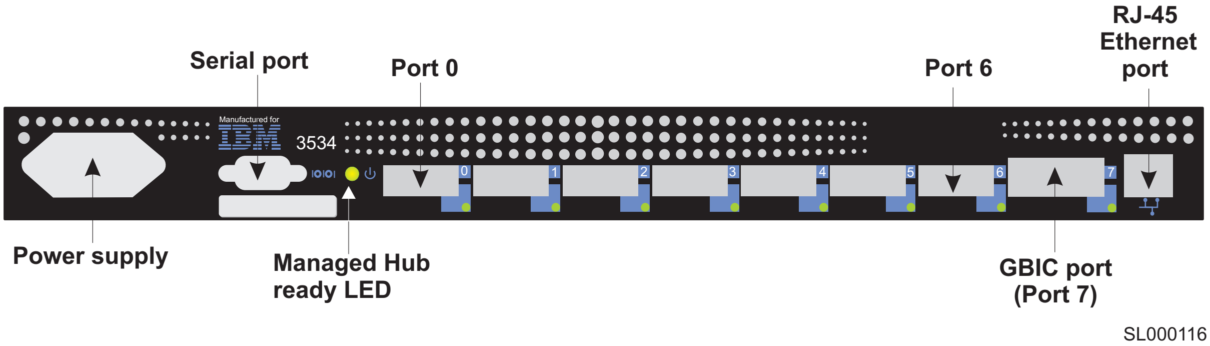


Figure 14. Ethernet port connections

2. Turn on the 3534 Managed Hub by plugging it into an electrical outlet. Make sure that the power cord is fully seated into the front of the unit, and that the green ready LED is on. Wait 2 minutes for diagnostics to complete.

3. From a LAN-attached server, type the Telnet IP address. If this is the initial installation, use the default IP address found on the label on the top left corner of the 3534 Managed Hub. If the 3534 Managed Hub has been installed before using the IP address on the label, continue using the current address on the label. If the IP address on the label

was not used, get the current IP address from the system administrator.

The 3534 Managed Hub responds with the following prompts. For each prompt, type in the information as shown and after each entry, press Enter.

a. Login: `admin`

   The 3534 Managed Hub is shipped with `admin` as the default administrator name.

b. Password: `password`

   The 3534 Managed Hub is shipped with `password` as the default password. You do not need to set the password as you type.

c. Ipaddress:admin> `ipAddrSet`

   This is the command to set the IP address.

d. Ethernet IP address [the current address will be shown]`: new IP address.`

   This is the new address provided by the system administrator.

e. Ethernet subnetmask [either the current subnetmask or the word `None` is displayed]: new `Subnetmask` or press Enter.

   This is the new subnetmask from the system administrator. If no subnetmask is required, press Enter.

f. Fibre-channel IP Address [None]: press Enter.

   Fibre-channel Subnetmask `[None]`: press Enter.

g. Gateway address [either the current gateway address or the word `None` is displayed]: enter a new gateway address or press Enter.

   This is the gateway address that the system administrator provided. If no gateway address is required, press Enter.

h. Ipaddress:admin> `logout`

   This ends the Telnet session.

4. You have completed the installation of the 3534 Managed Hub. To check the fibre-channel ports of the 3534 Managed Hub, see "Verifying 3534 Managed Hub installation" on page 24.

Verifying 3534 Managed Hub installation

To verify that the 3534 Managed Hub was installed correctly, perform the following steps:

1. Unplug the 3534 Managed Hub.

DANGER

> **An electrical outlet that is not correctly wired could place hazardous voltage on metal parts of the system or the products that attach to the system. It is the customer's responsibility to ensure that the outlet is correctly wired and grounded to prevent an electrical shock.** (72XXD201)

2. Plug the 3534 Managed Hub power cord into the electrical outlet.
3. Verify that the ready LED is on.
4. Wait 2 minutes while POST diagnostics run.
5. Verify that the ready LED is on.
6. Plug the appropriate wrap connector (black for short wavelength and gray for long wavelength) into each port, one at a time. Verify that each associated port LED is slowly blinking green.

   Ports 0 - 6 are short wavelength. If a GBIC is installed, port 7 can be either short or long wavelength.
7. If none of the checks fail, turn the 3534 Managed Hub over to the system administrator for use.

Downloading firmware

The 3534 Managed Hub is shipped with the latest level of code (firmware) available. However, when new code is released, you can easily download the new code to the 3534 Managed Hub. This task requires that you save data and executable software to your server.

The latest code can be obtained from the SAN Fibre Channel 3534 Managed Hub Web site at:

www.ibm.com/storage/fchub/

This site provides instructions for downloading the firmware and loading it on the 3534 Managed Hub. Loading new code can be done without disrupting 3534 Managed Hub activity. To make the new code functional, however, you must restart the 3534 Managed Hub.

You can download firmware to the 3534 Managed Hub from either a UNIX® host or a Windows host. For a UNIX host, no special software is needed. For Windows, you need the daemon to support a remote shell (RSH) with the firmware. This daemon is available from the SAN Fibre

Channel 3534 Managed Hub Web site. Firmware download is done using the **rpc** command running on top of TCP between the 3534 Managed Hub and the host.

Downloading firmware from a UNIX host

Perform the following procedure to download firmware from a UNIX host:

1. Download the firmware from the SAN Fibre Channel 3534 Managed Hub Web site. Remember the directory where you save the code.

   Code can only be loaded to the 3534 Managed Hub over the Ethernet LAN port.

2. Start a Telnet session to the 3534 Managed Hub from a LAN-attached server that has connectivity to the 3534 Managed Hub.

   The command format is:

   ```
   telnet [managed hub IP address]
   ```

3. Login as “admin”.

   ```
   login: admin
   ```

4. Password: `password`

   Respond to the password prompt with the current admin password. The 3534 Managed Hub is shipped with a default password of `password`.

5. Type the following command:

   ```
   firmwareDownload [“host name/IP address”], [“user
   name”], [“filename”]
   ```

   For example: `firmwareDownload “192.111.2.1”, “time”, “/tmp/os/v2.1.3”`

   The `host name` is the host name or the host IP address, the `username` is a valid host username, and the `filename` is a path to the new firmware file.

   The RSH server validates the user and delivers the file to the 3534 Managed Hub, where it is stored in flash memory.

DANGER

> **An electrical outlet that is not correctly wired could place hazardous voltage on metal parts of the system or the products that attach to the system. It is the customer’s responsibility to ensure that the outlet is correctly wired and grounded to prevent an electrical shock.** (72XXD201)

6. Unplug the 3534 Managed Hub power cord, then plug the power cord back into the electrical outlet to initiate the new firmware.

Downloading firmware from a Windows host

Perform the following procedure to download firmware from a Windows host:

1. Download the firmware from the SAN Fibre Channel 3534 Managed Hub Web site. Remember the directory where you save the code.
2. Download the two utilities (rshd.exe and cat.exe) from the Web site into the same directory as the firmware.
3. In a DOS window, type `rshd` to run the RSH daemon (there is no need to run cat.exe; this is done automatically).
4. Follow steps 2 through 6 in "Downloading firmware from a UNIX host" on page 25.

   Note: When downloading to a 3534 Managed Hub using the **firmwareDownload** command, use the UNIX directory addressing (forward slash /), not PC directory addressing (backward slash \) for the directory location in the command. For example, from NT the **firmwareDownload** command would be: `firmwareDownload “192.111.2.1”, “timm”, “/tmp/os/v2.1.3”`.

Chapter 3. IBM StorWatch Managed Hub Specialist

Note: Throughout this book, the term *switch* applies to both switches and hubs unless otherwise noted.

Note: Throughout this book, the IBM StorWatch SAN Fibre Channel Managed Hub Specialist is referred to as the StorWatch Specialist.

The StorWatch Specialist allows you to remotely monitor and manage a storage area network (SAN) of hubs and switches using a Java® capable Web browser from a standard desktop workstation. You can dynamically interact with any switch or hub in the SAN to monitor status and performance. Using the information provided, you can manage overall topology or make administrative changes to hubs, switches, or the network.

Overview of the StorWatch Specialist

The StorWatch Specialist provides the following capabilities:

- Central status monitoring

  From the Fabric view, you can display all switches and hubs in a fabric on a single screen (access detailed information) and administer any device in the SAN.

- Rapid access to any switch or hub

  From the Fabric view, you can click on a switch (hub) icon to access device status, port status, throughput, performance, and operating conditions such as temperature or fan and power supply status.

- Comprehensive asset management

  From the name server tables, you can get detailed information about all SAN devices in the fabric.

- Extensive administration and configuration capability

  You can configure and administer individual ports or devices using a wide range of functions encompassing device configuration, port management, and license key administration.

- Distributed zoning control

  You can apply zoning functions to appropriately configured hubs. Through the fabric operating system (OS), zoning configuration changes are automatically distributed to all switches in the fabric.

- Telnet interface for access to specialized functions

  Through the Telnet interface, perform functions available only through Telnet.

- Central maintenance functions

  You can add new firmware from your desktop.

Launching the StorWatch Specialist

Access to the StorWatch Specialist is provided through one of the following Java-enabled Web browsers.

For Windows 95, Windows 98, or Windows NT:

- Internet Explorer 4.0 or above
- Netscape 4.51 or above

For UNIX:

- Netscape 4.51 or above

In addition to the above, Java Plug-In 1.2.2 is also required.

Perform the following procedure to launch the StorWatch Specialist:

1. Start the Web browser, if it is not already active.
2. Type the hub name or IP address in the **Location/Address** field.
3. The Fabric View is displayed, showing all compatible switches and hubs in the fabric.

Note: The client system that you are using to connect to the 3534 Managed Hub must be able to resolve the switch name to the IP address, even if you are using the IP address in your Web browser. To set the 3534 Managed Hub name, see “Setting the 3534 Managed Hub name” on page 15.

StorWatch Specialist views

You access the StorWatch Specialist through a series of window views that display various aspects of your SAN, such as physical configuration, data throughput, statistics, and status, as well as windows that provide an administrative interface and a Telnet interface to your SAN. The StorWatch Specialist windows are organized as follows:

Fabric view
The Fabric view shows the number of switches and hubs in the fabric, with world-wide name (WWN), domain ID, device name, and network IP information. The Fabric view is the first view displayed and is the launch point for Switch view, Fabric Topology view, Name Server Table view, and the Zone Administration interface.

Fabric Topology view
The Fabric Topology view displays the physical configuration, including active domains, paths, and routing information.

Name Server Table view

The Name Server Table view displays the name server table for the fabric. Use this view to find information about the devices that are attached to the fabric.

Zone Administration interface

The Zone Administration interface provides an interface for configuring zoning: zone alias settings, zone settings, and zone configuration settings.

Switch view

The Switch view displays the switch and hub information. It provides a real-time view of overall status. The Switch view is the launch point for Port Statistics view, Performance view, Administrative interface, and Telnet interface.

Port Statistics view

The Port Statistics view displays statistics, general information, and status for a specific port.

Performance view

The Performance view graphically portrays real-time data throughput for each port and displays total bandwidth usage.

Administrative interface

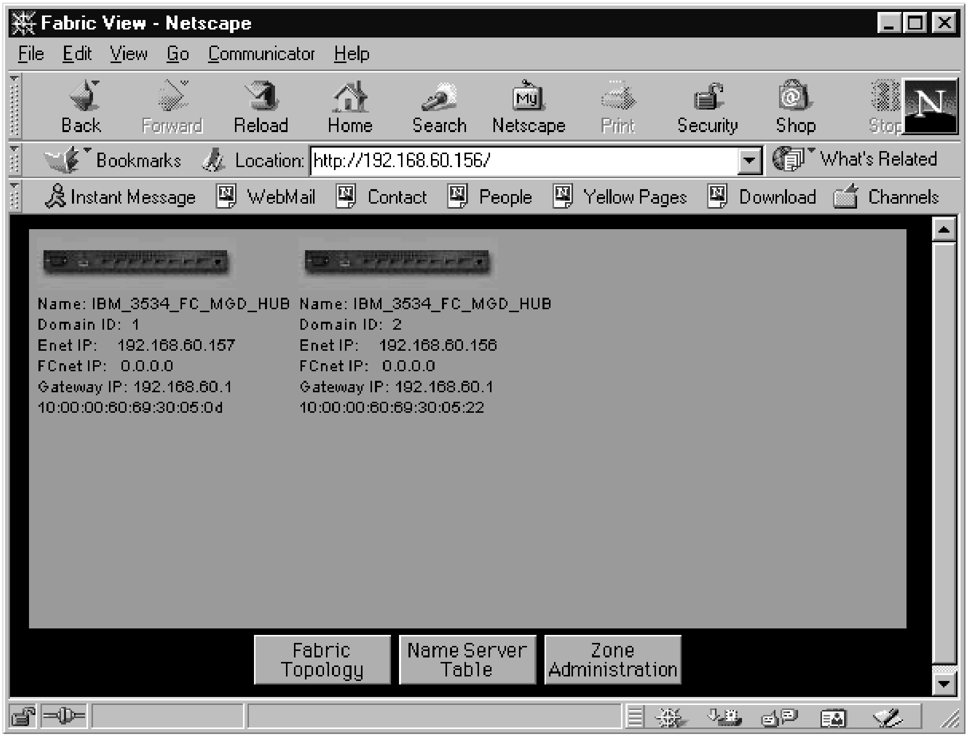
The Administrative interface provides an interface for performing functions such as upgrading firmware versions or reconfiguring a device.

Telnet interface

The Telnet interface provides an interface for using Telnet commands for device diagnostics, troubleshooting, and SAN management.

Fabric view

The Fabric view shows all the devices included in a fabric. It is the first Web page that is displayed after you connect to a device. From this view, you can display the Switch view for an individual device by clicking the switch icon, or you can access the Fabric Topology view, Name Server Table view, or Zone Administration interface by clicking the appropriate tab at the bottom of this view. See Figure 15 on page 30 for an example of the Fabric view.


Fabric View - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location:
What's Related
Instant Message WebMail Contact People Yellow Pages Download Channels
Fabric Topology
Name Server Table
Zone Administration

http://192.168.60.156/

Name: IBM_3534_FC_MGD_HUB
Domain ID: 1
Enet IP: 192.168.60.157
FCnet IP: 0.0.0.0
Gateway IP: 192.168.60.1
10:00:00:60:69:30:05:0d

Name: IBM_3534_FC_MGD_HUB
Domain ID: 2
Enet IP: 192.168.60.156
FCnet IP: 0.0.0.0
Gateway IP: 192.168.60.1
10:00:00:60:69:30:05:22

SL000122

Figure 15. Fabric view

The following is a description of the Fabric view fields:

Switch icon
The switch icon indicates the device type. Information about the device is shown following the icon.

Name The device name.

Domain ID
The number that uniquely identifies the device in a fabric.

Enet IP The Ethernet IP address.

FCnet IP The fibre-channel IP address.

Gateway IP
The gateway IP address.

WWN The unique numeric identifier (world-wide name) for each device; assigned by the manufacturer.

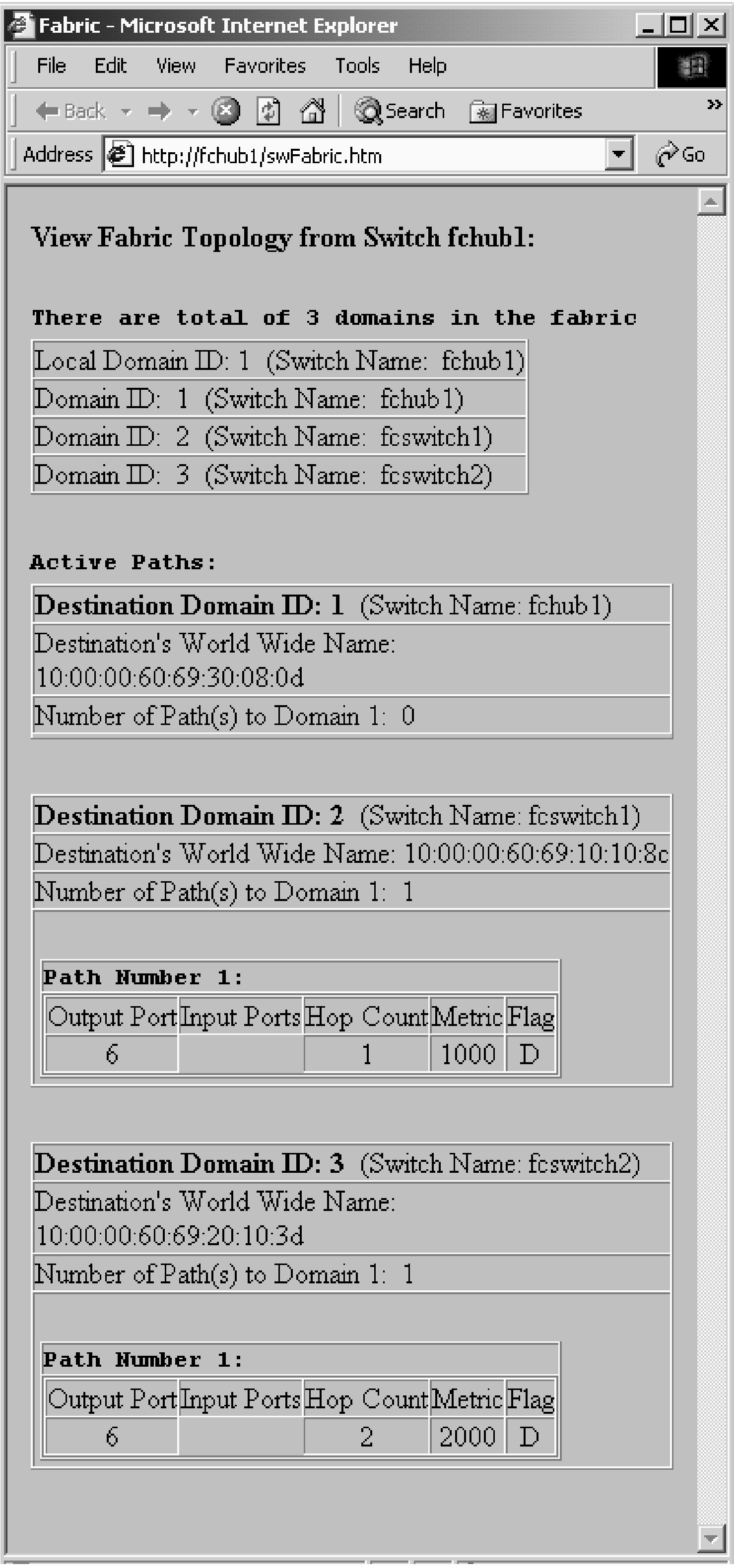
Fabric Topology
Click this tab to navigate to the Fabric Topology view.

Name Server Table
Click this tab to navigate to the Name Server Table view.

Zone Administration
Click this tab to navigate to the Zone Administration interface.

Fabric Topology view

The Fabric Topology view shows the physical configuration of the fabric, including active domains and paths. The topology is shown as viewed from the host domain (the device that was initially requested from the Web browser). Click the **Fabric Topology** tab on the Fabric View window to access the Fabric Topology view. See Figure 16 on page 32 for an example of this view.


Fabric - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://fchub1/swFabric.htm
Go

View Fabric Topology from Switch fchub1:

There are total of 3 domains in the fabric

Local Domain ID: 1 (Switch Name: fchub1)
Domain ID: 1 (Switch Name: fchub1)
Domain ID: 2 (Switch Name: fcswitch1)
Domain ID: 3 (Switch Name: fcswitch2)

Active Paths:

Destination Domain ID: 1 (Switch Name: fchub1)
Destination's World Wide Name: 10:00:00:60:69:30:08:0d
Number of Path(s) to Domain 1: 0

Destination Domain ID: 2 (Switch Name: fcswitch1)
Destination's World Wide Name: 10:00:00:60:69:10:10:8c
Number of Path(s) to Domain 1: 1

Path Number 1:

Output Port	Input Ports	Hop Count	Metric	Flag
6		1	1000	D

Destination Domain ID: 3 (Switch Name: fcswitch2)
Destination's World Wide Name: 10:00:00:60:69:20:10:3d
Number of Path(s) to Domain 1: 1

Path Number 1:

Output Port	Input Ports	Hop Count	Metric	Flag
6		2	2000	D

SL000123

Figure 16. Fabric Topology view

The following is a description of the Fabric Topology fields:

Destination Domain ID: (1, 2, or 3)

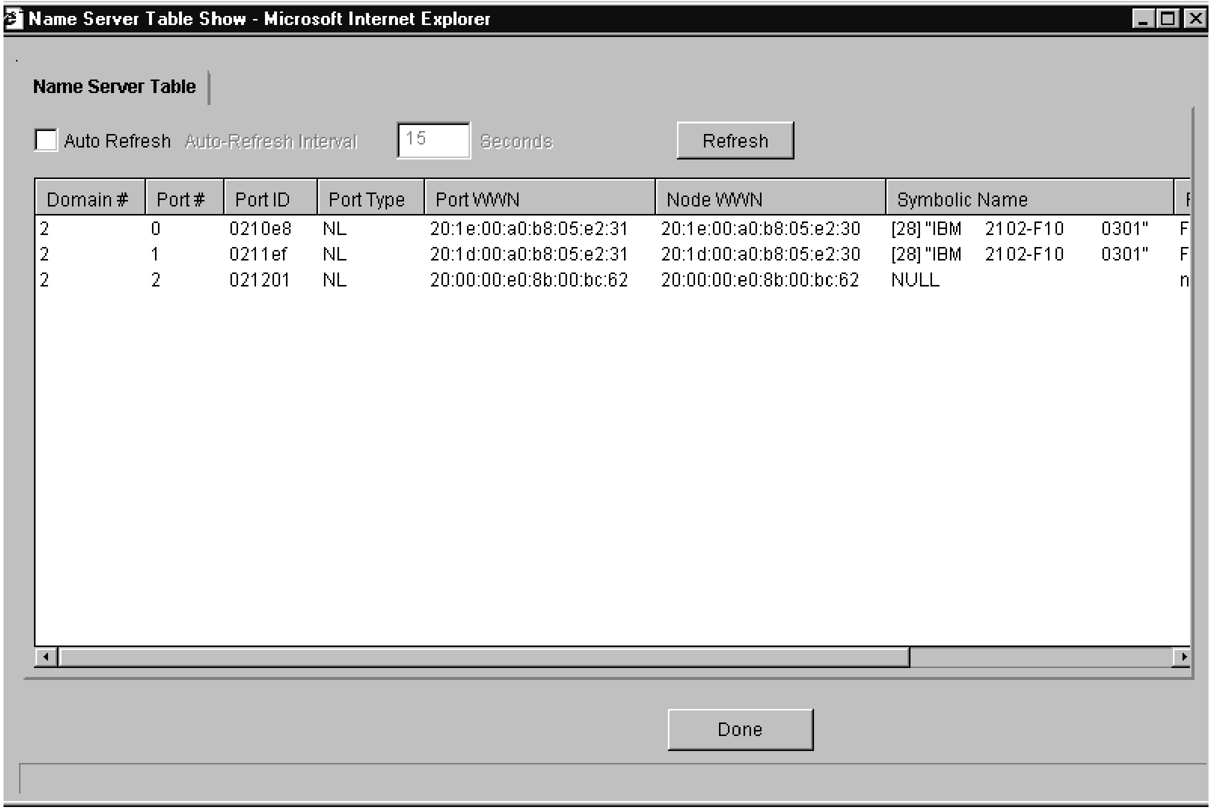
Displays a list of active domains in the fabric with switch name and switch domain ID.

Active Paths

Displays the active paths from the host domain to all remote domains within the fabric. Information is displayed by the domain ID associated with the switch name. It includes WWN and total number of paths by domain with output ports, input ports, hop count, metric, and flag for each path.

Name Server Table view

The Name Server Table view displays the name server table for the fabric. The name server table contains name server entries for the fabrics that are kept in the simple name server database. This includes all name server entries, not just those local to a single device. Click the **Name Server Table** tab at the bottom of the Fabric View window to access the Name Server Table view. See Figure 17 for an example of this view.



☐ Auto Refresh   Auto-Refresh Interval 15 Seconds

Domain #	Port #	Port ID	Port Type	Port WWN	Node WWN	Symbolic Name	F
2	0	0210e8	NL	20:1e:00:a0:b8:05:e2:31	20:1e:00:a0:b8:05:e2:30	[28] "IBM 2102-F10 0301"	F
2	1	0211ef	NL	20:1d:00:a0:b8:05:e2:31	20:1d:00:a0:b8:05:e2:30	[28] "IBM 2102-F10 0301"	F
2	2	021201	NL	20:00:00:e0:8b:00:bc:62	20:00:00:e0:8b:00:bc:62	NULL	n

SL000124

Figure 17. Name Server Table view

The following is a description of the Name Server Table fields:

Auto Refresh
Select **Auto Refresh** (check) to enable. Clear **Auto Refresh** again (uncheck) to disable.

Auto Refresh Interval
Displays the auto refresh interval in seconds.

Refresh Click **Refresh** to refresh data on demand.

Domain #
Displays the domain ID number of each switch.

Port # Displays the port number of the switch.

Port ID Displays the port ID of the switch (fibre-channel 24-bit ID in hexadecimal).

Port Type
Displays the port type of each attached device (`N` for fabric direct-attached port or `NL` for fabric direct-attached loop port).

Port WWN
Displays the WWN for the attached device port.

Node WWN
Displays the WWN for the attached device node.

Symbolic Name
Displays the symbolic name of the attached device assigned through the **SCSI INQUIRY** command.

FC4 Types
Displays the fibre-channel FC4 layer types supported by the device, such as IP, fibre-channel protocol (FCP), and so on.

COS Displays the fibre-channel classes of service supported by the device.

Member of Zones
Lists the member zones for this device.

Done Click **Done** to close the window.

Zone Administration interface

The Zone Administration interface consists of the following functions:

- Zone alias settings
- Zone settings
- Zone configuration settings

When administering zoning, do the following:

1. Define zone aliases to establish groupings (assigning aliases is optional). See “Zone Alias Settings” on page 35.
2. Create zone members. See “Zone Settings” on page 37.
3. Place zones into a zone configuration. See “Zone Configuration Settings” on page 39.
4. Enable the zone configuration.

For detailed information about zoning, see "Zoning concepts" on page 88.

Click the **Zone Administration** tab at the bottom of the Fabric View window (see Figure 15 on page 30) to access the Zone Administration window (see Figure 18).

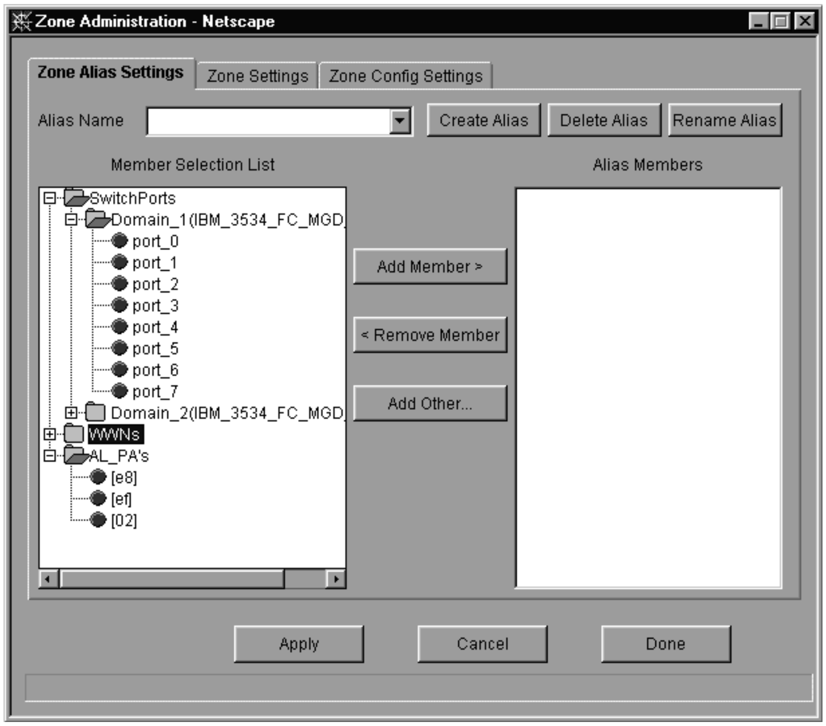
The first setting is displayed on the **Zone Alias Settings** tab. You can access the other zone administration settings by clicking the appropriate tab.

Note: If a device is added or removed from the network, you must save changes by clicking either **Apply** or **Done**, then relaunch zone administration to see the changes. You must have administrator privileges to access these functions.

Each setting is described as follows.

Zone Alias Settings

Use **Zone Alias Settings** (see Figure 18) to configure and manage alias membership. Zone aliases are optional.



SL000125

Figure 18. Zone Alias Settings view

The following is a description of the Zone Alias Settings fields:

Alias Name
Displays the alias that is currently selected.

Create Alias
Click for the dialog box to enter the name of the new alias; all names must be unique and should contain no spaces.

Delete Alias
Click for the dialog box to delete the alias that is displayed in the in **Alias Name** field.

Rename Alias
Click for the dialog box to enter the new name for the currently selected alias.

Member Selection List
Displays a list of available devices, ports, and WWNs.

Add Member
Select a member from **Member Selection List**, then click **Add Member** to add the alias to the list of members.

Remove Member
Select a member from the list of members for the currently selected alias, then click **Remove Member** to remove a member from the member list.

Add Other
Click for the dialog box to add a device domain, port, or WWN that is not in the **Member Selection List** menu.

Alias Members
Displays the members of the currently selected alias.

Apply Click to apply all changes made to the device during this session.

Note: Clicking **Apply** applies the changes that were made in all Zone Administration functions.

Cancel Click to cancel all changes and exit the Zone Administration window. Changes cannot be cancelled once they have been applied.

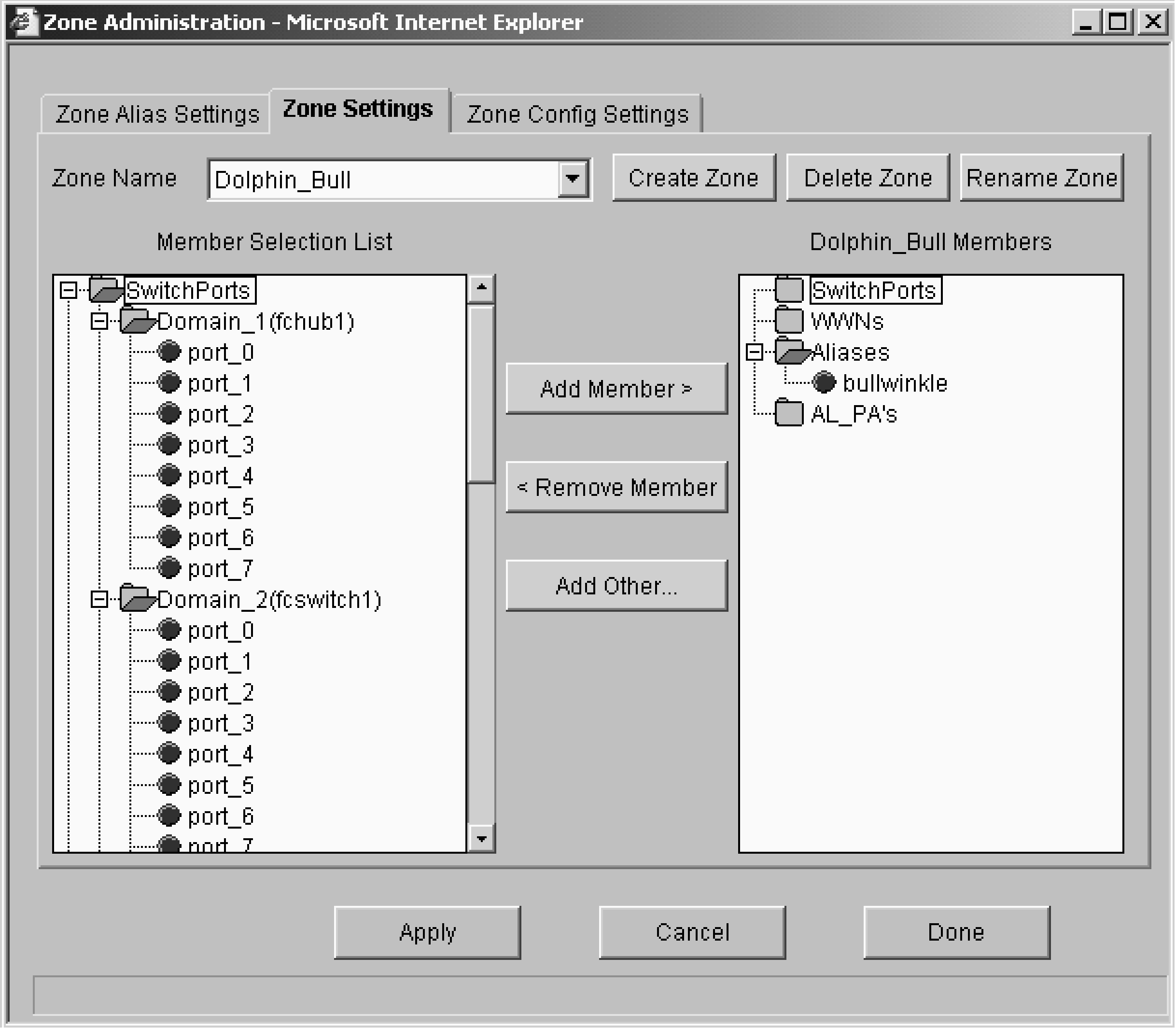
Done Click to apply all changes made to the device during this session and to close the window

Zone Settings

Use **Zone Settings** to create, delete, or rename zones, or to add or delete members from zones.

Also use **Zone Settings** to create a special broadcast zone. A broadcast zone is set up if the zone name *broadcast* is used. The broadcast zone name controls the delivery of broadcast packets in conjunction with IP-capable host bus adapters by restricting IP broadcast traffic to those elements (WWN or ports) included in that zone. Broadcast zones are independent of any other zones in force between the source and destination elements; for example, a broadcast is sent to all ports (WWN or domain, or port) that are defined in the broadcast zone even though a port is protected by a zone. Once created, enable the broadcast zone by placing the zone into a zone configuration, and then enable that zone configuration.

To access zone settings, click the **Zone Settings** tab, as shown in Figure 19, from any Zone Administration function.



Zone Name: Dolphin_Bull

SL000126

Figure 19. Zone Settings view

The following is a description of the Zone Settings fields:

Zone Name
Displays the currently selected zone.

Create Zone
Click for the dialog box to enter the name of the new zone; all names must be unique and should contain no spaces.

Delete Zone
Click for the dialog box to delete the currently selected zone.

Rename Zone
Click for the dialog box to enter a new name for the currently selected zone.

Member Selection List
Displays a list of available switches, ports, attached-device WWNs, and aliases.

Add Member
Select a member from the **Member Selection List** and click **Add Member** to add the zone to the list of members.

If a switch is selected, the switch and all ports are added to the zone. Individual ports are added by selecting a port from within a switch.

To add an attached-device WWN, select a node WWN (from the folder icon) or port WWN (from the blue circle icon) in the WWN sub-tree.

To add an alias, select it from the Aliases sub-tree; zone aliases must have been previously created.

Remove Member
Select a member from the Member Selection List for the currently selected zone and click **Remove Member** to remove a member from the member list.

Add Other
Click for a dialog box to add members that are not in the member selection list. The dialog box prompts for the WWN or the domain and port.

Zone Members
Displays the members of the currently selected zone.

Apply Click to apply all changes that were made to the device during this session.

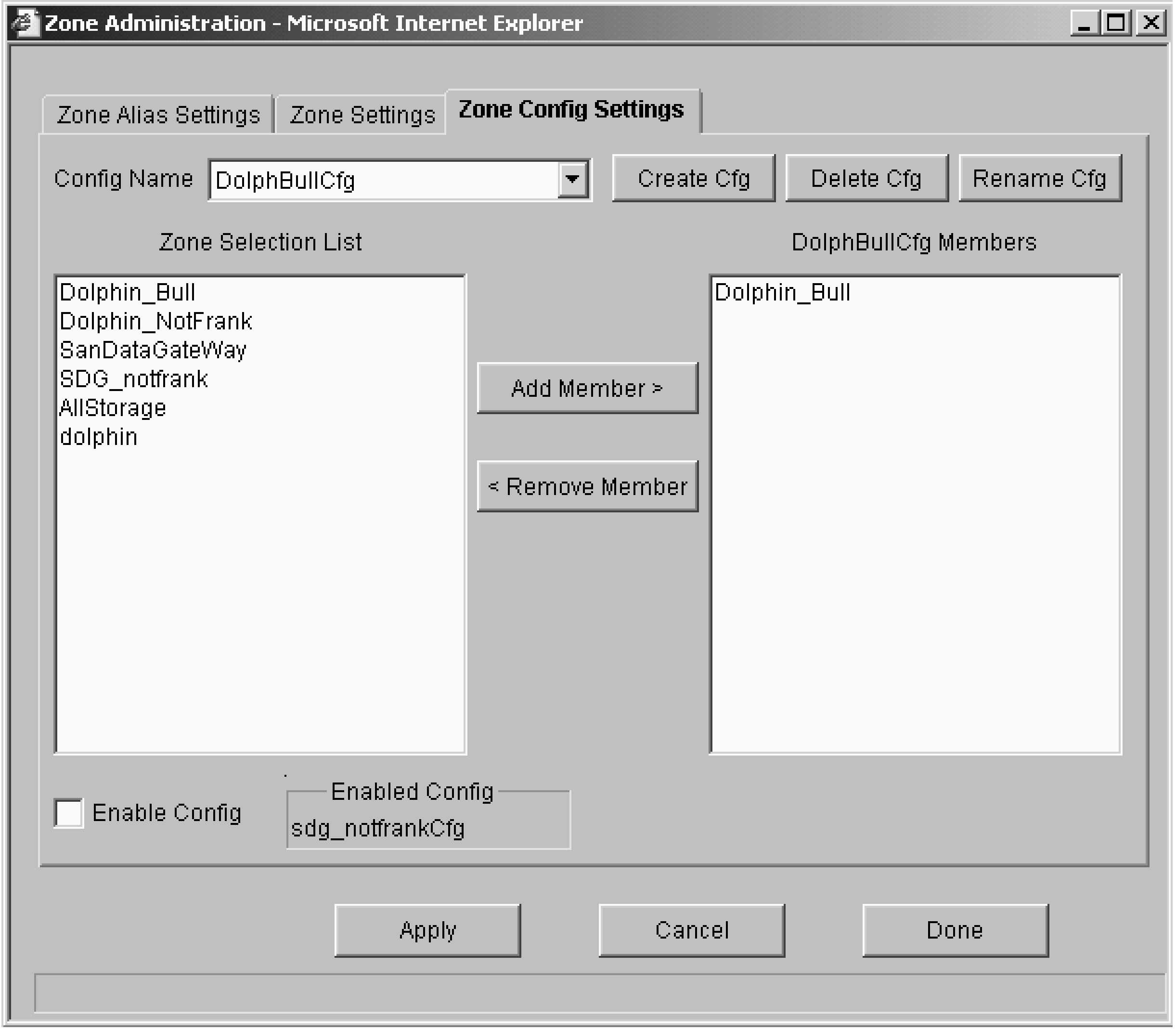
Note: Clicking **Apply** applies changes that were made in all Zone Administration functions.

Cancel Click to cancel all changes and exit Zone Administration. Changes cannot be cancelled once they have been applied.

Done Click to apply all changes made to the device during this session and to close the window.

Zone Configuration Settings

Use **Zone Configuration Settings**, as shown in Figure 20 on page 40, to create zone configurations, place zones into configurations, or to rename or delete zone configurations. Click the **Zone Config Settings** tab from any zone administration function to access the zone configuration settings.



Config Name: DolphBullCfg

Zone Selection List

Dolphin_Bull
Dolphin_NotFrank
SanDataGateWay
SDG_notfrank
AllStorage
dolphin

DolphBullCfg Members

Dolphin_Bull

□ Enable Config

Enabled Config: sdg_notfrankCfg

SL000127

Figure 20. Zone Config Settings view

The following is a description of the Zone Config Settings fields:

Config Name
Displays the currently selected configuration name.

Create Config
Click for a dialog box to enter the name of a new configuration; all names must be unique and contain no spaces.

Delete Config
Click for a dialog box to delete the currently selected configuration.

Rename Config
Click for a dialog box to enter a new name for the currently selected configuration.

Zone Selection List
This displays a list of available zones that can be added to the selected configuration.

Add Member
Click **Add Member** to add to the list of selected configuration members.

Remove Member
Select a member from the Zone Selection List, then click **Remove Member** to remove the member from the member list.

Config Members
Displays a list of all members for the currently selected zone configuration.

Enable Config
Select to enable the currently selected configuration; clear to disable.

Only one configuration can be enabled at a time; if no configurations are enabled, then zone configurations are not active in the fabric.

Apply Click to apply all changes that were made to the device during this session.

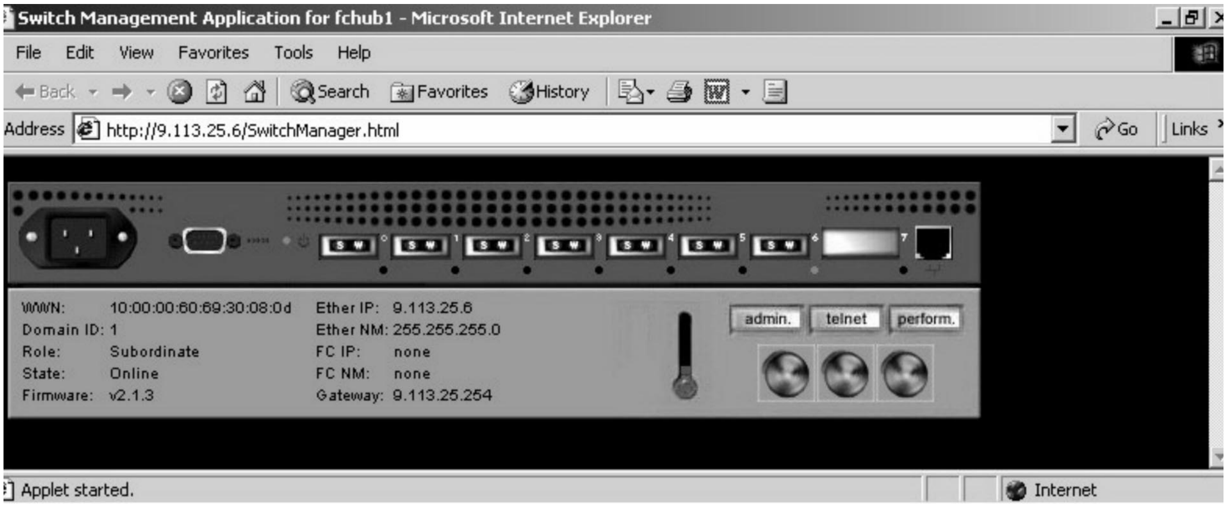
Note: Clicking **Apply** applies changes that were made in all Zone Administration functions.

Cancel Click to cancel all changes and exit Zone Administration. Changes cannot be cancelled after they have been applied.

Done Click to apply all changes that were made during this session and to close the window.

StorWatch Switch view

The Switch view shows the front panel of the 3534 Managed Hub and is displayed when you click on the 3534 Managed Hub from the Fabric view. The information that is displayed is very similar to a real time view of the 3534 Managed Hub status. See Figure 21 on page 42 for an example of the view.


Switch Management Application for fchub1 - Microsoft Internet Explorer

Address http://9.113.25.6/SwitchManager.html

WWN: 10:00:00:60:69:30:08:0d
Domain ID: 1
Role: Subordinate
State: Online
Firmware: v2.1.3

Ether IP: 9.113.25.6
Ether NM: 255.255.255.0
FC IP: none
FC NM: none
Gateway: 9.113.25.254

Applet started.

Figure 21. Switch view

The following is a description of the Switch view fields:

Port icon
The port icon indicates the GBIC type:

ID	Serial ID GBIC
CU	Copper
SW	Short wave
LW	Long wave
Blank	No GBIC present

A yellow outline around the port icon indicates a port failure.

For detailed port information, click the **port** icon for the Port Statistics view.

Number The number of the port.

LED status indicator

No light No device attached.

Steady yellow
Receiving light, but attached device is not online; check cable connections

Slow yellow
Disabled (diagnostics or **portDisable** command).

Fast yellow
Error, fault with port.

Steady green
Online (connected with device by cable).

Slow green
Online, but segmented (loopback cable or incompatible device).

Fast green
Internal loopback (diagnostic).

Flickering green
Online and transmitting or receiving frames.

Yellow and green
Port is bypassed.

WWN A unique numeric identifier for each switch; assigned by the manufacturer.

Domain ID
A number that uniquely identifies the switch in a fabric.

Role Principal device as defined in FC_SW protocol.

Subordinate
Device enabled, not principal device.

Disabled
Device disabled.

State The device states are:

Online

Offline

Testing

Faulty

Firmware
The fabric OS version.

Ether IP The Ethernet IP address.

Ether NM
The Ethernet netmask value.

FC IP The fibre-channel IP address.

FC NM The fibre-channel netmask value.

Gateway The IP address of the default gateway. The IP address must be properly set to access a switch from other networks.

Thermometer
The thermometer indicates the highest temperature from the last data sample. Click the thermometer to display the temperature readings from all switch thermo-sensors.

admin Click **admin** to link to the Administrative Interface, where you can perform switch management functions.

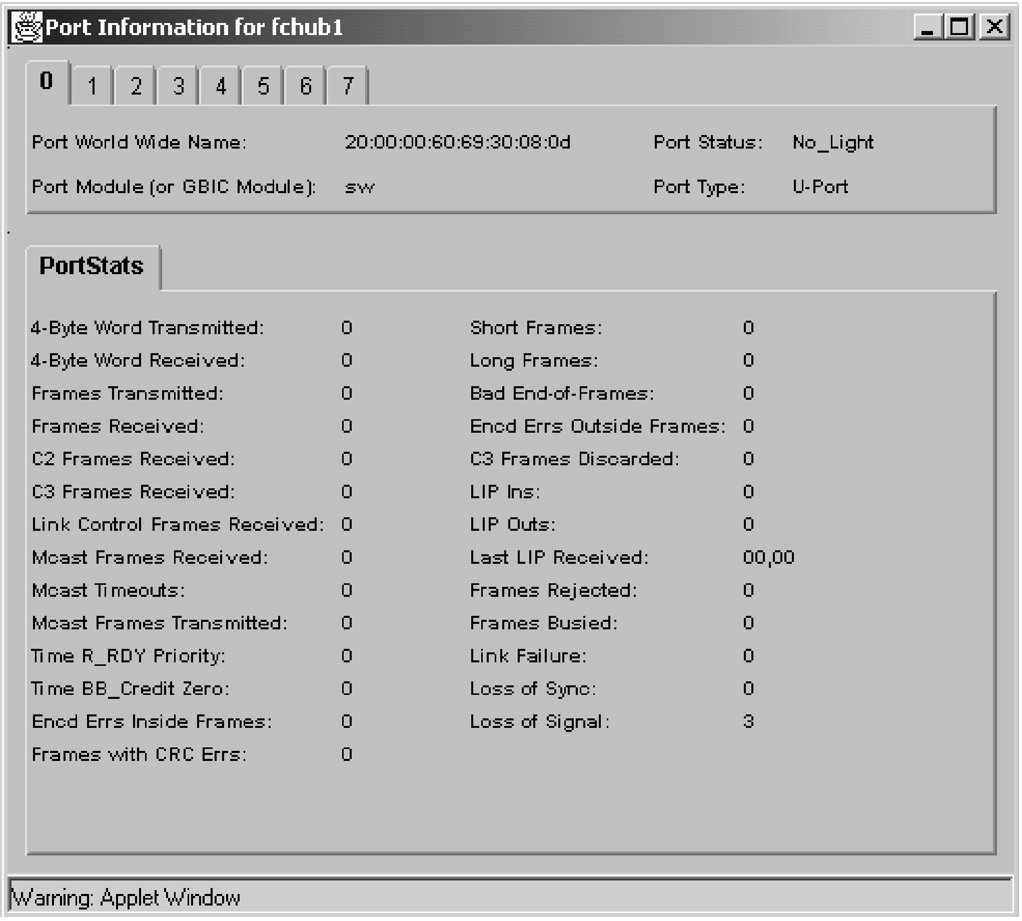
Telnet Click **Telnet** to launch a Telnet session.

Perform Click **perform** to link to the Performance view, where you can monitor switch performance.

Fans Spinning disks indicate that the fans are operating; if a disk stops spinning and turns yellow, the fan is experiencing a problem.

Port Statistics view

To access the Port Statistics view, click on any port in the Switch view. The Port Statistics view, as shown in Figure 22, provides statistics by port. To display statistics for a particular port, click on the appropriate tab at the top of the window. Port information is automatically updated whenever a port is selected. This information is also refreshed periodically while the port is selected.



Port World Wide Name:	20:00:00:60:69:30:08:0d	Port Status:	No_Light
Port Module (or GBIC Module):	sw	Port Type:	U-Port

4-Byte Word Transmitted:	0	Short Frames:	0
4-Byte Word Received:	0	Long Frames:	0
Frames Transmitted:	0	Bad End-of-Frames:	0
Frames Received:	0	Encd Errs Outside Frames:	0
C2 Frames Received:	0	C3 Frames Discarded:	0
C3 Frames Received:	0	LIP Ins:	0
Link Control Frames Received:	0	LIP Outs:	0
Mcast Frames Received:	0	Last LIP Received:	00,00
Mcast Timeouts:	0	Frames Rejected:	0
Mcast Frames Transmitted:	0	Frames Busied:	0
Time R_RDY Priority:	0	Link Failure:	0
Time BB_Credit Zero:	0	Loss of Sync:	0
Encd Errs Inside Frames:	0	Loss of Signal:	3
Frames with CRC Errs:	0		

Warning: Applet Window

SL000129

Figure 22. Port Statistics view

The following is a description of the Port Statistics fields:

Port World-Wide Name
The world-wide name (WWN) for this port.

Port Module (or GBIC Module)

GBIC or fixed port type:

--	No GBIC present.
sw	Short wave GBIC or fixed port.
lw	Long wave GBIC.
id	Could include any of the above.

Port Status

No_Module
No GBIC module in this port.

No_Light
Port is not receiving light.

No_Sync
Port is receiving light but is out of sync.

In_Sync Port is receiving light and is in sync.

Laser_Flt
Port is signaling a laser fault (defective GBIC or imbedded optical).

Port_Flt Port is marked faulty (defective). GBIC or imbedded optical cable or device.

Diag_Flt Port failed diagnostics.

Online Port is up and running.

Lock_Ref
Port is locking to reference signal.

Port Type

E_Port	Switch link port
G_Port	Generic port
U_Port	Universal port
L_Port	Loop port

Note: U_port is when the link is not initialized.
G_port is an intermediate state before.
E_port (during link initialization).
G_port displays briefly in Web Tools before an E_port is established.

Port Stats

4-Byte Word Transmitted
The number of 4-byte words transmitted.

4-Byte Word Received
The number of 4-byte words received.

Frames Transmitted
The number of frames transmitted.

Frames Received
The number of frames received.

C2 Frames Received
The number of class 2 frames received.

C3 Frames Received
The number of class 3 frames received.

Link Control Frames Received
The number of link control frames received.

Mcast Frames Received
The number of multicast frames received.

Mcast Timeouts
The number of multicast timeouts.

Mcast Frames Transmitted
The number of multicast frames transmitted.

Time R_RDY Priority
The number of times R_RDY has priority over frames to be sent.

Time BB_Credit Zero
The number of times BB_Credit went to zero.

Encd Errs Inside Frames
The number of encoding errors inside frames.

Frames with CRC Errs
The number of frames with CRC errors.

Short Frames
The number of frames shorter than the minimum.

Long Frames
The number of frames longer than the maximum.

Bad End-of-Frames
The number of frames with bad end-of-frames.

Encd Errs Outside Frames
The number of frames with encoding errors outside frames.

C3 Frames Discarded
The number of class 3 frames discarded.

LIP Ins The number of loop initialization procedures (LIPs) received.

LIP Outs The number of times loop initialized by FL_port.

Last LIP Received
The last LIP received: AL_PD, AL_PS.

Frames Rejected
The number of F_RJTs sent.

Frames Busied
The number of F_BSYs sent.

Link Failure
The number of times NOS received or sent.

Loss of Sync
The number of times loss of sync occurred.

Loss of Signal
The number of times loss of signal occurred.

Performance view

The Performance view, as shown in Figure 23, displays throughput for each port and for the entire hub. Throughput is shown in megabytes per second. The hub throughput is the sum of throughput for all ports. Port throughput represents the number of bytes that are received plus the number of bytes that are transmitted.

In the Performance view, the horizontal axis represents elapsed time, and the vertical axis represents throughput. Each port graph contains up to 60 seconds of performance data. The switch graph at the bottom contains up to 4 minutes of data.

To access this view, click **perform** from the Switch view.

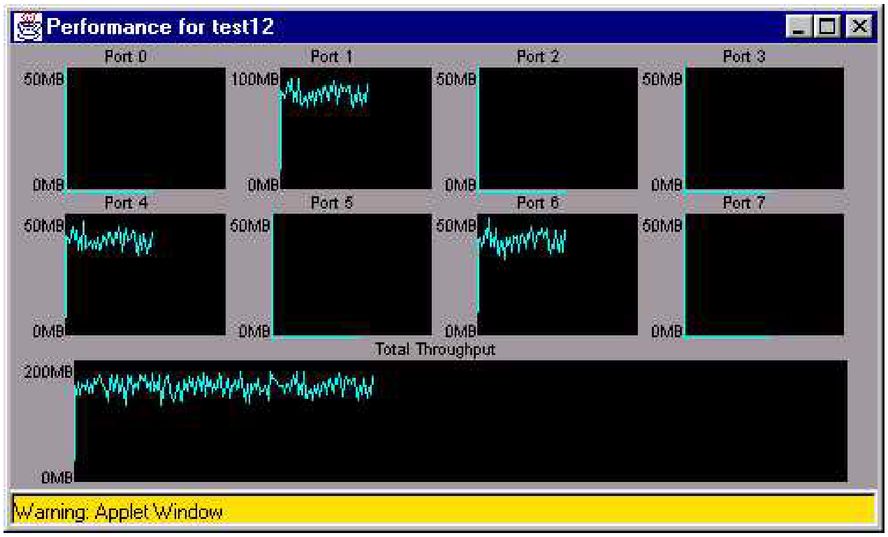


Figure 23. Performance view

Administrative interface

The Administrative interface consists of the following functions. To access these functions, click **admin** from the Switch view. The first function that is displayed is Switch Administration. You can access all other administrative interface functions by clicking the appropriate tab from any function.

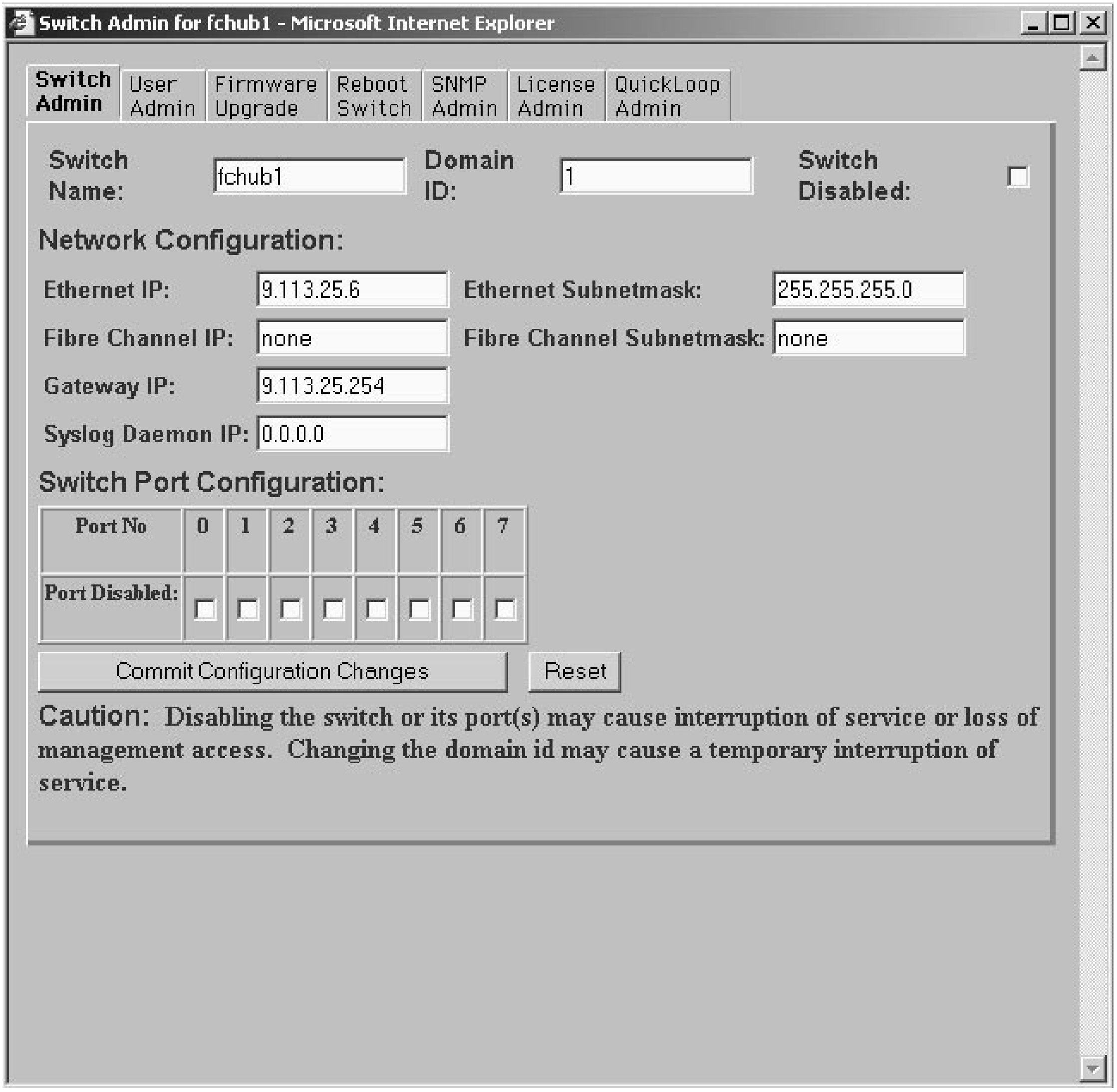
Important: You must have administrator authority to access these functions.

- Switch Administration
- User Administration
- Firmware Upgrade
- Reboot Switch
- SNMP Administration
- License Administration
- QuickLoop Administration

Switch Administration

Use the Switch Administration function to change IP information, disable a switch or hub, change the domain, change the switch name, or to see which ports are disabled.

To access Switch Administration, click **admin** from the Switch view or click the **Switch Admin** tab, as shown in Figure 24 on page 49, from any Administration function.



Switch Name: fchub1

Domain ID: 1

Switch Disabled: □

Network Configuration:

Ethernet IP: 9.113.25.6

Ethernet Subnetmask: 255.255.255.0

Fibre Channel IP: none

Fibre Channel Subnetmask: none

Gateway IP: 9.113.25.254

Syslog Daemon IP: 0.0.0.0

Switch Port Configuration:

Port No	0	1	2	3	4	5	6	7
Port Disabled:	□	□	□	□	□	□	□	□

Caution: Disabling the switch or its port(s) may cause interruption of service or loss of management access. Changing the domain id may cause a temporary interruption of service.

SL000130

Figure 24. Switch Admin view

The following is a description of the Switch Administration fields:

Switch Name

Displays or sets the switch (hub) name. To change the name, type the new name in this field.

Domain ID

Displays or sets the switch domain ID. Domain IDs must be unique within a fabric.

To change the domain ID, type the new domain ID in this field. Use a number from 1 - 239 for normal operating mode (FCSW compatible) and a number from 0 - 31 for VC encoded address format mode.

Switch Disabled
Select to disable; clear to enable.

Ethernet IP
Displays or sets the IP address for Ethernet connection to the switch. To change the address, type the new address in this field.

Ethernet Subnetmask
Displays or sets the Ethernet subnetmask. The default value is none. Contact your network administrator for the value to enter. If the subnetmask is changed, restart the Web browser.

Fibre channel IP
Displays or sets the fibre-channel IP address. To change the address, type the new address in this field.

Fibre channel Subnetmask
Displays or sets the fibre-channel subnetmask. If the subnetmask value is changed, restart the Web browser.

Gateway IP
Displays or sets the gateway IP address. Contact your network administrator for the IP address. If the address is changed, restart the Web browser.

Syslog Daemon IP
Displays or sets the destination station IP address that is used for sending events using syslog protocol to the host. Contact your network administrator for the IP address.

Port Disabled
If the box is checked, the port is disabled. To enable the port, clear the check box.

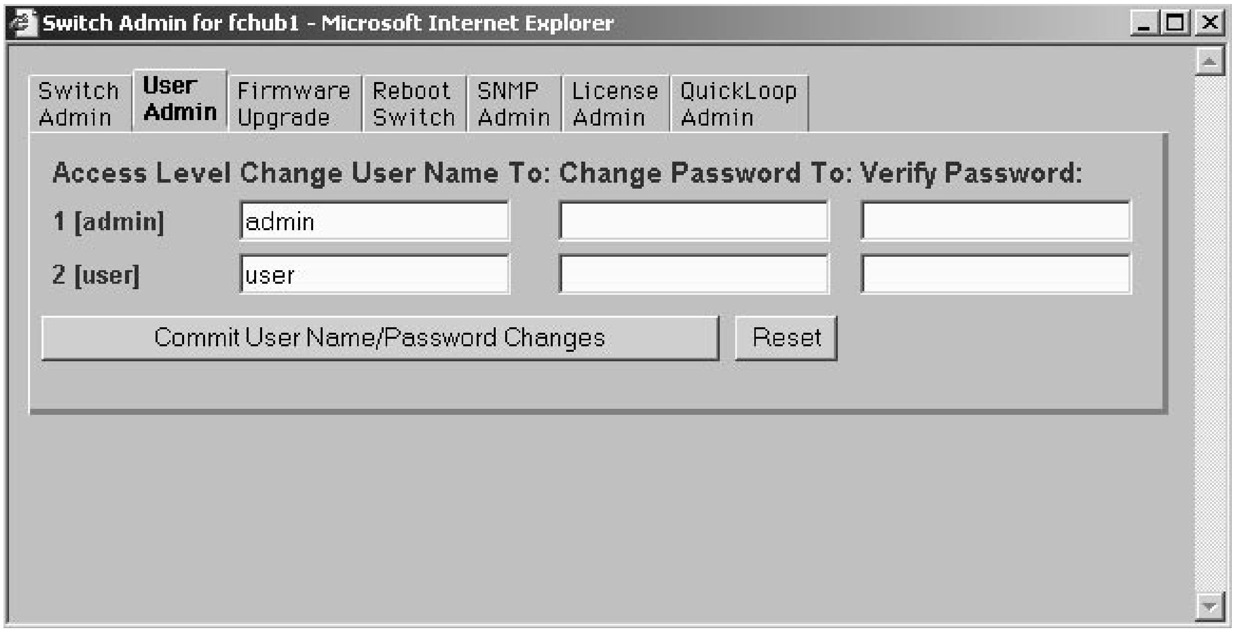
Commit Configuration Changes
Click to apply any changes made.

Reset Click to reset all fields to the values that were set when Switch Administration was launched.

User Administration

Use the User Administration function to rename accounts or to change passwords.

To access User Administration, click the **User Admin** tab, as shown in Figure 25, from any Administration function.



Access Level	Change User Name To:	Change Password To:	Verify Password:
1 [admin]	admin		
2 [user]	user		

Figure 25. User Admin view

The following is a description of the User Administration view fields:

Change User Name To
Type the new user name.

Change Password To
Type the new password.

Verify Password
Type the password again to verify.

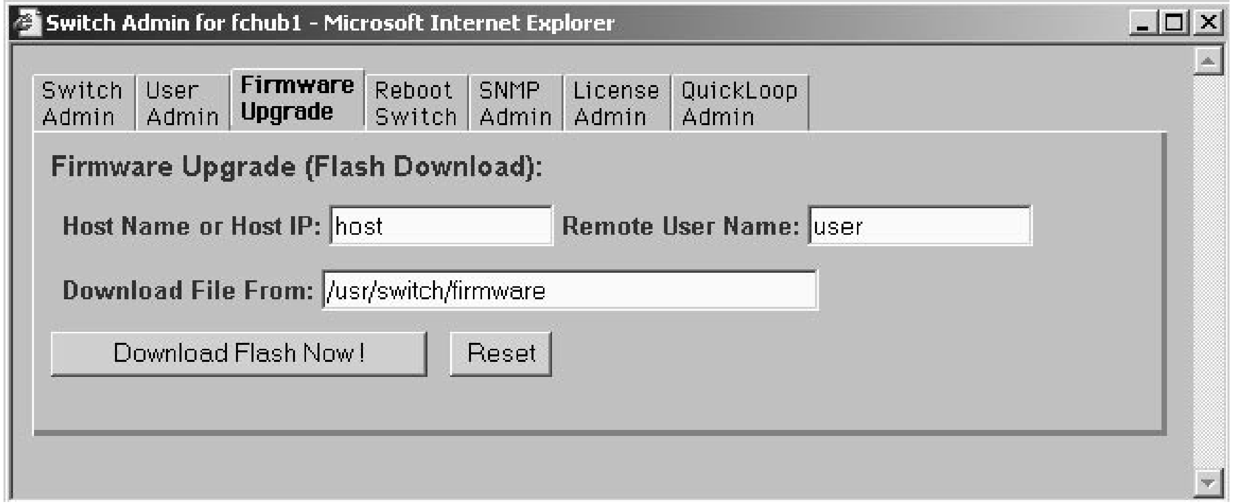
Commit User Name/Password Changes
Click to apply any changes made.

Reset Click to reset all fields to the values that were set when User Administration was launched.

Firmware Upgrade

Use the Firmware Upgrade function to download firmware upgrades.

To access Firmware Upgrade, click the **Firmware Upgrade** tab, as shown in Figure 26, from any Administration function.



Firmware Upgrade (Flash Download):

Host Name or Host IP: host   Remote User Name: user

Download File From: /usr/switch/firmware

SL000132

Figure 26. Firmware Upgrade view

The following is a description of the Firmware Upgrade fields:

Host Name or Host IP
Displays or sets the host name or the host IP address. To change the name or address, type the new value in this field.

Remote User Name
Displays or sets the remote user name. To change the name, type the new name in this field.

Download File From
Displays or sets the absolute directory path from the source host where the binary fabric OS resides. To change the path, type the new path in this field. (You must use forward slashes (/) when downloading fabric OS from a Windows system.)

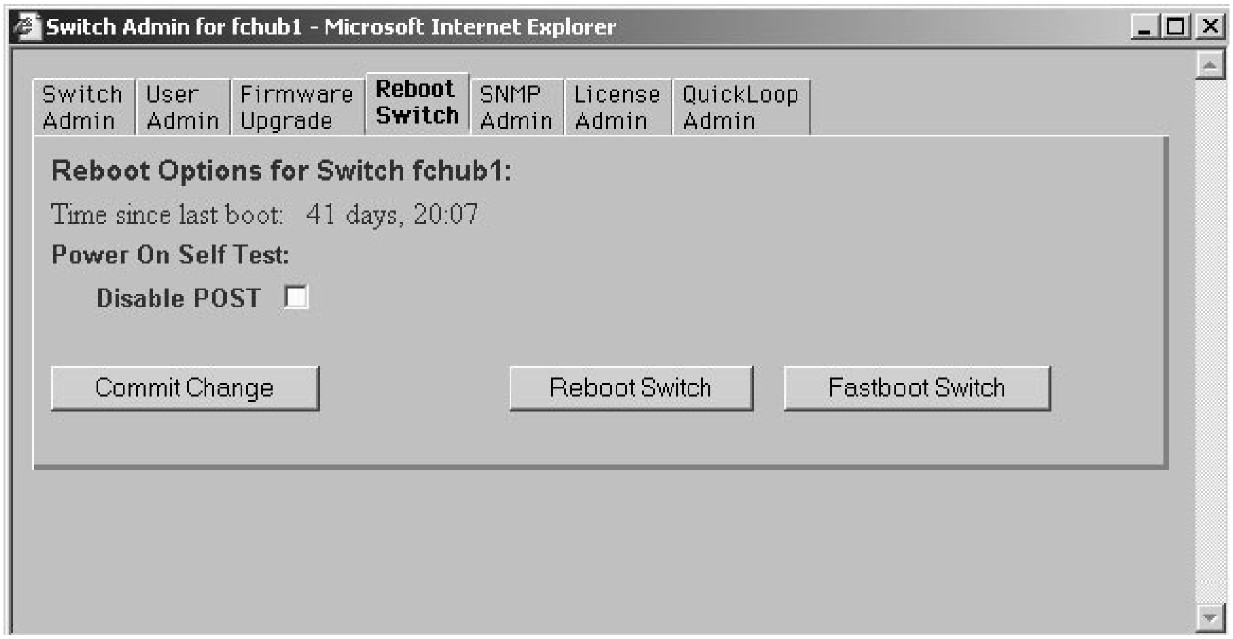
Download Flash Now
Click to download the firmware.

Reset Click to reset all fields to the values that were set when Firmware Upgrade was launched.

Reboot Switch

Use the Reboot Switch function to restart the switch. POST can also be disabled for future restarts.

To access Reboot Switch, click the **Reboot Switch** tab, as shown in Figure 27, from any Administration function.



Reboot Options for Switch fchub1:

Time since last boot: 41 days, 20:07

Power On Self Test:

Disable POST □

Figure 27. Reboot Switch view

The following is a description of the Reboot Switch fields:

Disable POST
Select this check box to disable POST for future restarts; clear the check box to enable POST.

Commit Change
Click to save settings.

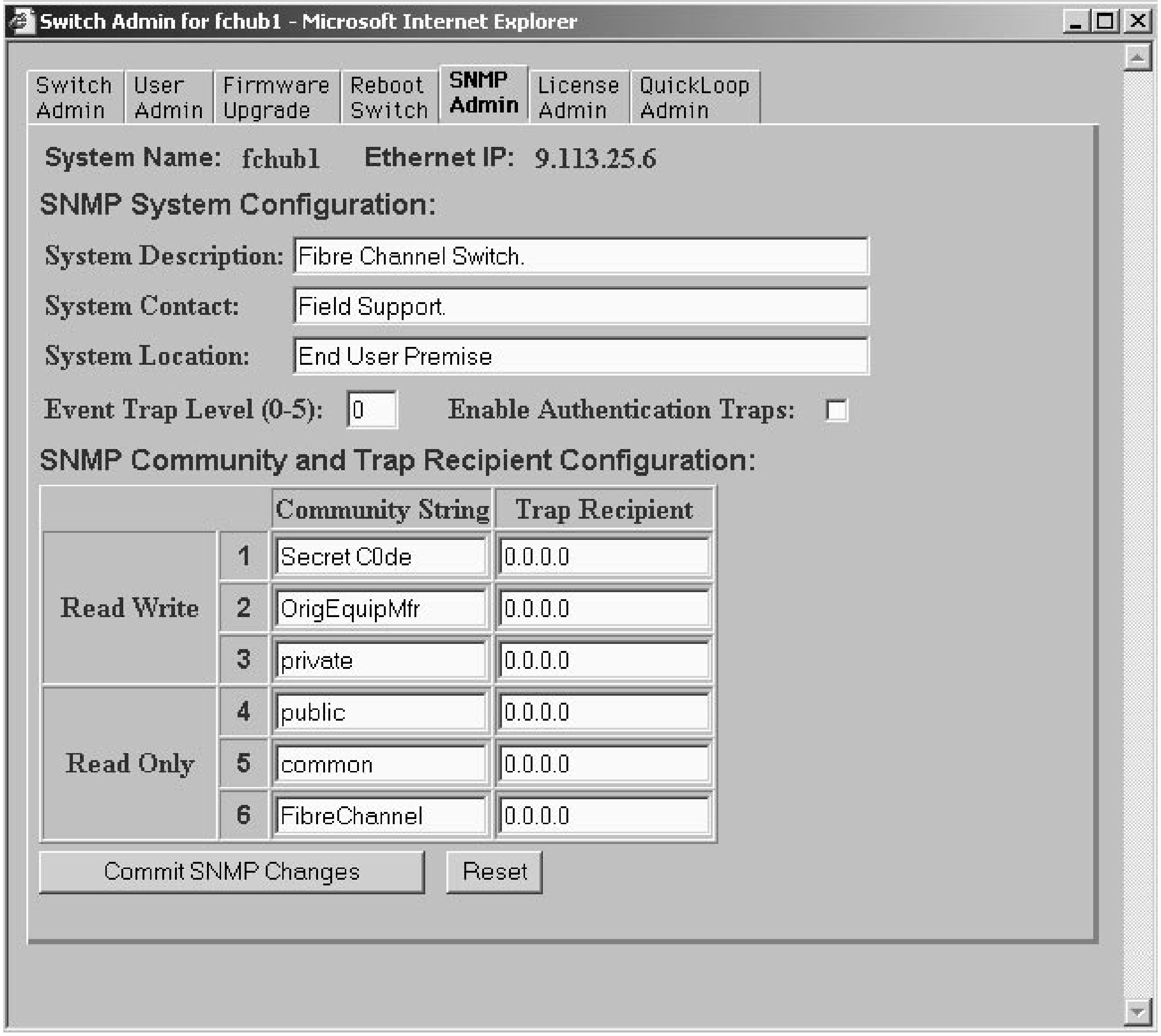
Reboot Switch
Click to restart the switch.

Fastboot Switch
Click to perform a fast restart. A fast restart bypasses POST. (It is the same as a restart with POST disabled.)

SNMP Administration

Use the SNMP Administration function to set the SNMP options.

To access SNMP Administration, click the **SNMP Admin** tab, as shown in Figure 28, from any Administration function.



System Name: fchub1 Ethernet IP: 9.113.25.6

SNMP System Configuration:

System Description: Fibre Channel Switch.

System Contact: Field Support.

System Location: End User Premise

Event Trap Level (0-5): 0 Enable Authentication Traps: □

SNMP Community and Trap Recipient Configuration:

		Community String	Trap Recipient
Read Write	1	Secret C0de	0.0.0.0
	2	OrigEquipMfr	0.0.0.0
	3	private	0.0.0.0
Read Only	4	public	0.0.0.0
	5	common	0.0.0.0
	6	FibreChannel	0.0.0.0

SL000134

Figure 28. SNMP Admin view

The following is a description of the SNMP Administration fields

System Description
Displays or sets the system description. The default is Fibre Channel Switch.

System Contact
Displays or sets the contact information for switch. The default is Field Support.

System Location
Displays or sets the location of the switch. The default is End User Premise.

Event Trap Level
Sets the severity level of switch events that prompt SNMP traps. The default is 0.

Enable Authentication Traps
Select to enable authentication traps; clear to disable (recommended).

Read Write Community String
Displays or sets up to three strings that work with the SNMP **set** command.

Read Only Community String
Displays or sets up to three strings that work with the SNMP **get** or **get-next** command.

Trap Recipient
Displays or sets the recipients for the traps (usually the IP address of the SNMP management station).

Commit SNMP Changes
Click to apply any changes made.

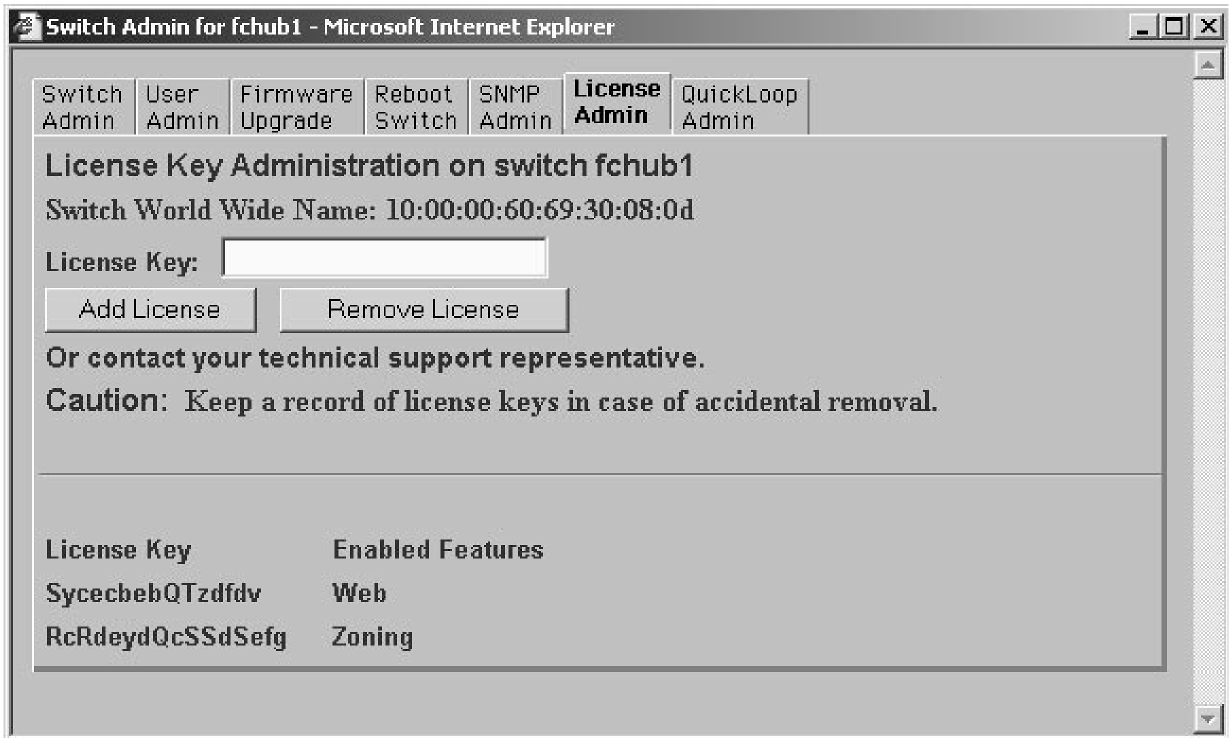
Reset Click to reset all fields to the values that were set when SNMP Administration was launched.

Note: To disable the community string or trap recipient fields, leave the fields empty.

License Administration

Use the License Administration function to add or remove licenses. This function also displays a list of installed license keys and features.

To access License Administration, click the **License Admin** tab, as shown in Figure 29, from any Administration function.



License Key Administration on switch fchub1

Switch World Wide Name: 10:00:00:60:69:30:08:0d

Or contact your technical support representative.

Caution: Keep a record of license keys in case of accidental removal.

License Key	Enabled Features
SycecbebQTzdfdv	Web
RcRdeydQcSSdSefg	Zoning

SL000135

Figure 29. License Admin view

The following is a description of the License Administration fields:

License Key
Type the license key to be added or removed.

Add License
Click to add the specified license.

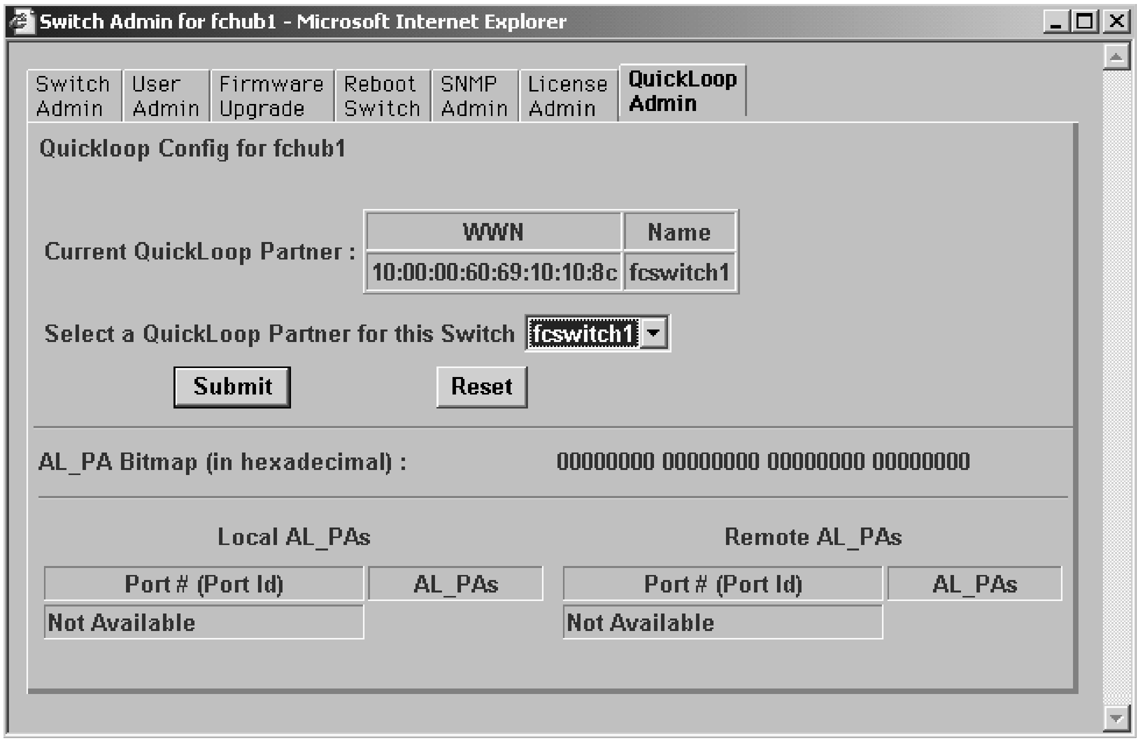
Remove License
Click to remove the specified license.

Keys and Enabled Features
Displays the license keys and features that are enabled on the switch.

Note: The 3534 Managed Hub comes standard with zoning and the IBM StorWatch Managed Hub Specialist functions enabled. The License Administration function is used for optional functions.

QuickLoop Administration

The StorWatch Specialist is used to view Quickloop configuration information and to set the QuickLoop partner hub or switch. To access QuickLoop Administration, click the **QuickLoop Admin** tab, as shown in Figure 30, from any Administrative function.



Quickloop Config for fchub1

Current QuickLoop Partner :

WWN	Name
10:00:00:60:69:10:10:8c	fcswitch1

Select a QuickLoop Partner for this Switch fcswitch1

AL_PA Bitmap (in hexadecimal) : 00000000 00000000 00000000 00000000

Local AL_PAs

Port # (Port Id)	AL_PAs
Not Available	

Remote AL_PAs

Port # (Port Id)	AL_PAs
Not Available	

SL000136

Figure 30. QuickLoop Admin view

The following is a description of the quickloop Administration fields:

Current QuickLoop Partner
Displays the WWN address and name of the current partner.

Select a QuickLoop Partner for this Switch
Provides a drop-down list of QuickLoop partners that you can select.

Submit Click to add the selected QuickLoop partner to the members list.

Reset Click to remove a selected QuickLoop partner from the members list.

Al_PA Bitmap (in hexadecimal)
Displays the AL_PA address of the bitmap in hexadecimal.

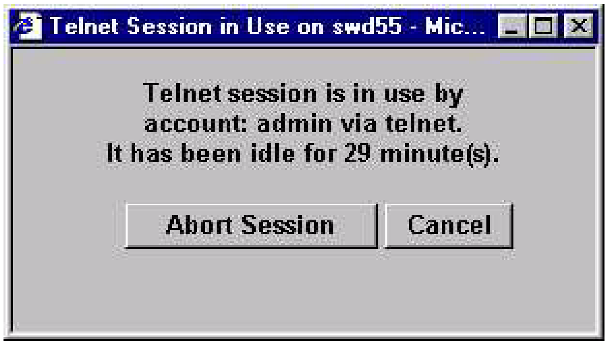
Local AL_PAs
Lists the available local AL_PA ports and their addresses.

Remote AL_PAs
Lists the available remote AL_PA ports and their addresses.

Telnet interface

To access the Telnet interface, click **Telnet** from the Switch view. This displays a Telnet session directly from your Web browser. Only one Telnet session can be active at a time. If a session is already active, a dialog box is displayed (see Figure 31). Click **Abort Session** to end the existing Telnet session, or click **Cancel** to cancel the transaction.

Note: You must have administrator authority to end a Telnet session.


Telnet Session in Use on swd55 - Mic...

Telnet session is in use by
account: admin via telnet.
It has been idle for 29 minute(s).

Figure 31. Telnet Session in Use dialog box

Chapter 4. Feature code upgrades

This chapter describes the following optional features:

- Entry Fabric Switch upgrade
- Fabric Watch upgrade

IBM 3534 Entry Fabric Switch feature code upgrade

The IBM 3534 Entry Fabric Switch feature is configured as a high-speed interconnect for fibre-channel arbitrated loop (FC_AL) environments. As an alternative to hub-based solutions, the Entry Fabric Switch feature provides a true switching environment that provides enhanced performance, increased availability through better fault isolation, and investment protection through migration to full fabric topologies. The Entry Fabric Switch feature is ideally suited for low-end SAN environments with hosts and devices that support FC_AL. The Entry Fabric Switch feature supports the use of FL_ports only.

The Entry Fabric Switch feature supports all of the functionality of the 3534 Managed Hub and provides a low-cost fabric capability. The 3534 Managed Hub delivers true SAN fabric performance in a single switch topology. It provides a set of features that are superior to those of other switches with the ability to upgrade to full fabric functionality. The Entry Fabric Switch feature supports F and FL ports and the name server (1E_port).

See the *IBM SAN Fibre Channel Switch 2109 Model S08 User's Guide* for information about switch usability. This book introduces the IBM 2109 Model S08 switch and its features. It also provides information about using the IBM StorWatch SAN Fibre Channel Switch Specialist, setting up zoning, and methods for managing the IBM 2109 S08 Switch remotely.

The *IBM SAN Fibre Channel Switch 2109 Model S08 User's Guide* can be viewed at the following Web site:

www.ibm.com/storage/fcswitch/

With this upgrade applied, the 3534 Managed Hub performs as an 8-port switch with a single E_port.

Fabric Watch feature code upgrade

Fabric Watch is an optionally licensed product and requires a valid license key to function.

Note: To verify whether the Fabric Watch license is already installed on the hub, type `licenseShow` on the Telnet command line. For additional information, see "Installing Fabric Watch through Telnet" on page 63.

This section describes the Fabric Watch software and how to install it, plus detailed information for using thresholds to manage hub functions.

Fabric Watch allows the SAN manager to monitor key fabric and hub elements, making it easy to quickly identify and escalate potential problems. It monitors each element for out-of-boundary values or counters and provides notification when any elements exceed the defined boundaries. The SAN manager can configure which elements, such as error, status, and performance counters within a 3534 Managed Hub, are monitored.

Fabric Watch runs on 3534 mANAGED Hubs with Fabric OS, version 2.2 or later, and can be accessed through the IBM StorWatch Specialist, a Telnet interface, a Simple Management Network Protocol (SNMP)-based enterprise manager, or by modifying and uploading the Fabric Watch configuration file to the hub.

Fabric Watch monitors the following elements:

- Fabric events (such as topology reconfigurations and zone changes)
- Hub environment (fans, power supplies, and temperature)
- Ports (state changes, errors, and performance)
- GBICs (for hubs equipped with smart GBICs)

With Fabric Watch, each hub continuously monitors error and performance counters against a set of defined ranges. This and other information specific to each monitored element is made available by Fabric Watch for viewing and, in some cases, modification. This set of information about each element is called a *threshold*, and the upper and lower limits of the defined ranges are called *boundaries*.

If conditions exceed the acceptable ranges, an event is considered to have occurred. One or more alarms (reporting mechanisms) are generated if configured for the relevant threshold. There are three types of alarms:

- SNMP trap
- Entry in the hub event log
- Locking of the port log to preserve the relevant information

The service representative can deploy Fabric Watch as shipped, or you can customize your configuration profile using the **fwConfigure** commands. See "fwConfigure" on page 74.

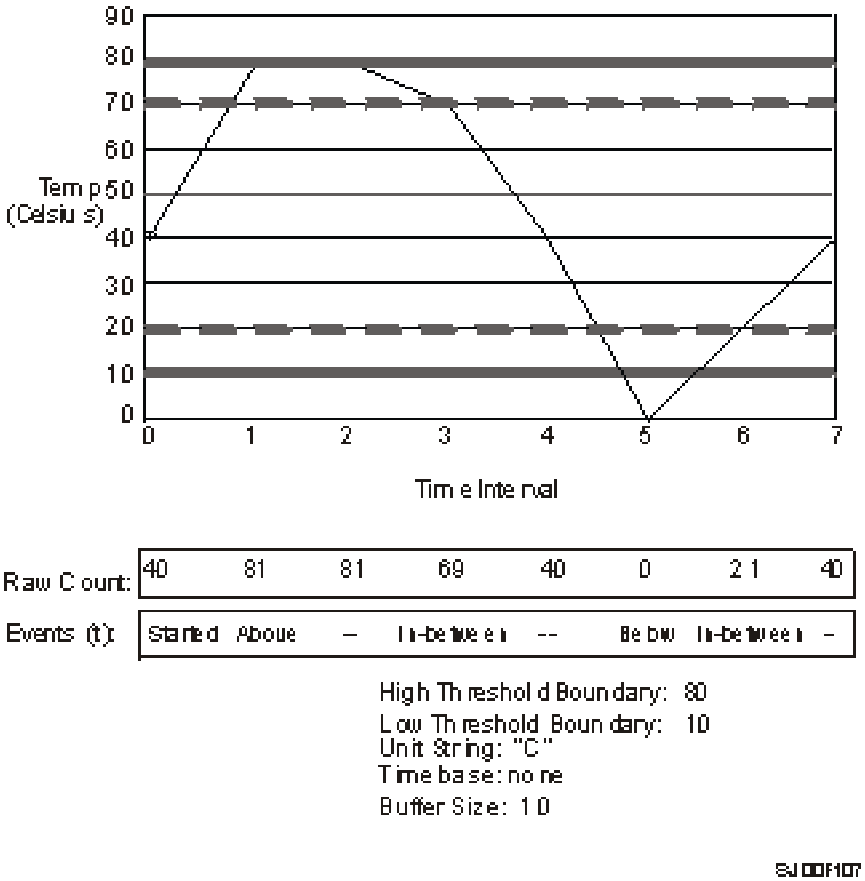
Threshold behavior models

There are three threshold behavior models: range, rising or falling, and change monitor.

Range threshold

A range threshold tracks whether a fabric element is within a specified range. It includes a minimum and maximum boundary for the area, with buffer zones to prevent repeated events due to oscillation of the value over a threshold boundary. If the value exceeds the low or high threshold boundary, an event is generated. It can also generate events while the value is outside the limits or when it re-enters the prescribed range.

An example of a range threshold is temperature, as shown in Figure 32.



Raw Count:	40	81	81	69	40	0	21	40
Events (t):	Started	Above	–	In-between	--	Below	In-between	–

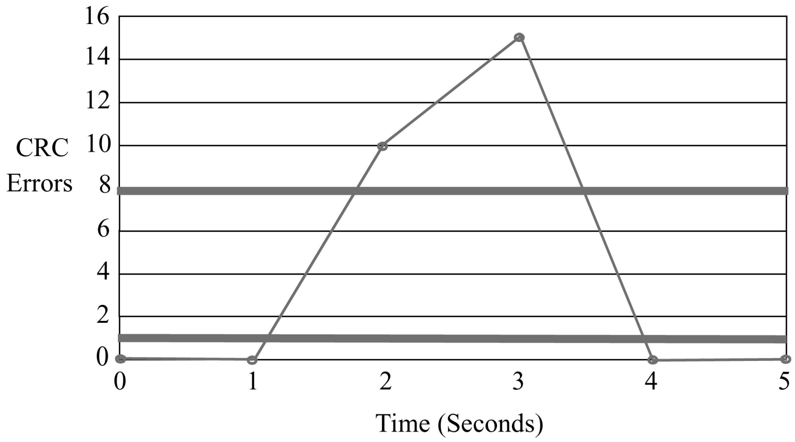
High Threshold Boundary: 80
Low Threshold Boundary: 10
Unit String: "C"
Time base: none
Buffer Size: 10

Figure 32. Example of range threshold: temperature (Celsius)

Rising or falling threshold

A rising or falling threshold tracks whether an element is on the desired side of a boundary. It includes an upper and lower boundary, and the buffer zones are always 0. Events can be selected for transitions between the boundaries. Rising or falling thresholds are typically used for rate-based counters.

An example of a rising and falling threshold is error rate, as shown in Figure 33.



Rate-based Count:	0	0	10	15	0	0
Raw Count:	0	0	10	25	25	25
Events (t):	Started	Below	Above	--	Below	--

High Threshold Boundary: 8
Low Threshold Boundary: 1
Unit String: “Error(s)”
Time base: second
Buffer Size: 0

SJ00F108

Figure 33. Example of rising and falling threshold: error rate

Changing monitor threshold

A changing monitor threshold generates events whenever a counter value changes, regardless of the type of change. This type of threshold is usually used to indicate state changes, such as zoning changes. Because change monitor thresholds include no boundaries, no illustration is provided.

Installing Fabric Watch

In order to run Fabric Watch, a license must be installed on each 3534 Managed Hub where you want to enable Fabric Watch. A license might have been installed in the hub at the factory. If not, contact your IBM sales representative to obtain a license key.

Fabric Watch requires a 3534 Managed Hub with Fabric OS version 2.2 or later. A Fabric Watch license can be installed either with Telnet commands or the IBM StorWatch Specialist.

Installing Fabric Watch through Telnet

Perform the following procedure to install Fabric Watch through Telnet.

1. Log onto the hub by Telnet using an account that has administrative privileges.
2. To determine whether a Fabric Watch license is already installed on the hub, type licenseShow on the Telnet command line.

   A list is of all of the licenses currently installed on the hub is displayed. For example:

```
admin> licenseShow
1A1AaAaaaAAAA1a:
Release v2.2
Web license
Zoning license
SES license
```

   If the Fabric Watch license is not included in the list or is incorrect, continue with step 3.

3. Type the following on the command line:

   `licenseAdd “key”`

   where *“key”* is the license key provided to you, surrounded by double quotes. The license key is case sensitive and must be entered exactly as given.

4. Verify that the license was added by typing the following on the command line:

   `licenseShow`

   If the Fabric Watch license is not listed, repeat step 3. If the Fabric Watch license is listed, continue with step 5.

5. Load the Fabric Watch classes and areas by typing `fwClassIniton` the command line, or restarting the hub.

The Fabric Watch feature is available as soon as step 5 is complete.

Installing Fabric Watch using the IBM StorWatch Specialist

Perform the following procedure to install Fabric Watch using the IBM StorWatch Specialist.

1. Launch the Web browser. Type the hub name or IP address in the **Location/Address** field (for example: `http://111.222.33.1`), and press Enter.

   The IBM StorWatch Specialist launches, displaying the Fabric View.
2. Click **Admin** on the relevant hub panel.

   The Logon window is displayed.
3. Type a logon name and password with administrative privileges and press Enter.

   The Administration View is displayed.
4. Select the **License Admin** tab, type the license key in the **License Key**: field, and click **Add License**.
5. Load the Fabric Watch classes and areas by typing the Telnet command `fwClassInit` on the command line or by restarting the hub.

The Fabric Watch feature is available as soon as step 5 is complete.

Using Fabric Watch

Fabric Watch provides information about each out-of-boundary condition discovered, including:

- The name of the threshold
- The current value of the element counter
- The unit of measurement (for example, degrees Celsius, RPM, or unit of time)
- The time base for the counter, used to compute the rate of change (for example, events per minute)
- Historical information about the last alarmed event that was generated

You can view and modify Fabric Watch settings using the IBM StorWatch Specialist, the Telnet interface, an SNMP-based enterprise manager, or the configuration file.

IBM StorWatch Specialist

Using the IBM StorWatch Specialist, you can:

- View the fabric and hub events through the fabric-wide Event View.
- View and modify the threshold and alarm configurations through the Fabric Watch View.
- Upload and download the configuration file from the **Config Admin** tab in the Hub Admin window.

Telnet interface

You can perform the following actions using a Telnet interface:

- Query fabric and hub events using the **fwShow** command.
- Query and modify threshold and alarm configurations using the **fwConfigure** command. Both the default and customized settings are provided.
- Upload and download the configuration file using the **configUpload** and **configDownload** commands.

SNMP-based enterprise manager

The Fabric Watch configuration information is stored as Management Information. Base (MIB) variables, allowing you to perform the following actions:

- Query the MIB variable for individual fabric and hub elements
- Query and modify threshold and alarm configurations
- Receive generated SNMP traps when threshold conditions are met

Configuration file

You can view and modify the threshold and alarm configurations by uploading the configuration file from the hub to the host, editing the file with a text editor, then downloading the modified file back to the hub. You can then ensure a uniform configuration throughout the fabric by distributing the configuration file to all the hubs in the fabric.

The configuration file can be uploaded and downloaded through either the IBM StorWatch Specialist (the **Config Admin** tab in the Hub Admin window) or by using **configUpload** and **configDownload** commands. After downloading the configuration file back to the hub, you must either restart the hub or use the **fwConfigReload** command to reload the configuration file.

Classes

Fabric and hub elements are organized into groupings of closely related elements called *classes*. There are seven major classes:

Fabric Monitors key fabric resources such as fabric reconfiguration, zoning changes, and new fabric logins.

Environmental
Monitors hub environment functions such as temperature, power supply, and fan status.

Port Monitors port error and performance counters.

E_port Monitors E_port error and performance counters.

F/FL_port (optical)
Monitors optical F/FL_Pport error and performance counters.

GBICs Monitors operational values for smart GBICs.

In addition, each class is subdivided into areas, as listed in Table 7.

Table 7. Fabric Watch classes and areas

Class	Area	Description
Fabric	Loss of E_port	Monitors E_port status.
	Fabric reconfiguration	Monitors fabric configuration changes.
	Segmentation changes	Monitors segmentation changes.
	Domain ID changes	Monitors forcible domain ID changes.
	Zoning changes	Monitors changes to currently enabled zoning configuration.
	Fabric to QuickLoop changes	Monitors ports to detect changes from fabric to QuickLoop or QuickLoop to fabric.
	Fabric logins	Monitors the number of host device fabric logins.
	GBIC change	Monitors insertion and removal of GBIC.
Environmental	Temperature	Monitors hub temperature.
	Fan	Monitors operation of hub fans.
	Power supply	Monitors status of each power supply.
Port	Link failure count	Monitors link failure for each port.
	Loss of synchronization count	Monitors port sync loss.
	Loss of signal count	Monitors port signal loss.
	Primitive sequence protocol error	Monitors port protocol errors.
	Invalid transmission word	Monitors port invalid words.
	Invalid CRC count	Monitors port CRC errors.
	Receive performance	Monitors port receive performance.
	Transmit performance	Monitors port transmit performance.
	State changes	Monitors port state changes.

Table 7. Fabric Watch classes and areas (continued)

Class	Area	Description
E_port	Link failure count	Monitors the error rate of each E_port.
	Loss of synchronization count	Monitors the E_port sync loss.
	Loss of signal count	Monitors E_port signal loss.
	Primitive sequence protocol error	Monitors E_port protocol errors.
	Invalid transmission word	Monitors E_port invalid words.
	Invalid CRC count	Monitors E_port CRC errors.
	Receive performance	Monitors E_port receive performance.
	Transmit performance	Monitors E_port transmit performance.
	State changes	Monitors E_port state changes.
F/FL_port (optical)	Link failure count	Monitors the error rate of each optical F/FL_port.
	Loss of synchronization	Monitors optical F/FL_port sync loss.
	Loss of signal count	Monitors optical F/FL_port signal loss.
	Primitive sequence protocol error	Monitors optical F/FL_port protocol errors.
	Invalid transmission word	Monitors optical F/FL_port invalid words.
	Invalid CRC count	Monitors optical F/FL_port CRC errors.
	Receive performance	Monitors optical F/FL_port receive performance.
	Transmit performance	Monitors optical F/FL_port transmit performance.
	State changes	Monitors optical F/FL_port state changes.

Table 7. Fabric Watch classes and areas (continued)

Class	Area	Description
F/FL_port (copper)	Link failure count	Monitors the error rate of each copper F/FL_port.
	Loss of synchronization count	Monitors copper F/FL_port sync loss.
	Loss of signal count	Monitors copper F/FL_port signal loss.
	Primitive sequence protocol error	Monitors copper F/FL_port protocol errors.
	Invalid transmission word	Monitors copper F/FL_port invalid words.
	Invalid CRC count	Monitors copper F/FL_port CRC errors.
	Receive performance	Monitors copper F/FL_port receive performance.
	Transmit performance	Monitors copper F/FL-port transmit performance.
	State changes	Monitors copper F/FL_port state changes.
GBIC (Smart GBIC)	Temperature	Monitors GBIC temperature.
	Receiver power	Monitors GBIC receiver power.
	Transmitter power	Monitors GBIC transmitter power.
	Current	Monitors GBIC current.

Threshold naming conventions

All threshold names consist of the following three items, with no separators:

- The abbreviation for the class name (alphabetic characters, lowercase). Table 8 lists the valid class name abbreviations.

Table 8. Valid class name abbreviations

Class	Abbreviation
Fabric	fabric
Environment	env
Port	port
E_port	eport
F/FL_port (optical)	fopport

Table 8. Valid class name abbreviations

Class	Abbreviation
F/FL_port (copper)	fcuport
GBIC	gbic

- The abbreviation for the area name (alphabetic characters, title case). For example, “Temp” for the Temperature area.
- The index number for the number of the item within the series. This index number consists of three numbers, for example: 000 for the first port, 001 for the next, and so on. Index numbers begin with 000 for the Fabric, Port, E_port, F/FL_port (optical), F/FL_port (copper), and GBIC classes. Index numbers for the Environment class begin with 001.

Example of a threshold name:

The threshold corresponding to the first thermometer in the hub is in the Environment class, Temperature area, and is therefore named envTemp001.

Events

An event is generated each time a boundary, as defined by the threshold, is crossed. Boundaries are not inclusive, so events are generated only when a boundary is exceeded, not when the monitored value has only reached them. If the event has an assigned alarm, an alarm is also generated. The alarm can be designated as an SNMP trap, an entry in the hub error log, locking of the port log, or a combination of these options.

When an item such as an E_port, F/FL_port (optical), F/FL_port (copper), smart GBIC, fan, or power supply is removed, Fabric Watch might raise an event (such as a below event); then the threshold is hidden and disabled. When an item is added, the threshold is displayed and enabled, and Fabric Watch might raise an event.

Event policies control the generation of events, and can be configured for either triggered events or continuous events.

Triggered events

A triggered event results in a single event when a boundary is exceeded. The event is not generated again until the threshold value has returned within the boundaries and then once again exceeded them. For example, if the hub temperature exceeds the upper boundary, a triggered event is generated at the point the boundary is crossed, but is not repeated while the temperature remains above the upper boundary.

The following events can be generated as triggered events:

Started No alarm is generated.

Below The counter is below the lower boundary. Must be preceded by a start, above, or in-between event.

Above The counter is above the upper boundary. Must be preceded by a start, below, or in-between event.

Exceeded
The counter is below the lower boundary or above the upper boundary. Accompanies a below or above event.

Changed The counter value has changed.

In-between
The counter falls below the upper boundary minus buffer, or rises above the lower boundary plus buffer. Must be preceded by an above or below event. If the buffer is set to zero, this event is suppressed.

Continuous events

A continuous event results in an event at each time interval from when the boundary is initially exceeded until the threshold value has returned within the boundaries. For example, if port usage is above the upper boundary, a new event is generated at each behavior interval until usage falls below the upper boundary. The following events can be generated as continuous events:

Started No alarm is generated.

Below The counter is below the lower boundary.

Above The counter is above the upper boundary.

Exceeded
The counter is below the lower boundary or above the upper boundary. Accompanies a below or above event.

Changed The counter has changed.

Alarms

Each event can generate one or more alarms. Fabric Watch supports three types of alarms: SNMP trap, error log entry, and locking of the port log.

SNMP trap

The following information is forwarded to an SNMP management station:

- The name of the element
- The class, area, and index of the threshold
- The type of event generated
- The element value

- The new state of the element

Error log entry

The internal error log maintains a record of the event, up to a maximum of 64 entries. If configured to do so, error log entries are forwarded to the syslogd facility.

Locking of the port log

This alarm freezes the hub port log to retain detailed information about a problem. Typically, this is used in conjunction with the error log entry.

Configuring thresholds and alarms

The configuration of thresholds and alarms can be divided into two categories: threshold values and threshold area values.

Threshold values

Threshold values apply to the specific threshold. They are not stored in the configuration file, and return to the default values when the hub is restarted. The following threshold values can be modified.

Status Can be enabled or disabled. It is enabled by default.

Behavior type
Allows setting of the event policy to triggered or continuous. It is set to triggered by default.

Behavior interval
The interval between the same type of alarm. This value applies only to continuous events. The default interval is 1 second.

The threshold area values include boundaries and alarms, and apply to all the thresholds within an area. Changes are stored in the configuration file.

Boundaries

The following boundary information can be modified:

Unit string
Represents unit value. Only the default unit strings are supported by Fabric Watch.

Time base
The time period within which a specified event is measured. It can be from one second to one day. Shorter time periods are more sensitive to fluctuations and therefore provide more detailed information.

Low boundary
The minimum value. An event is generated if the element value falls below this boundary.

High boundary
The maximum value. An event is generated if the element value rises above this boundary.

Buffer size
The size of the buffer set up to decrease generation of in-between events due to oscillation of the element value over a boundary.

The following alarms can be added or deleted:

ERRLOG Logs errors to the hub. If configured properly, it sends a message to the syslog daemon.

SNMP-TRAP
Sends traps to the SNMP agent.

PORT-LOG-LOCK
The Fabric Watch freezes the port log to preserve the log information that is generated at the time of the event. This is done for diagnostic purposes.

Telnet commands overview

This section provides information about the Telnet commands that are available for managing the Fabric Watch feature.

The Telnet commands become available through the shell admin account when the license key is installed. To use a Telnet command, log into the relevant hub with administrative privileges, enter the command along with any required operands, and press Enter.

Note: Fabric Watch can be accessed simultaneously from different connections, by Telnet, SNMP, IBM StorWatch Specialist, or by modifying and uploading the Fabric Watch configuration file to the hub. In this case, changes from one connection might not be updated to the other, and some might be lost. If “`Committing configuration...`” is displayed during a Telnet session, then the configuration might have recently been modified from another connection.

Table 9 contains a summary of the Fabric Watch Telnet commands, along with a reference to the detailed explanations of the command

Table 9. Fabric Watch Telnet commands

Command	**Description**	**Page**
fwClassInit	Initializes all classes under Fabric Watch.	73
fwConfigReload	Reloads the Fabric Watch configuration.	73
fwConfigure	Displays and allows modification of threshold information and the Fabric Watch configuration.	74

Table 9. Fabric Watch Telnet commands (continued)

Command	**Description**	**Page**
fwShow	Displays the thresholds that are monitored by Fabric Watch.	77

Telnet commands

fwClassInit command

Use the **fwClassInit** command to initialize all classes under Fabric Watch.

syntax

```
fwClassInit
```

Availability

Administrator

Description

Use this command to initialize all classes under Fabric Watch. The **fwClassInit** command should only be used after installing a Fabric Watch license, to initialize the licensed Fabric Watch classes.

Operands

None

Example

```
sw:admin> fwClassInit
gbicRegister: re-register 0x0
0x10f6c260
fwClassInit: Fabric Watch initialized
```

See also

fwConfigReload
fwConfigure
fwShow

fwConfigReload

Use the **fwConfigReload** command to reload the Fabric Watch configuration.

syntax

```
fwConfigReload
```

Availability

Administrator

Description

Use this command to reload the Fabric Watch configuration. This command should only be used after downloading a new Fabric Watch configuration file from a host.

Operands

None

Example

```
sw:admin> fwConfigReload
fwConfigReload: Fabric Watch configuration reloaded
```

See also

configUpload
configDownload
fwClassInit
fwConfigure
fwShow

fwConfigure

Use the **fwConfigure** command to display the Fabric watch configuration or status. It is also used to modify the configuration.

syntax

`fwConfigure`

Availability

Administrator

Description

Use the command to allow the admin account to display and modify threshold information and the Fabric Watch configuration. Hub elements that are monitored by Fabric Watch are divided into classes, which are further divided into areas. In addition, each area can include from 0 - 16 thresholds. The Fabric Watch classes and areas are provided in the following list.

Class	Area
Fabric	Loss of E_port
	Fabric reconfigure
	Segmentation changes
	Domain ID changes
	Zoning changes
	Fabric to QuickLoop changes
	Fabric logins
	GBIC change
Environmental	
	Temperature
	Fan
	Power supply
Port	Link failure count
	Loss of synchronization count
	Loss of signal count
	Primitive sequence protocol error

Invalid transmission word
Invalid CRC count
Receive performance
Transmit performance
State changes

E_port Link failure count
Loss of synchronization count
Loss of signal count
Primitive sequence protocol error
Invalid transmission word
Invalid CRC count
Receive performance
Transmit performance
State changes

F/FL_port (optical)
Link failure count
Loss of synchronization count
Loss of signal count
Primitive sequence protocol error
Invalid transmission word
Invalid CRC count
Receive performance
Transmit performance
State changes

F/FL_port (copper)
Link failure count
Loss of synchronization count
Loss of signal count
Primitive sequence protocol error
Invalid transmission word
Invalid CRC count
Receive performance
Transmit performance
State changes

GBIC Temperature
Received power
Transmitted power
Current

Operands

None

Example

The following example shows displaying the Fabric Watch configuration and status:

```
sw:admin> fwConfigure
1 : Environment class
2 : GBIC class
3 : Port class
4 : Fabric class
5 : E-Port class
6 : F/FL Port (Copper) class
7 : F/FL Port (Optical) class
8 : quit
Select a class => : (1..8) [8] 1
1 : Temperature
2 : Fan
3 : Power Supply
4 : return to previous page
Select an area => : (1..4) [4] 1
Index ThresholdName Status CurVal
LastEvent LastEventTime LastVal
LastState
==========================================
1 envTemp001 enabled 33 C
started 10:28:59 on 02/01/2000 0 C
Informative
2 envTemp002 enabled 34 C
started 10:28:59 on 02/01/2000 0 C
Informative
3 envTemp003 enabled 36 C
started 10:28:59 on 02/01/2000 0 C
Informative
4 envTemp004 enabled 35 C
started 10:28:59 on 02/01/2000 0 C
Informative
5 envTemp005 enabled 36 C
started 10:28:59 on 02/01/2000 0 C
Informative
1 : refresh
2 : disable a threshold
3 : enable a threshold
4 : advanced configuration
5 : return to previous page
Select choice => : (1..5) [5]
```

See also

fwClassInitfw
ConfigReload
fwShow

fwShow

Use the **fwShow** command to display the thresholds that are monitored by Fabric Watch.

Syntax

```
fwShow
```

Availability

All users

Description

Use this command to display the thresholds that are monitored by Fabric Watch. If no parameters are entered, a summary of all thresholds is displayed and printed. If a valid threshold name is entered as a parameter, detailed information pertaining only to that threshold is displayed and printed.

Operands

None

Fabric Watch view (optional software)

You can use the Fabric Watch view to monitor fabric elements for potential problem conditions. This feature requires an active Fabric Watch license.

To access the Fabric Watch view:

1. Launch the Web browser.
2. Enter the hub name or IP address in the **Location/Address** field and press Enter. For example:

   ```
   http://switch name/
   ```

   IBM StorWatch Specialist launches, displaying the fabric view.
3. Click on the **hub** icon.

   The Hub view is displayed.
4. Click on the **watch** icon.

   The Fabric Watch view is displayed, with the **Threshold** tab (described in the following section) selected by default.

Fabric Watch view contains three tabs: **Threshold**, **Boundaries Config**, and **Alarm Config**. The following items are visible regardless of which tab is selected:

Refresh button

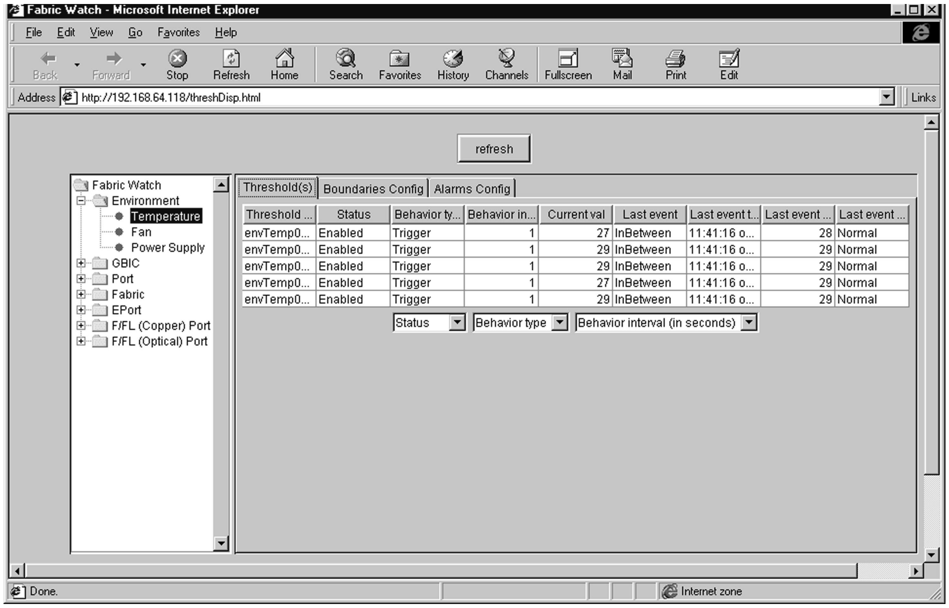
Click to update the information in the Fabric Watch view.

Fabric Watch tree

The folders represent Fabric Watch classes, and the bullets represent Fabric Watch areas. You can click on a folder to view a list of the areas in the class represented by the folder. You can click on a bullet to view the information for the selected area in the tabs to the right.

Threshold tab

You can use the **Threshold** tab to configure Fabric Watch thresholds. See Figure 34 on page 78.


Fabric Watch - Microsoft Internet Explorer
File Edit View Go Favorites Help
Back Forward Stop Refresh Home Search Favorites History Channels Fullscreen Mail Print Edit
Address http://192.168.64.118/threshDisp.html
Links
refresh
Fabric Watch
Environment
Temperature
Fan
Power Supply
GBIC
Port
Fabric
EPort
F/FL (Copper) Port
F/FL (Optical) Port
Threshold(s)
Boundaries Config
Alarms Config
Status
Behavior type
Behavior interval (in seconds)
Done.
Internet zone

Threshold ...	Status	Behavior ty...	Behavior in...	Current val	Last event	Last event t...	Last event ...	Last event ...
envTemp0...	Enabled	Trigger	1	27	InBetween	11:41:16 o...	28	Normal
envTemp0...	Enabled	Trigger	1	29	InBetween	11:41:16 o...	29	Normal
envTemp0...	Enabled	Trigger	1	29	InBetween	11:41:16 o...	29	Normal
envTemp0...	Enabled	Trigger	1	27	InBetween	11:41:16 o...	29	Normal
envTemp0...	Enabled	Trigger	1	29	InBetween	11:41:16 o...	29	Normal

SJ00F130

Figure 34. Threshold tab in the Fabric Watch view

The **Threshold** tab includes the following fields:

Threshold Name
Displays the names of the thresholds in the class or area selected in the Fabric Watch tree. Names are comprised of class name, area name, and threshold index number.

Status Displays the current status. To change the threshold status, select the threshold name, click the **Status** drop-down list, and select the new status.

Behavior type
Sets or displays the behavior type. To change the threshold behavior type, select the threshold name, click the **Behavior type** drop-down list, and select the new behavior.

Behavior interval
Sets or displays the behavior interval. To change the threshold behavior interval, select the threshold name, click the **Behavior interval** drop-down list, and select the new interval.

Current val column
Displays the current value of the counter.

Last event
Displays the type of the last event that generated an alarm.

Last event time
Displays the time that the last event was generated.

Last event val
Displays the last value of the counter (that is, the value that generated the last event).

Last event state
Displays the last state of the event.

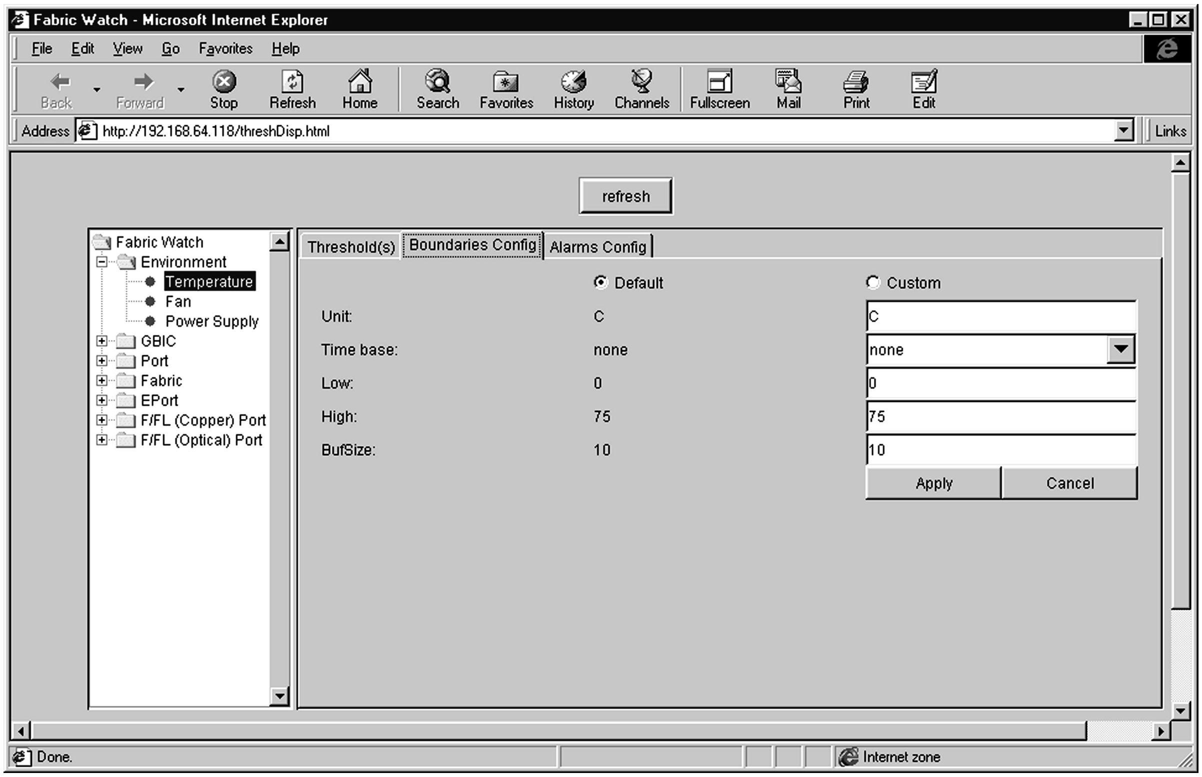
Status drop-down list
Click to select the status (enabled or disabled) of the selected threshold.

Behavior type drop-down list
Click to select the type of event (triggered or continuous) for the selected threshold.

Behavior interval drop-down list
Click to select the interval between alarms for the selected threshold.

Boundaries Config tab

Click the **Boundaries Config** tab to configure Fabric Watch boundaries. See Figure 35.


Fabric Watch - Microsoft Internet Explorer
File Edit View Go Favorites Help
Back Forward Stop Refresh Home Search Favorites History Channels Fullscreen Mail Print Edit
Links
refresh
Fabric Watch
Environment
Temperature
Fan
Power Supply
GBIC
Port
Fabric
EPort
F/FL (Copper) Port
F/FL (Optical) Port
Threshold(s) Boundaries Config Alarms Config
Apply Cancel
Done.
Internet zone

Address http://192.168.64.118/threshDisp.html

	● Default	○ Custom
Unit:	C	C
Time base:	none	none
Low:	0	0
High:	75	75
BufSize:	10	10

SL000162

Figure 35. Boundaries Config tab in the Fabric Watch view

The **Boundaries Config** tab includes the following fields:

Default Displays the default values for area config alarms:

Changed
Exceeded
Below
Above
InBetween

Select Syslog, SNMP_Trap, or Port log lock to indicate the type of alarm you want to associate with each event.

Custom Specifies the custom values for area config alarms:

Changed
Exceeded
Below
Above
InBetween

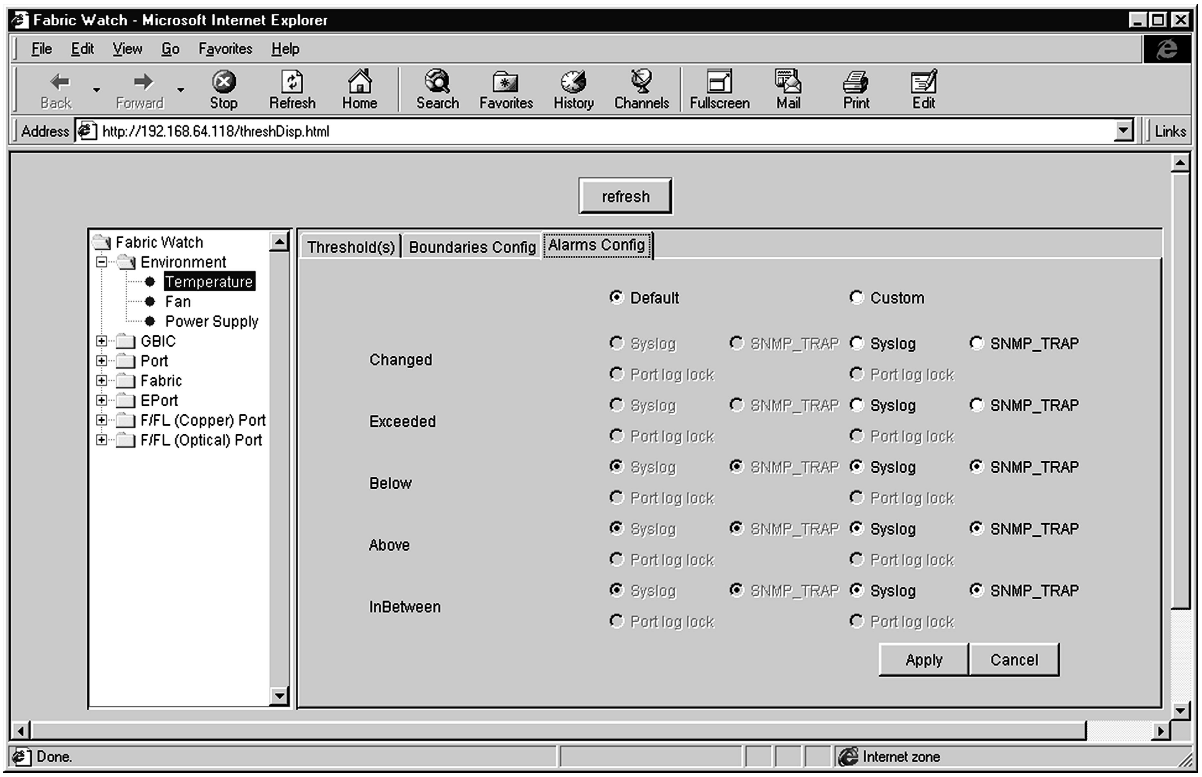
Select Syslog, SNMP_Trap, or Port log lock to indicate the type of alarm that you want to associate with each event.

Apply Click to apply specified values.

Cancel Click to cancel changes made to custom values.

Alarm config tab

Click the **Alarm Config** tab to configure Fabric Watch alarms. See Figure 36.



Address: http://192.168.64.118/threshDisp.html

● Default ○ Custom

	Default		Custom	
Changed	○ Syslog	○ SNMP_TRAP	○ Syslog	○ SNMP_TRAP
	○ Port log lock		○ Port log lock	
Exceeded	○ Syslog	○ SNMP_TRAP	○ Syslog	○ SNMP_TRAP
	○ Port log lock		○ Port log lock	
Below	● Syslog	● SNMP_TRAP	● Syslog	● SNMP_TRAP
	○ Port log lock		○ Port log lock	
Above	● Syslog	● SNMP_TRAP	● Syslog	● SNMP_TRAP
	○ Port log lock		○ Port log lock	
InBetween	● Syslog	● SNMP_TRAP	● Syslog	● SNMP_TRAP
	○ Port log lock		○ Port log lock	

SL000161

Figure 36. Alarm Config tab in Fabric Watch view

The Alarm Config tab includes the following fields:

Default Displays the default values for area config alarms:

Changed
Exceeded
Below
Above
InBetween

Select Syslog, SNMP_Trap, or Port log lock to indicate the type of alarm that you want to associate with each event.

Custom Specifies the custom values for area config alarms:

Changed
Exceeded
Below
Above
InBetween

Select Syslog, SNMP_Trap, or Port log lock to indicate the type of alarm that you want to associate with each event.

Apply Click to apply specified values.

Cancel Click to cancel changes made to custom values.

The Fabric Watch subsystem group is available with a Fabric Watch license.

Fabric Watch sends an enterprise-specific trap for an event that is about to be monitored.

Hub view

The Hub view is a representation of the front panel of the 3534 Managed Hub and is displayed when you click on a hub icon from the Fabric view. The information that is displayed is as close as possible to a real-time view of hub status. If the hub is not functioning properly, a message explains the problem that was detected.

To access the hub view:

1. Launch the Web browser.
2. Enter the hub name or IP address in the **Location/Address** field and press Enter. For example:

   ```
   http://switch name/
   ```

   IBM StorWatch Specialist launches and displays the Fabric view.
3. Click on the **hub** icon.

   The Hub view is displayed.

Following is a description of the items and information that are available in Hub view.

Watch (optional software)
Click to access Fabric Watch, if a license is installed.

Getting help

Contact your IBM sales representative for technical support. This includes hardware and software support, all repairs, and spare components. Be prepared to provide the following information to the support personnel:

- The hub serial number
- The hub WWN
- The output from the **supportShow** Telnet command
- A detailed description of the problem
- The topology configuration
- Any troubleshooting steps that you have already performed

Getting software updates

Contact your IBM sales representative for software updates and maintenance releases or see the Web site at:

www.ibm.com/storage/fcswitch/

New hub firmware can be installed from the following host operating systems:

- UNIX
- Windows NT
- Windows 98
- Windows 95
- Windows 2000 millennium

Chapter 5. Zoning

Note: Throughout this book, the term *switch* applies to both switches and hubs unless otherwise noted.

This chapter contains general information about managing and monitoring a switch using zoning. See Chapter 7. QuickLoop Zoning on page 111 for more information. The following topics are discussed:

- Overview
- Zoning components
- Zone management
- Zone enforcement
- Multiswitch fabrics
- Zoning commands

Overview

Zoning is used to set up barriers between different operating environments, to deploy logical fabric subsets by creating defined user groups, or to create test or maintenance areas, or both, which are separated within the fabric.

Zoning gives you the flexibility to manage a storage area network (SAN) to meet different closed user groups objectives.

Figure 37 on page 86 shows a typical use of zoning. Zoning is a fabric management service used to create logical device subsets within a SAN, and enables resource partitioning for management and access control.

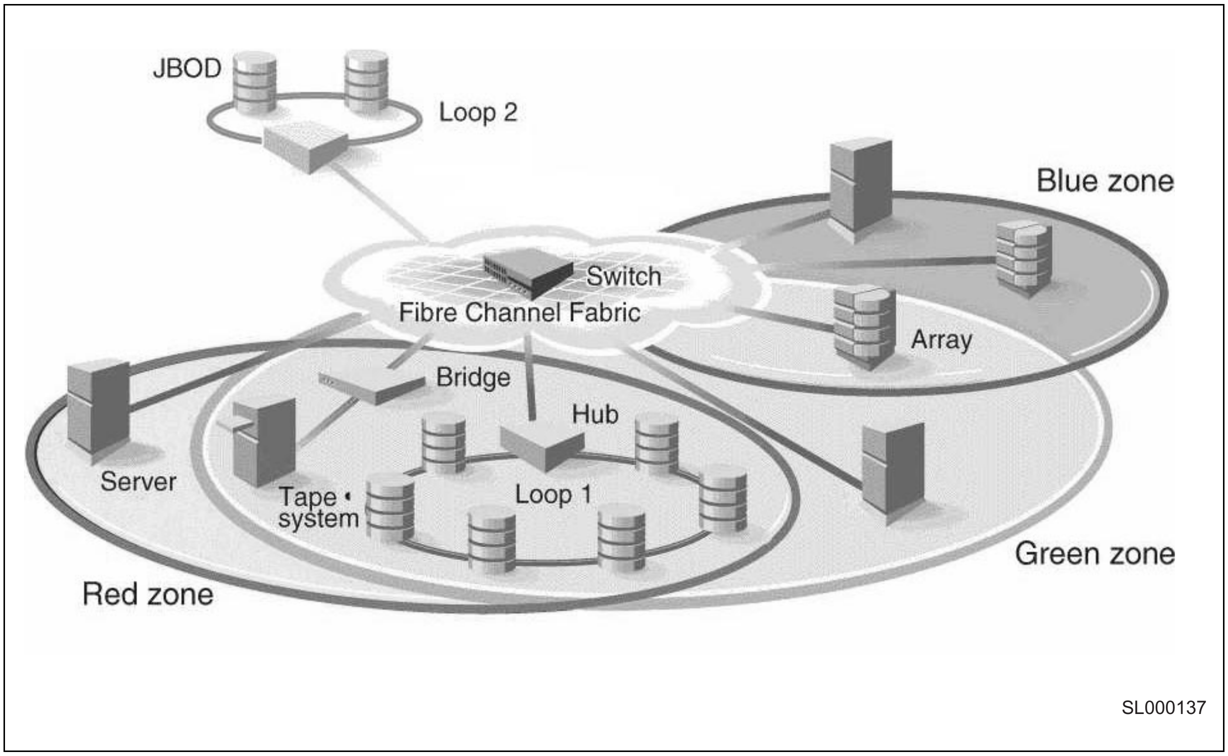


Figure 37. A fabric with three zones

The benefits of zoning include:

- Increased environmental security where and when needed.
- Optimization of information technology (IT) resources in response to user demand and changing user profiles.
- Versatility to customize environments as needed.

One or more switches create the fibre-channel fabric. This infrastructure is used to deploy and manage IT resources as a network. Using zoning, fabric-connected devices are arranged into logical groups over the physical fabric configuration. Zoning is one of the fabric services that provide automatic and transparent management for the SAN.

Increased SAN control

Zoning allows you to create segmentation or zones within a fabric. The zones are comprised of selected storage devices, servers, and workstations. It also enforces access of information to only the devices in the defined zone.

Zones can be configured dynamically. The number of zones and zone members are effectively unlimited. Zones vary in size and shape, depending on the number of fabric-connected devices and device locations. Devices can be members of more than one zone. In addition, temporary zones can be created, for example, for enterprise backup. Zone members detect only members in their zones and, therefore, only access each other. A device that is not included in a zone is not available to the zone devices.

Functions of zoning

Zoning involves:

- *Zone management* – Telnet commands or the StorWatch Specialist are used to:
  - Create, delete, and display zones
  - Add or remove zone members
  - Configure zone sets
- *Zone enforcement* – the fabric automatically and transparently restricts access to only the devices that are defined zone members.
- *Zone specification* – you create and manipulate the zones, zone configurations, and zone aliases.

Uses for zoning

Uses for zoning include:

- Providing integrated support for heterogeneous environments by isolating systems that have different operating environments or uses.
- Creating fabric functional areas by separating test or maintenance areas from production areas.
- Designating closed user groups by including certain zone devices for exclusive use by zone members.
- Simplifying resource usage by consolidating equipment logically for convenience.
- Promoting time-sensitive functions by creating a temporary zone used to back up a set of devices that are members of other zones.
- Securing fabric areas by providing another level of software security to control port-level access.

Zoning concepts

This section discusses zones, zoning concepts, and zoning components.

Zone definition

A zone is a set of devices that access one another. All devices that are connected to a fabric can be configured into one or more zones. Devices that are in the same zone can see each other, devices that are in different zones cannot.

Every zone has a name that begins with a letter and is followed by any number of letters, digits, and the underscore character (_). Names are case sensitive, for example Zone_1 and zone_1 are different zones. Note that spaces are not allowed.

Every zone has a member list, consisting of one or more members (empty zones are not allowed). See "Zone members" for more information about member list specifications.

The maximum number of zones and the maximum number of members in a zone are constrained by memory usage. Because these limits are greater than the number of devices connected to a fabric, they are effectively unlimited.

Zone definitions are persistent. That is, the definition remains in effect after restarts and power on and off cycles until the definition is deleted or changed.

A device can be a member of multiple zones.

Zoning components

Zoning has several components, in addition to the zones themselves. These components are:

- Zone members
- Zone aliases
- Zone configurations

These components are generically referred to as zone objects.

Zone members

All zone members can be specified using one of the following notations:

- Physical fabric port number
- Node world-wide name
- Port world-wide name

A physical fabric port number notation is specified as a pair of decimal numbers (*s*, *p*), where:

- *s* - is the switch number (domain ID)
- *p* - is the switch port number

For example, 2,12 specifies port 12 on switch number 2. When a zone member is specified by a physical fabric port number, any and all devices connected to that port are in the zone. If this port is an arbitrated loop, all loop devices are in the zone.

A world-wide name notation (node and port) is specified as an 8-hex number separated by colons, for example 10:00:00:60:69:00:00:8a. Zoning has no field knowledge within a world-wide name, the eight bytes are simply compared with the node and port names presented by a device in a login frame (fabric login [FLOGI] or port login [PLOGI]). When a zone member is specified by node name, all ports on that device are in the zone. When a zone member is specified by port name, only that single device port is in the zone

The type of zone members used to define a zone can be mixed and matched. For example, a zone that is defined with the following members:

2,12; 2,14; 10:00:00:60:69:00:00:8a

would contain the devices that are connected to switch 2, ports 12 and 14, and the device with either node name or port name of 10:00:00:60:69:00:00:8a, whichever port in the fabric it is connected to.

For examples of zone members, see "Zoning setup and administration" on page 92.

Zone aliases

Zone aliases simplify repetitive port number entries or world-wide names. A zone alias is a C-style name for one or more port numbers or world-wide names. For example, the name *host* could be used as an alias for 10:00:00:60:69:00:00:8a.

Zone configurations

A zone configuration is a set of zones. At any one time, zoning can be disabled or one zone configuration can be in effect. When a zone configuration is in effect, all zones that are members of that configuration are in effect. You select which zone configuration is currently in effect.

The set of zone configurations defined in a fabric cannot be the same as:

- The configuration that is currently in effect.
- The configurations that are saved in the flash memory of the switch.

The following three terms are used to differentiate between these configurations:

Defined configuration

The defined configuration is the complete set of all zone objects that have been defined in the fabric. There can be multiple zone configurations defined, although only one can be in effect at a time. There might be inconsistencies in the definitions, there might be zones or aliases that are referenced but are not defined, or there might be duplicate members. The defined configuration is the current state of the administrator’s input.

Effective configuration

The effective configuration is a single zone configuration that is currently in effect. The devices that a server initiator detects are based on this configuration.

The effective configuration is built when a specified zone configuration is enabled. This configuration is compiled by checking for undefined zone names, zone alias names, or other inconsistencies. This is done by expanding zone aliases, removing duplicate entries, and building the effective configuration.

Saved configuration

The saved configuration is a copy of the defined configuration, plus the name of the effective configuration that is saved in flash memory by the **cfgSave** command. There might be differences between the saved configuration and the defined configuration if you have modified any zone definitions and have not saved them.

The saved configuration is automatically reloaded by the switch during start up. If a configuration was in effect when it was saved, the same configuration is reinstated with an automatic **cfgEnable** command.

Example of zone configuration

Figure 38 on page 91 shows a single configuration (USA_cfg) with three zones. The zones are defined as follows:

- The red and green zones share six disk drives on a loop.
- The blue and green zones share one storage array.
- The blue zone has a dedicated storage array.

Note that the JBOD with Loop 2 *is not* in any zone and cannot be accessed from any zone where the configuration is in effect.

The disks are specified by world-wide name and the hosts are specified by physical port.

The following example shows how commands are used to configure zones.

```
admin> aliCreate "array1", "21:00:00:20:37:0c:76:85; 21:00:00:20:37:0c:71:df"
admin> aliAdd "array1", "21:00:00:20:37:0c:72:51; 21:00:00:20:37:0c:71:0a"
admin> aliCreate "array2", "21:00:00:20:37:0c:66:23; 21:00:00:20:37:0c:73:7f"
admin> aliAdd "array2", "21:00:00:20:37:0c:9c:6b; 21:00:00:20:37:0c:66:3a"
admin> aliCreate "loop1", "21:00:00:20:37:0c:67:e3; 21:00:00:20:37:0c:76:1f"
admin> aliAdd "loop1", "21:00:00:20:37:0c:6a:40; 21:00:00:20:37:0c:59:7e"
admin> zoneCreate "Red_zone", "1,0; loop1"
admin> zoneCreate "Blue_zone", "1,1; array1; 1,2; array2"
admin> zoneCreate "Green_zone", "1,0; loop1; 1,2; array2"
admin> cfgCreate "USA_cfg", "Red_zone; Blue_zone; Green_zone"
admin> cfgEnable "USA_cfg"
zone config "USA_cfg" is in effect
```

Figure 38 shows the configuration, with an additional disk drive loop to which none of the zones can communicate.

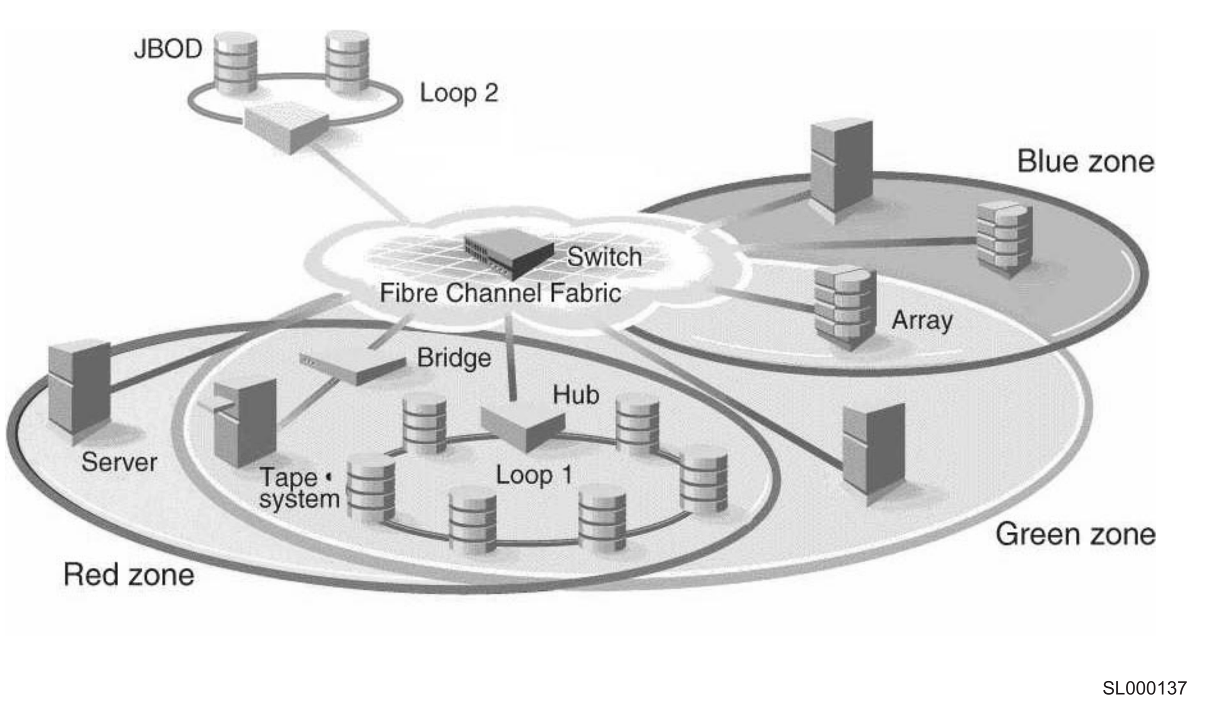


Figure 38. Example of zone configuration

Using zoning

This section contains general information and examples for managing and monitoring the switch using zoning. This section discusses:

- Zoning setup and administration of zoning

- Zone management
- Zone enforcement
- Multiswitch fabrics

Zoning setup and administration

A zone is specified by a zone name. A zone member is specified by a physical fabric port number, a node world-wide name, or a port world-wide name. Aliases (symbolic names) can be used for easy administration of zones or members. A set of zones is configured during zone specification.

You select which zone configuration is currently in effect. At any one time, you might decide that zoning is disabled or one zoning configuration is in effect, such as for backup. Once zoning is in effect, devices (or ports) that are not in a zone are not accessible for use until they are added to a zone.

Zone management

Zone management is performed using Telnet or StorWatch Specialist through out-of-band by logging into a switch. Any switch in the fabric can be used; a change that is made to the zoning information on one switch is replicated through all fabric switches

Zoning uses logical device subsets within a SAN network for resource partitioning for management and access control. Within a zone the device sets can access one another. All fabric-connected devices can be configured into one or more zones. Devices that are in different zones do not see each other.

Enforcing a zone

Zoning is enforced by the simple name server (SNS) and hardware. Zoning does not change the SNS protocol. Host device drivers query SNS using existing commands and have no knowledge that zoning is in effect. If no zone configuration is in effect, responses to SNS queries are based on all fabric-connected devices. If a zone configuration is in effect, responses to SNS queries contain information about only those devices that are in the requestor’s zone. On switches, a zone can also be enforced because hardware specifies the zone by physical fabric port number.

Adding multiple items

Multiple items can be added to a zone using zone commands. The command syntax is:

```
zoning-command “name of zone”, “member  ; member  ;
member”
```

Where `name of zone` could be a zone name, an alias name, or a configuration name, depending on if the command is for a zone, alias, or configuration, respectively. The members are separated by semicolons, but within a single pair of double quotes.

For example:

```
zoneAdd “Red_zone”, “1,10;1,12”
```

adds domain 1, port 10 and domain 1, port 12 to zone `“Red_zone”`.

Commands that can take a multiple item parameter list are:

- Configuration commands: `cfgCreate, cfgAdd`, and **cfgRemove**
- Zone commands: `zoneCreate, zoneAdd`, and `zoneRemove`
- Alias commands: `aliCreate, aliAdd, and aliRemove`

See "Zone commands" on page 99 for a complete description of these commands.

Multiswitch fabrics

There are two types of data used by zoning:

- Zone configuration data
- N_Port login data

Zone configuration data

This data is shown as the defined configuration by the **cfgShow** command, and is stored in flash by the **cfgSave** command. This data is a replicated database, all fabric switches have a complete copy. Whenever you make a configuration change, the switch where the change is made forwards the change to all fabric switches using vendor-unique interswitch protocol.

N_Port login data

N_Port login data is stored locally on each switch. N_Port login data is used to translate the world-wide name into physical port numbers when world-wide names are used in zone definitions. The zone checking procedure runs entirely on the local switch when a match can be made by physical port number alone, but when the physical port number is not sufficient, the local switch must query the remote switch to get login data. This data is cached on the local switch until a state change notification renders it invalid.

Adding a new switch

A new switch is a switch that has not previously been connected to a zoned fabric and that has had no zone configuration data entered into it. If a switch has been connected to a zoned fabric, or has had zone configuration data previously entered, see “Adding a new fabric” on page 94. A switch that has been configured for zoning can be returned to this new switch state by using the **cfgClear** command *before* connecting it to the fabric.

When a new switch is connected to a fabric, all zone configuration data is immediately copied from the fabric into the new switch. If a zone configuration is enabled in the fabric, the same configuration becomes enabled in the new switch. After this operation, the **cfgShow** command displays the same output on all switches in the fabric, including the new switch.

Adding a new fabric

Adding a new fabric (a fabric where there is no zone configuration information) to an existing zoned fabric is similar to adding a new switch. All switches in the new fabric inherit the zone configuration data. If a zone configuration is enabled, the same configuration becomes enabled in the fabric. After this operation, **cfgShow** displays the same output on all switches in the joined fabric, including the new switches.

Merging two fabrics

If two fabrics that have zone configuration information are joined, it is more complex. The zoning software attempts to merge the two zone configurations.

The simplest case is where both fabrics have identical zone configuration data and the same configuration is enabled. In this case, the fabrics join to make one larger fabric with the same zone configuration in effect across the whole new fabric.

If the fabrics have different zone configuration data, the two sets of information are merged if possible, or the interswitch link (ISL) is segmented if a merge is not possible. Merging is not possible if:

- Zoning is enabled in both fabrics and the zone configuration that is enabled is different (*cfg* mismatch)
- The name of a zone object in one fabric is used for a different type of zone object in the other fabric (*type* mismatch)
- The definition of a zone object in one fabric is different from its definition in the other fabric (*content* mismatch)

When this condition is detected by the switches between the ISL, each switch displays an error message on its LCD, Telnet console, and syslog.

Splitting a fabric

If an ISL goes down, causing a fabric to split into two separate fabrics, each new fabric retains the same zone configuration.

If the ISL is replaced and no changes have been made to the zone configuration in either new fabric, the two fabrics are guaranteed to merge back into one single fabric. If changes have been made to either zone configuration, the rules under "Merging two fabrics" apply.

Zoning commands

Zoning is managed by logging into a switch using Telnet or StorWatch Specialist. Any IBM or compatible switch can be used. A change made to the zoning information on one switch is replicated through all switches in the fabric.

This section contains information and examples on managing zones, including:

- Zone alias commands
- Zone configuration commands
- Zone commands
- Configuration management commands

The zoning commands are added to the shell *admin* account to manage zones, zone aliases, and zone configurations.

All **Add**, **Create**, **Delete**, and **Remove** commands modify the defined configuration. This has no affect on the enabled configuration until a **cfgEnable** command is run. As these commands are run, the parameter syntax is checked, but the changes are not in force until the next **enable** command is run. Table 10 summarizes the zoning commands.

Table 10. Zoning commands

Command	Description	See page
Zone alias commands		
aliAdd	Adds a member to a zone alias	96
aliCreate	Creates a zone alias	97
aliDelete	Deletes a zone alias	97
aliRemove	Removes a member from a zone alias	97
aliShow	Shows a zone alias definition	97
Zone configuration commands		

Table 10. Zoning commands (continued)

Command	Description	See page
cfgAdd	Adds a zone to a configuration	98
cfgCreate	Creates a zone configuration	98
cfgDelete	Deletes a zone configuration	98
cfgRemove	Removes a zone from a configuration	98
cfgShow	Shows a zone configuration definition	99
Zone commands		
zoneAdd	Adds a member to a zone	99
zoneCreate	Creates a zone	99
zoneDelete	Deletes a zone	100
zoneRemove	Removes a member from a zone	100
zoneShow	Shows a zone definition	100
Configuration management commands		
cfgClear	Clears all zone configurations	101
cfgDisable	Disables a zone configuration	101
cfgEnable	Enables a zone configuration	101
cfgSave	Saves zone configurations in flash memory	101
cfgShow	Shows a zone configuration definition	102

Zone alias commands

Zone alias commands let you manipulate the zone aliases.

aliAdd

The **aliAdd** command adds one or more new alias members to an existing zone alias. The command displays a list of one or more physical fabric port numbers (for example: `1,2`) or world-wide name (for example, 10:00:00:60:69:00:00:8a) separated by semicolons. White spaces are ignored. The `alias_members` list cannot contain other zone aliases. The following example shows the **aliAdd** command.

```
admin> aliAdd “array1”, “21:00:00:20:37:0c:72:51; 21:00:00:20:37:0c:71:0a”
admin> aliAdd “array2”, “21:00:00:20:37:0c:9c:6b; 21:00:00:20:37:0c:66:3a”
admin> aliAdd “loop1”,  “21:00:00:20:37:0c:6a:40; 21:00:00:20:37:0c:59:7e”
```

aliCreate

The **aliCreate** command creates a new zone alias. The alias_name is a C-style name for this zone alias and cannot be used for any other zone object. The command displays a list of one or more physical fabric port numbers (for example: `1,2`) or world-wide name (for example, 10:00:00:60:69:00:00:8a) separated by semicolons. White space is ignored. The alias_members list cannot contain other zone aliases. The following example shows the **aliCreate** command.

```
admin> aliCreate “array1”, “21:00:00:20:37:0c:76:8c; 21:00:00:20:37:0c:71:d2”
admin> aliCreate “array2”, “21:00:00:20:37:0c:66:23; 21:00:00:20:37:0c:73:7f”
admin> aliCreate “loop1”,  “21:00:00:20:37:0c:67:e3; 21:00:00:20:37:0c:76:1f”
```

The **aliDelete** command deletes an existing zone alias. The following example shows the **aliDelete** command.

```
admin> aliDelete “array2”
```

aliRemove

The **aliRemove** command removes one or more alias members from an existing zone alias. The members to be removed are found by an exact string match when removing multiple members. The order is important. If this command results in all members being removed, the zone alias is deleted. The following example shows the **aliRemove** command.

```
admin> aliRemove “array1”, “21:00:00:20:37:0c:71:d2”
```

aliShow

The **aliShow** command prints the specified zone alias definition if a parameter is given; otherwise, all zone configuration information is printed. The following example shows the **aliShow** command.

```
admin> aliShow
Defined configuration:
 cfg:   USA_cfg Red_zone; Blue_zone
 zone:  Blue_zone
                0,1; array1; 0,2; array2
 zone:  Red_zone
                0,0; loop1
 alias: array1  21:00:00:20:37:0c:76:8c; 21:00:00:20:37:0c:71:02
 alias: array2  21:00:00:20:37:0c:66:23; 21:00:00:20:37:0c:73:7f
 alias: loop1   21:00:00:20:37:0c:76:85; 21:00:00:20:37:0c:71:df
```

Zone configuration commands

Zone configuration commands let you manipulate the zone configurations.

cfgAdd

The **cfgAdd** command adds one or more new cfg members to an existing zone configuration. `cfg_members` is a list of one or more zone names separated by semicolons. White space is ignored. The following example shows the **cfgAdd** command.

```
admin> cfgAdd “USA_cfg”, “Green_zone”
```

cfgCreate

The **cfgCreate** command creates a new zone configuration. The `cfg name` is a C-style name for this zone configuration and cannot already be used for any other zone object. `cfg_members` is a list of one or more zone names separated by semicolons. White space is ignored. The following example shows the **cfgCreate** command.

```
admin> cfgCreate "USA_cfg", "Red_zone; Blue_zone; Green_zone"
```

cfgDelete

The **cfgDelete** command deletes an existing zone configuration. The following example shows the **cfgDelete** command.

```
admin> cfgDelete "USA_cfg"
```

cfgRemove

The **cfgRemove** command removes one or more cfg_members from an existing zone configuration. The members to be removed are found by an exact string match when removing multiple members. The order is important. If this command results in all members being removed, the zone configuration is deleted. The following example shows the **cfgRemove** command.

```
"USA_cfg", "Green_zone"
```

cfgShow

The **cfgShow** command prints the specified zone configuration definition if a parameter is given, otherwise all zone configuration information is printed. The following example shows the **cfgShow** command.

```
admin> cfgShow
Defined configuration:
 cfg:   USA_cfg Red_zone; Blue_zone; Green_zone
 zone:  Blue_zone
                0,1; array1; 0,2; array2
 zone:  Red_zone
                0,0; loop1
 alias: array1  21:00:00:20:37:0c:76:8c; 21:00:00:20:37:0c:71:02
 alias: array2  21:00:00:20:37:0c:76:22; 21:00:00:20:37:0c:76:28
 alias: loop1   21:00:00:20:37:0c:76:85; 21:00:00:20:37:0c:71:df

Effective configuration:
 cfg:   USA_cfg
 zone:  Blue_zone
                0,1
                21:00:00:20:37:0c:76:8c
                21:00:00:20:37:0c:71:02
                0,2
                21:00:00:20:37:0c:76:22
                21:00:00:20:37:0c:76:28
 zone:  Red_zone
                0,0
```

Zone commands

Zone commands let you manipulate the zones within a fabric.

zoneAdd

The **zoneAdd** command adds one or more new `zone members` to an existing zone. zone_members is a list of one or more physical fabric port numbers (for example: `1,2`), world-wide name (for example, 10:00:00:60:69:00:00:8a), or zone alias names separated by semicolons. White space is ignored. The following example shows the **zoneAdd** command.

```
admin> zoneAdd “Blue_zone”, “array2; array3; array4; array5;”
```

zoneCreate

The **zoneCreate** command creates a new zone. The zone_name is a C-style name for the zone and cannot already be used for any other zone object. zone_members is a list of one or more physical fabric port numbers (for example: `1,2`), world-wide name (for example, 10:00:00:60:69:00:00:8a), or zone alias names separated by semicolons. White space is ignored. The following example shows the **zoneCreate** command.

```
admin> zoneCreate “Red_zone”, “0,0; loop1”
admin> zoneCreate “Blue_zone”, “0,1; array1; 0,2; array2”
admin> zoneCreate “Green_zone”, “0,0; loop1; 0,2; array2”
```

zoneDelete

The **zoneDelete** command deletes an existing zone. The following example shows the **zoneDelete** command.

```
admin> zoneDelete “Blue_zone”
```

zoneRemove

The **zoneRemove** command removes one or more zone members from an existing zone. The members to be removed are found by an exact string match when removing multiple members. The order is important. If this command results in all members being removed, the zone is deleted. The following example shows the **zoneRemove** command.

```
admin> zoneRemove “Blue_zone”, “array2”
```

zoneShow

The **zoneShow** command prints the specified zone definition if a parameter is given; otherwise, all zone configuration information is printed. The following example shows the **zoneShow** command.

```
admin> zoneShow
Defined configuration:
 cfg:   USA_cfg Red_zone; Blue_zone; Green_zone
 zone:  Blue_zone
                0,1; array1; 0,2; array2
 zone:  Red_zone
                0,0; loop1
 alias: array1  21:00:00:20:37:0c:76:8c; 21:00:00:20:37:0c:71:02
 alias: array2  21:00:00:20:37:0c:76:22; 21:00:00:20:37:0c:76:28
 alias: loop1   21:00:00:20:37:0c:76:85; 21:00:00:20:37:0c:71:df

Effective configuration:
 cfg:   USA_cfg
 zone:  Blue_zone
                0,1
                21:00:00:20:37:0c:76:8c
                21:00:00:20:37:0c:71:02
                0,2
                21:00:00:20:37:0c:76:22
                21:00:00:20:37:0c:76:28
 zone:  Red_zone
                0,0
                21:00:00:20:37:0c:76:85
                21:00:00:20:37:0c:71:df
```

Configuration management commands

Configuration management commands let you configure the zones.

cfgClear

The **cfgClear** command removes all zone information from the fabric.

If a zone configuration is enabled, it is first disabled. All defined zone objects are deleted. However, the saved configuration remains in flash memory. The following example shows the **cfgClear** command.

```
admin> cfgClear
```

To clear the configuration from memory, type **cfgSave** after **cfgClear**.

cfgDisable

The **cfgDisable** command disables the current zone configuration. The fabric returns to nonzoning mode where all devices see each other.The following example shows the **cfgDisable** command

```
admin> cfgDisable “USA_cfg”
```

cfgEnable

The **cfgEnable** command enables the zone configuration. The specified zone configuration is compiled by checking for undefined zone names, zone alias names, or other inconsistencies. This is done by expanding zone aliases, removing duplicate entries, and building the effective configuration. If the compilation fails, the previous state is unchanged (zoning is disabled if it was previously disabled or the previous effective configuration remains in effect). If the compilation succeeds, the previous effective configuration is disabled and this new configuration is enabled. The following example shows the **cfgEnable** command.

```
admin> cfgEnable “USA_cfg”
zone config “USA_cfg” is in effect
```

cfgSave

The **cfgSave** command writes a copy of the defined configuration plus the name of the effective configuration to flash memory in all fabric switches. The saved configuration is automatically reloaded by the switch during start up and, if a configuration was in effect when it was saved, the same configuration is reinstated with an automatic **cfgEnable** command. The following example shows the **cfgSave** command.

```
admin> cfgSave
Updating flash ...
```

cfgShow

The **cfgShow** command prints the output of the specified zone configuration definition if a parameter is given; otherwise, all zone configuration information is printed. The following example shows the **cfgShow** command.

```
admin> cfgShow
Defined configuration:
 cfg:   USA1    Blue_zone
 cfg:   USA_cfg Red_zone; Blue_zone
 zone:  Blue_zone
                0,1; array1; 0,2; array2
 zone:  Red_zone
                0,0; loop1
 alias: array1  21:00:00:20:37:0c:76:8c; 21:00:00:20:37:0c:71:02
 alias: array2  21:00:00:20:37:0c:76:22; 21:00:00:20:37:0c:76:28
 alias: loop1   21:00:00:20:37:0c:76:85; 21:00:00:20:37:0c:71:df

Effective configuration:
 cfg:   USA_cfg
 zone:  Blue_zone
                0,1
                21:00:00:20:37:0c:76:8c
                21:00:00:20:37:0c:71:02
                0,2
                21:00:00:20:37:0c:76:22
                21:00:00:20:37:0c:76:28
 zone:  Red_zone
                0,0
```

Chapter 6. QuickLoop

Note: Throughout this book, the term *switch* applies to both switches and hubs unless otherwise noted.

The QuickLoop feature supports legacy devices. The legacy devices refer to devices that are in a private loop direct attach (PLDA) environment. The QuickLoop feature allows these devices to be attached to a storage area network (SAN) and to operate no differently than in a PLDA environment.

For a list of supported devices, see the Web site at:

www.ibm.com/storage/fchub/

Features

The QuickLoop has the following features:

- A maximum of 126 devices can be supported within a loop created by the QuickLoop function.
- The QuickLoop conforms to fibre-channel standards.
- Ports (looplets) of up to two switches in a fabric can be included in a loop.
- Each looplet supports transfer rates of 100 MBps and multiple devices can communicate simultaneously in different looplets.
- A fabric can have several loops, but any one switch can only be in one loop.
- Public hosts that support an arbitrated loop being attached to a loop port are treated as private devices. For example, their FLOGI is rejected.
- Hosts attached to ports with the QuickLoop can communicate to all devices attached to ports provided by the QuickLoop.
- Other public hosts can also communicate with devices attached to the QuickLoop ports.
- Individual looplets can be taken out of service manually or automatically, if a looplet error is detected. The looplet is reinstated when the error condition is cleared.
- QuickLoop port management is achieved using the Telnet interface or the StorWatch fibre-channel switch expert.

User interfaces

There are three methods to manage the QuickLoop: Telnet commands, the front panel, or the StorWatch Specialist.

Telnet Commands

The Telnet shell has three commands:

- **qlPartner** command: Specifies the world-wide name (WWN) of the partner switch of a dual-switch loop.
- **qlShow** command: Lists QuickLoop information.
- **qlHelp** command: Lists QuickLoop help information.

Note: The QuickLoop is enabled through Telnet or the StorWatch Specialist and is maintained after a power on and off cycle or is disabled using Telnet.

QuickLoop configurations

Two basic configurations are supported:

- Single-switch: All looplets of a QuickLoop reside in one switch.
- Dual-switch: Looplets of a QuickLoop span across two cascaded hubs.

Both configurations allow up to 126 NL_port devices in one QuickLoop.

In a mixed loop and SAN configuration, fabric devices (public) can access loop devices (private), but not vice versa. There can be multiple loops within a SAN and each can be either single-switch or dual-switch. However, devices in two different loops cannot communicate with each other.

Sample configurations

Note: The switch shown in Figure 39 on page 105 and the switches shown in Figure 40 on page 106 are examples of switches operating in QuickLoop mode and might not be representative of your product. These figures show possible loop configurations. In each example, the connected lines represent the logical loop or the ports that form the loop.

Figure 39 on page 105 shows a high-performance multitarget connectivity to a single logical PLDA where the entire switch operates in QuickLoop mode. The switch serves as a concentrator, similar to a hub. However, a switch offers throughput performance on each looplet of 100 MBps.

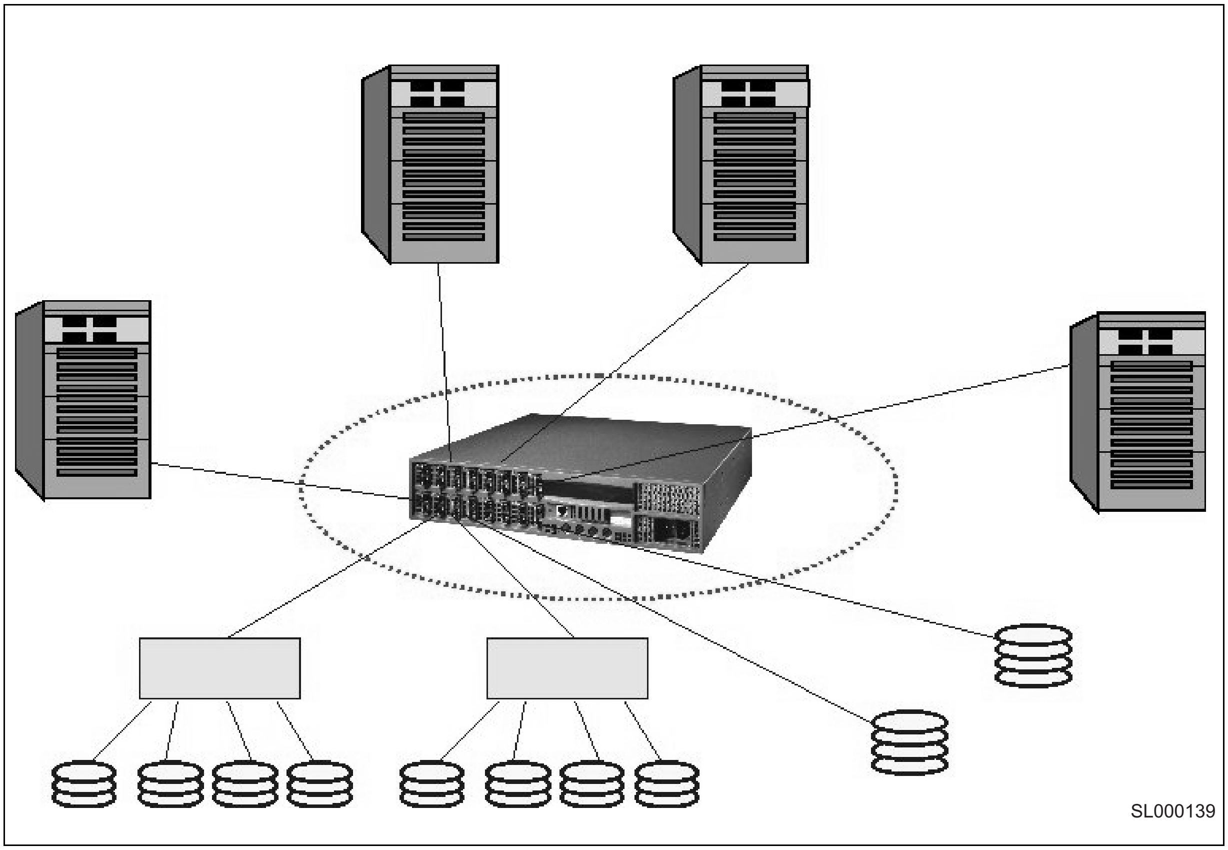


Figure 39. QuickLoop configuration showing a single switch

Figure 40 shows a longwave laser connected by cascading two switches in a single logical PLDA where two switches operate in QuickLoop mode. The switches are used to interconnect devices of up to 10 km (6.2 mi).

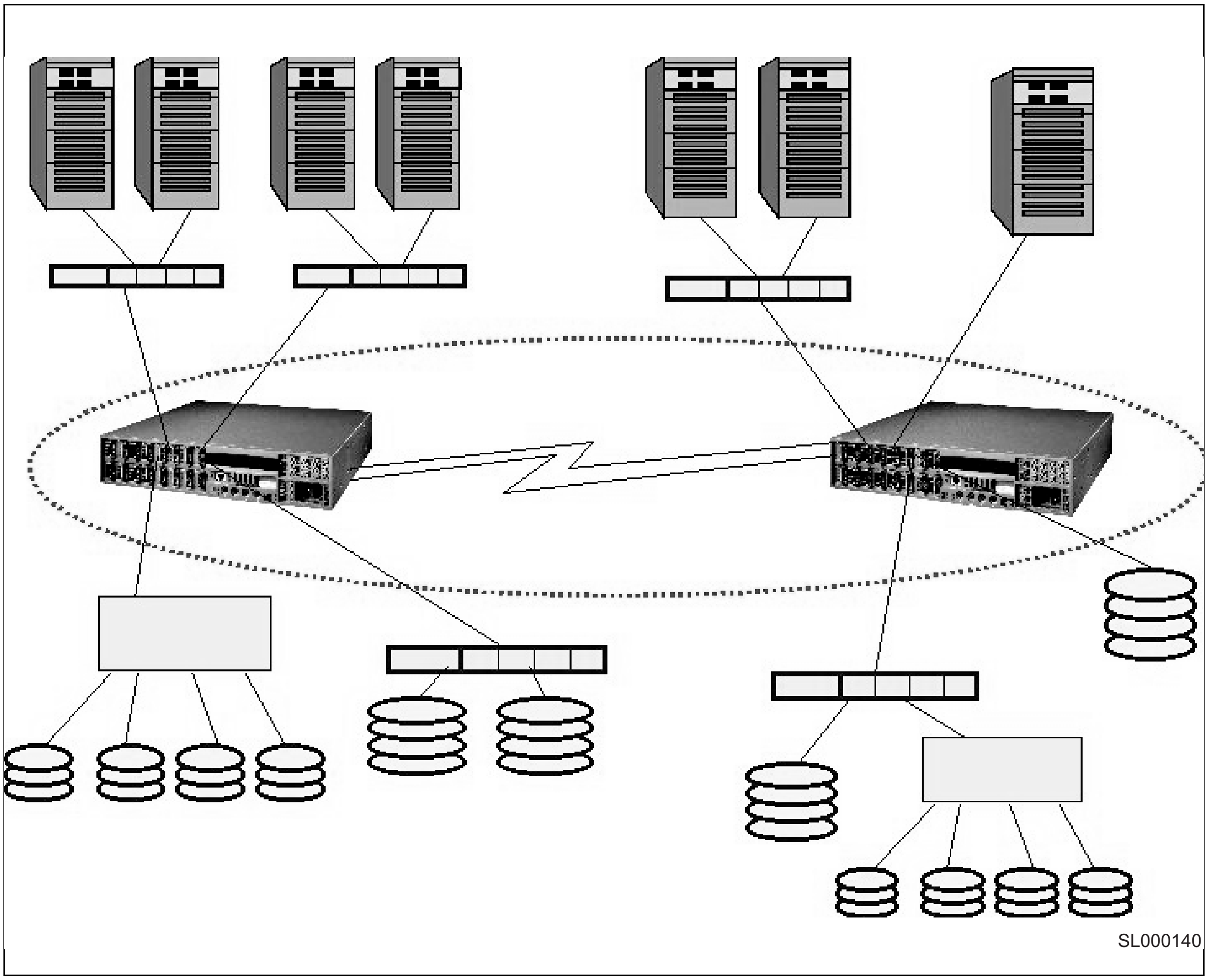


Figure 40. QuickLoop configuration showing two switches

QuickLoop commands

Following is a description of the QuickLoop commands that are run using Telnet.

qlPartner

The **qlPartner** command prints and sets the QuickLoop partner. For a dual-switch QuickLoop, you must issue the command on both switches, by including the world-wide name (WWN) of the remote switch. To set QuickLoop in single-switch mode, include a zero with the command.

The following example shows the **qlPartner** command.

```
admin> qlPartner 0
Setting QuickLoop to single-switch mode,
Committing configuration...done.

admin> qlPartner
QuickLoop is in single-switch mode, partner is not specified.

admin> qlPartner "10:00:00:60:69:10:02:0d"
Setting QuickLoop to dual-switch mode,
Committing configuration..done.

admin> qlPartner
QuickLoop is in dual-switch mode, partner is 10:00:00:60:69:10:02:0d.
```

qlShow

The **qlshow** command shows the current QuickLoop configuration. In the following example, QuickLoop is in the dual-switch QuickLoop mode.

```
admin> qlshow
Self: 10:00:00:60:69:30:05:0d domain 1
Peer: 10:00:00:60:69:30:05:22 domain 2
State: Master
Scope: dual
AL_PA bitmap: 10000000 00000000 00000000 00000003
Remote AL_PAs
       [021000]: e8
       [021100]: ef
       [021200]: 02
Local AL_PAs
       [011300]: 01
Local looplet states
       Member: 0 1 2 3 4 6 7
       Online: - - - 3 - - -
       Looplet 0: offline
       Looplet 1: offline
       Looplet 2: bypassed
       Looplet 3: online
       Looplet 4: offline
       Looplet 6: offline
       Looplet 7: offline
```

The following describes the **qlShow** command fields:

Self The local switch WWN and domain number.

Peer The remote switch with its WWN and domain number, if QuickLoop is in dual-switch mode.

State Indicates whether the local switch is the master or nonmaster.

Scope Indicates the QuickLoop mode as dual or single switch.

AL_PA bitmap
All AL_PAs in the entire QuickLoop.

Remote AL_PAs
The looplets and devices that are in QuickLoop mode on the remote switch.

Local AL_PAs
The looplets and devices that are in QuickLoop mode on the local switch.

Local looplet states
The looplets, member (switch ports), online (QuickLoop ports), looplet status (port).

Using the StorWatch Specialist

The StorWatch Specialist is used to view QuickLoop configuration information and set the QuickLoop partner hub or switch. See Figure 41.

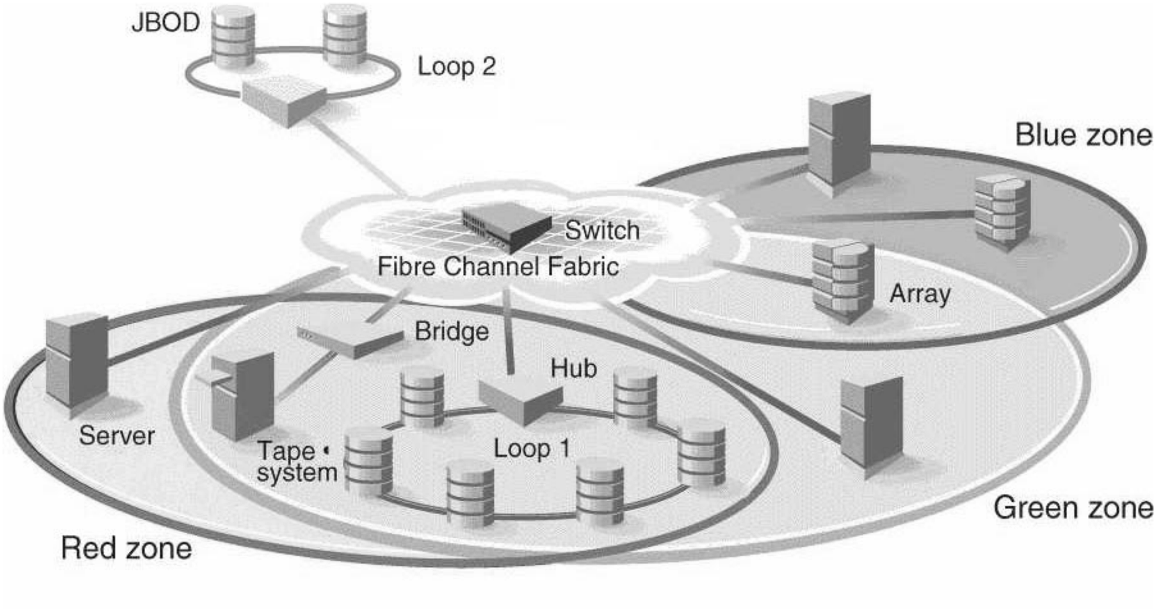


Figure 41. QuickLoop configuration view

Note: QuickLoop commands are available only in the 2109 Switch or an IBM 3534 SAN Fibre Channel Managed Hub with LoopSwitch and QuickLoop Fibre Channel installed.

Fault isolation

Fault isolation is very important in a loop, considering that the loop can consist of multiple looplets across multiple hubs (up to two). The goal is to minimize the impact of a faulty looplet or switch on the normal loop functions.

Hub level

In a dual-hub loop, the following conditions indicate that the partner switch is not functioning properly:

- No hub with the configured partner switch WWN is found in the fabric.
- No response is received from the partner hub during the initial handshake.
- An inconsistent response is received from the partner hub.
- A response not received in time during loop initialization.

Once it is determined that a switch is not functioning properly, it is skipped from loop initialization.

Port level

A 3534 Managed Hub U_port (universal port) is a port in an uninitialized state. Once initialized, the 3534 Managed Hub U_port becomes either an L_port (loop port) or E_port (expansion port).

Note: There is only one E_port per 3534 Managed Hub.

The following conditions are considered faulty in regards to the related looplet:

- A U_Port fails to become the loop initialization master (of the local looplet) within a time limit after LIPs are received from or sent to the port.
- A loop initialization sequence is not received back by a U_Port within a time limit after the same sequence is sent.
- The frequency of LIPs received from a U_port exceeds a threshold.
- Physical level errors, for example, loss of sync, laser fault, and so on.

Once a looplet is determined faulty, it is not included in loop initialization.

Chapter 7. QuickLoop Zoning

Note: Throughout this book, the term *switch* applies to both switches and hubs unless otherwise noted.

Switch code level 2.1.3. now supports zoning with QuickLoop. QuickLoops can be zoned for switches.

QuickLoop zoning allows you to do the following:

- Segment a QuickLoop into independent QuickLoops. You can use QuickLoop zoning to build multiple QuickLoops within a single switch or QuickLoop switch pair.
- Limit the scope of the QuickLoop initialization procedure (LIP) propagation to only those looplets in the same zone. A *looplet* refers to the devices attached to a single switch port. QuickLoop zoning ensures that LIPs do not affect operation on unrelated looplets.
- Zone QuickLoops by port or by an arbitrated QuickLoop physical address (AL_PA). Loop zone members cannot be specified by device world-wide names (WWNs).

QuickLoop zoning limitations include the following:

- AL_PA zoning can only be used on a single QuickLoop on the fabric. Only one QuickLoop can be configured on a fabric.
- QuickLoop zoning allows you to create separate, independent, QuickLoops within a QuickLoop, however, there is a single AL_PA address space within a single QuickLoop. Devices with hard AL_PAs must have unique AL_PAs within a QuickLoop.
- All QuickLoop zone members must be attached to a QuickLoop port. For example, QuickLoop 2.1.3 does not support public devices on fabric ports within a QuickLoop zone. Zones that do not contain AL_PAs whose members are defined by ports and WWNs can include public devices and private targets on a QuickLoop.
- If you enable QuickLoop zoning by defining an AL_PA list, all switches must be v2.1.3 or the fabric will segment.
- If WWNs are used for zoning, the QuickLoop devices do not have to be explicitly zoned. You can use WWN to zone the public devices without creating a zone for the QuickLoop (that is, the QuickLoop continues to operate).
- If hard zoning (domain, port) is used to zone the public devices, the QuickLoop devices must also be zoned using hard zoning.

See Table 11 for zoning rules.

Table 11. Zoning rules

Type of zone	AL_PA	Port	WWN
Public zoning	No	Yes	Yes
QuickLoop zoning	Yes	Yes	No

Using QuickLoop zones

In addition to zoning fabrics, zoning also allows you to zone QuickLoops. By partitioning selected devices within a QuickLoop into a QuickLoop zone you can enhance management of a Fibre Channel Arbitrated Loop (FC-AL) in a legacy environment.

In QuickLoop zoning, devices within a QuickLoop can be partitioned within that QuickLoop to form QuickLoop zones. In other words, a QuickLoop zone is a subset of a QuickLoop and can include only QuickLoop devices.

QuickLoop zoning advantages

In addition to all the advantages of fabric zoning (security, customization of environments, and optimization of IT resources) QuickLoop zoning can protect devices from disruption by unrelated devices during a critical process, for example, during a tape backup session.

In a QuickLoop with zoning enabled, transmission of the loop initialization primitive (LIP) signal and loop initialization are controlled by the switch. The LIP is transmitted only to looplets within the affected zone; other looplets on the QuickLoop are not affected. In this way, unwanted disruption to devices can be controlled.

QuickLoop zones

QuickLoop zones are hardware enforced; switch hardware prevents unauthorized data transfer between ports within the zone, allowing devices to be partitioned into zones to restrict system access to selected devices. Once devices are included in a zone, they are visible only to other devices within that zone.

QuickLoop zone members are designated by looplet (port number), or by arbitrated loop physical address (AL_PA). There are 126 unique AL_PAs per QuickLoop; therefore, a QuickLoop zone can contain no more than 126 devices.

Configuring QuickLoop zones

To configure QuickLoop zoning, perform the following steps:

1. Create a QuickLoop.

   A QuickLoop is comprised of FL_ports on one or two switches within the fabric. To create a QuickLoop, specify a QuickLoop name (referred to as a *qloop name* for zoning), followed by a list of AL_PAs to be included. QuickLoop names define the switch (or pair of switches) that make up the QuickLoop.

   A QuickLoop name must be a unique alphanumeric string beginning with an alpha character. The underscore character (_) is allowed and names are case sensitive. For example, Qloop1 is not the same name as qloop1.

2. Define the QuickLoop zone.

   A QuickLoop zone is a group of FL_ports or AL_PAs that can communicate with each other. These ports and AL_PAs must reside within the same QuickLoop. In a QuickLoop zone, every member must be either a looplet (FL_port) or an AL_PA within a single QuickLoop. QuickLoop zones can overlap looplets, but they must be confined to a single QuickLoop. QuickLoop zones are hardware enforced, but zones within a single looplet are not enforceable; therefore it is recommended that you do not partition devices within a looplet into different zones.

   To define a QuickLoop zone, specify the list of members to be included and assign a unique zone name. A QuickLoop zone name must be a unique alphanumeric string beginning with an alpha character. The underscore character (_) is allowed and zone names are case sensitive. For example, Zone1 is not the same name as zone1. To create a QuickLoop zone, specify QuickLoop zone members by looplet, by AL_PA, or by combination of the two.

   To specify by looplet, specify the QuickLoop zone name in quotation marks, and then the physical ports to be included in quotation marks. For example:

```
“QLZoneName”, “0,0; 0,1; 2,6; 2.7; 2,8”
```

   To specify zone members by AL_PA, specify the QuickLoop zone name in quotation marks, and then the QuickLoop name and desired AL_PAs in quotation marks. All AL_PAs must be associated with a QuickLoop name. For example:

```
“QLZoneName”, “qloop1[01,02,04,e0,e1,e2]”
```

   A combination of looplet and AL_PA can be specified. For example:

```
“QLZoneName”, “0,2; 0,3; qloop1[ca,cb,e1,e2]
```

3. Define the QuickLoop zone configuration.

   A QuickLoop zone configuration is a group of QuickLoop zones that are enforced whenever that zone configuration is enabled.

   To define a QuickLoop zone configuration, assign a zone configuration name and specify the QuickLoop zone names to be included. The QuickLoop names of the QuickLoop zones must also be included in the zone configuration. A QuickLoop zone configuration name must be a unique alphanumeric string beginning with an alpha character. The underscore character (_) is allowed and zone configuration names are case sensitive. For example, QLConfig_1 is not the same name as qlconfig_1.

4. Enable the QuickLoop zone configuration.

   To enable a QuickLoop zone configuration, select the configuration to be enabled.

QuickLoop zones using ports

A QuickLoop zone limits the scope of LIP propagation and QuickLoop initialization. This limitation is determined for each LIP occurrence, and the source of the LIP. An LIP is sent to the smallest number of looplets possible.

Figure 42 on page 115 defines three QuickLoop zones. The notation used is:

```
<switch #, port #>
```

- qlZone1 includes ports 0,0 and 0,1.
- qlZone2 includes ports 0,2, 0,3, and 0,4.
- qlZone3 includes ports 0,4, and 0,5.

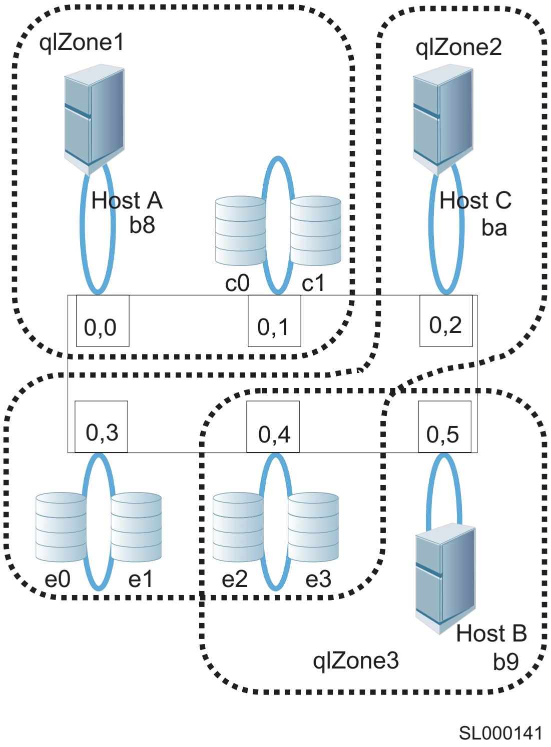


Figure 42. Port-based zoning

In this example, qlZone2 and qlZone3 have overlapping zone members (0,4). qlZone1 is an exclusive zone, and its ports are exclusively in a single zone.

- Host A receives the map of devices that are associated with ports 0,0 and 0,1; that is, AL_PA [b8, c0, c1]. The map is used to indicate those devices that are part of the QuickLoop.
- Host C receives the map of devices that are associated with ports 0,2, 0,3, and 0,4; that is, AL_PA [ba, e0, e1, e2, e3].
- Host B receives the map of devices that are associated with ports 0,4 and 0,5; that is, AL_PA [b9, e2, e3].
- LIPs initiated within qlZone1 are only propagated to ports 0,0 and 0,1.
- LIPs initiated within qlZone2 or qlZone3 are propagated to ports 0,2, 0,3, 0,4, and 0,5, which is the union of all ports in common zones.

Whenever a zone is changed or reconfigured, an LIP is generated to all affected looplets to indicate the configuration change.

Configuring a QuickLoop zone uses the same interfaces (Telnet or StorWatch Specialist) as are used for standard zones. However,

- Only switch ports can be used. QuickLoop zones cannot be configured with WWNs.

- The selected ports must all be in the corresponding switches (single switch or QuickLoop switch pair) comprising the QuickLoop.
- Only QuickLoop ports can be configured. If fabric ports are included, it is not a QuickLoop zone.

Arbitrated loop physical address (AL_PA) zoning

AL_PA zoning allows zone members to be designated by their arbitrated loop physical addresses and is typically used for devices with hard AL_PAs. AL_PA zoning is convenient in that zoning is still effective if the connection to the switch is changed from one port to another port. However, it can be more complex to manage.

Specifying an AL_PA indirectly causes an LIP to be received on all devices contained within the corresponding looplet. For example, if you configure qlZone4 to include AL_PAs [b9, e3] as shown in Figure 42 on page 115, the device with AL_PA e2 also receives the LIP because it is on the same looplet as device e3. However, the map returned to host C is [b9, e3], and the host is unable to send frames to device e2.

Creating zones

Use Telnet commands or the StorWatch Specialist to create a QuickLoop zone with AL_PA components.

Some examples of creating a QuickLoop zone using the **zoneCreate** command follow.

- Create a zone to include multiple AL_PAs as a list in square brackets:

```
zoneCreate “qlzone3”, “[b9,e2]”
```

- Zones can include both ports and AL_PA components. Separate the components by a semicolon:

```
zoneCreate “qlzone3”, “0,1; [80]”
```

- An AL_PA list can be specified, in which case all AL_PAs in the list will be included:

```
zoneCreate “qlzone3”, “0,1;[80,81,82,84,88]”
```

- AL_PAs can also be included in alias definitions.

```
aliCreate “host_group1”, “[80,81,82,84,88]”
```

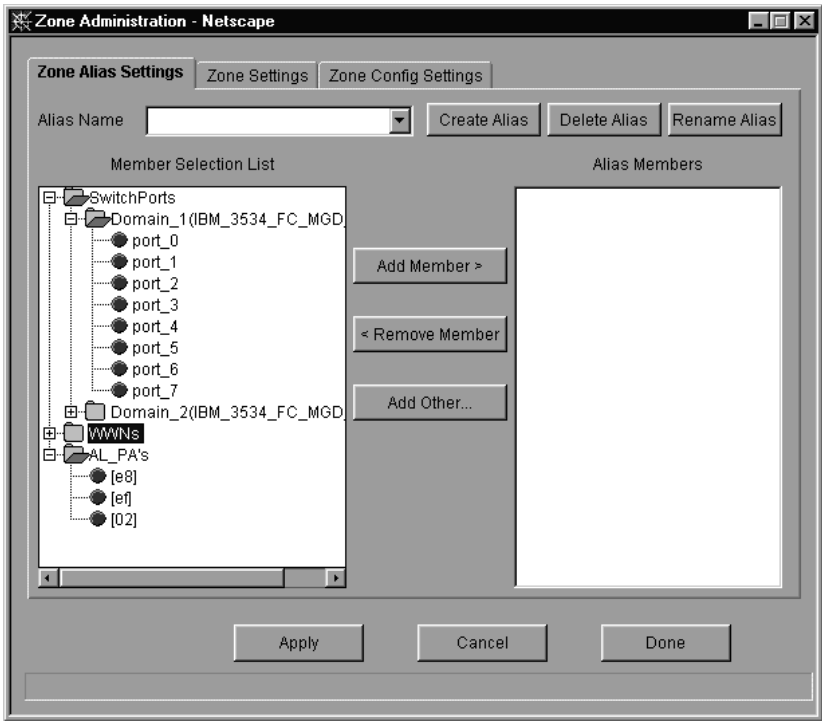
The following example contains a listing of valid AL_PAs.

```
0x00, 0x01, 0x02, 0x04, 0x08, 0x0f,
0x10, 0x17, 0x18, 0x1b, 0x1d, 0x1e, 0x1f,
0x23, 0x25, 0x26, 0x27, 0x29, 0x2a, 0x2b, 0x2c, 0x2d, 0x2e,
0x31, 0x32, 0x33, 0x34, 0x35, 0x36, 0x39, 0x3a, 0x3c,
0x43, 0x45, 0x46, 0x47, 0x49, 0x4a, 0x4b, 0x4c, 0x4d, 0x4e,
0x51, 0x52, 0x53, 0x54, 0x55, 0x56, 0x59, 0x5a, 0x5c,
0x63, 0x65, 0x66, 0x67, 0x69, 0x6a, 0x6b, 0x6c, 0x6d, 0x6e,
0x71, 0x72, 0x73, 0x74, 0x75, 0x76, 0x79, 0x7a, 0x7c,
0x80, 0x81, 0x82, 0x84, 0x88, 0x8f,
0x90, 0x97, 0x98, 0x9b, 0x9d, 0x9e, 0x9f,
0xa3, 0xa5, 0xa6, 0xa7, 0xa9, 0xaa, 0xab, 0xac, 0xad, 0xae,
0xb1, 0xb2, 0xb3, 0xb4, 0xb5, 0xb6, 0xb9, 0xba, 0xbc,
0xc3, 0xc5, 0xc6, 0xc7, 0xc9, 0xca, 0xcb, 0xcc, 0xcd, 0xce,
0xd1, 0xd2, 0xd3, 0xd4, 0xd5, 0xd6, 0xd9, 0xda, 0xdc,
0xe0, 0xe1, 0xe2, 0xe4, 0xe8, 0xef
```

To create a QuickLoop zone using StorWatch Specialist, do the following:

- AL_PA selection: StorWatch Specialist 2.1.3 includes AL_PAs in the **Member Selection List** in the Zone Administration panel as shown in Figure 43 on page 118. You can select the required AL_PAs in the zone from the appropriate list.

- You can also use the **Add Other** button to manually enter the AL_PAs necessary for zone configuration. The syntax is identical to that of Telnet; that is a list of AL_PAs, enclosed in square brackets and separated by commas.



SL000142

Figure 43. Zone Administration view

Chapter 8. Managing the 3534 Managed Hub with SNMP

Note: Throughout this book, the term *switch* applies to both switches and hubs unless otherwise noted.

The resident SNMP agent allows remote management of the 3534 Managed Hub using IP over Ethernet and fibre-channel interfaces.

This section provides an overview of key concepts about switch and hub management based on simple network management protocol (SNMP).

Within the SNMP model, a manageable network consists of one or more manager systems (or network management stations), and a collection of agent systems (or network elements):

- A manager system runs a management application that monitors and controls the network elements.
- An agent system is a network device such as a fibre-channel switch, a hub, or a bridge, that has an agent responsible for carrying out operations requested by the manager. Therefore, an agent is the interface to a managed device.

The manager communicates with an agent using the SNMP. The switch agent supports both SNMP version 1 (SNMPv1) and community-based SNMP version 2 (SNMPv2C). SNMP allows the following management activities:

- A manager can retrieve management information, such as its identification, from an agent. There are three operations for this activity:
  - SNMP-GET
  - SNMP-NEXT
  - SNMP-BULKGET (SNMPv2C)
- A manager can change management information on the agent. The operation for this activity is SNMP-SET.
- An agent can send information to the manager without being explicitly polled for. This operation is termed a *trap* in SNMPv1 or a *notification* in SNMPv2C. Traps or notifications alert the manager to events that occur on the agent system, such as a restart. For the rest of this chapter, the term *trap* is used.

The information about an agent is known as the management information base (MIB). It is an abstraction of configuration and status information. A specific type or class of management information is known as an MIB object or variable. For example, the MIB variable *`sysDescr`* defines the description of an agent system. The existence of a particular value for an MIB object in the agent system is known as an MIB object instance, or simply an instance. Some MIB objects have only a single instance for a given agent system. For example, the system description and the instance is denoted as `sysDescr.0`. Other MIB objects have multiple instances. For example, the operational status of each fibre-channel port on a switch and a particular instance can be denoted as: `swFCPortOperStatus.5”`

MIB objects are conceptually organized in a hierarchical tree structure. Each branch in the tree has a unique name and numeric identifier. Intermediate branches of the tree serve as a way to group related MIB objects together. The *leaves* of the tree represent the actual MIB objects. Figure 44 shows the tree structure, with special attention to the Internet MIB tree and the fibre-channel MIB tree.

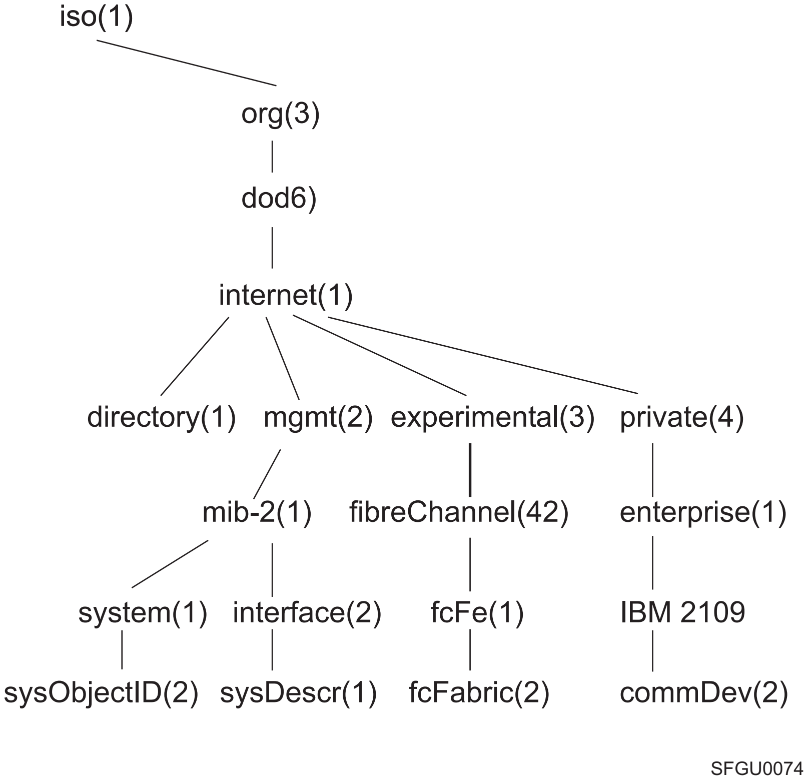


Figure 44. MIB tree

An MIB object is therefore uniquely identified or named by its position in the tree. A full object identifier consists of the identifier of each branch along the path through the tree. For example, the object `sysObjectID` has the full identifier of `1.3.6.1.2.1.1.2.` For readability, notation can be used, for example `{system 1}.`

The agent of the switch supports the following:

- SNMPv1 and SNMPv2c
- Command-line utilities to provide access to configure the agent
- MIB-II system group, interface group, and SNMP group
- Fabric element MIB
- Vendor specific MIBs
- Standard generic traps
- Enterprise specific traps

SNMP transports

The SNMP agent that resides on the embedded processor supports UDP/IP over the Ethernet interface (see Figure 44 on page 120). This transport provides an immediate plug-and-play support for the switch, once the IP address has been assigned.

MIB-II support

There are 11 groups of objects specified in MIB-II. The SNMP agent of the switch supports three of these groups. The eight additional groups do not apply.

The three groups supported include:

- System group (object ID is {iso, org, dod, internet, mgmt, mib-2, 1})
- Interfaces group (object ID is {iso, org, dod, internet, mgmt, mib-2, 2})
- SNMP group (object ID is {iso, org, dod, internet, mgmt, mib-2, 11})

The following variables are modifiable using the SNMP **set** command, given an appropriate community with read-write access:

sysDescr
This variable notifies the system that this is a managed hub.

```
IBM_3534_FC_mgdhub
```

sysObjectID
System object identifier vendor’s authoritative identification `(1.3.6.1.4.1.1588.2.1.1.1).`

sysUpTime
The time since the agent was last initialized

sysContact
The identification and contact information for this switch. The default setting is `Field Support`.

sysLocation
The physical location of the switch. The default setting is `End User Premise`.

The interface group supports three interface drivers: software loopback, Ethernet, and fibre-channel IP.

Fabric element MIB support

There are five object groups defined:

- Configuration group
- Operation group

- Error group
- Accounting group
- Capability group

The agent supports all groups, except the Accounting group, which is better supported in the fibre-channel port group of the vendor-unique MIB.

Vendor-unique MIB

Five groups of MIBs are defined and supported:

- Switch system group
- Fabric group
- SNMP agent configuration group
- Fibre-channel port group
- Name server group

Generic traps

Setting up the SNMP connection of the switch to an existing managed network allows the network system administrator to receive the following generic traps:

coldStart
This trap indicates that the agent has reinitialized itself such that the configuration of the agent might be altered. This also indicates that the switch has restarted.

linkDown
This trap indicates that an IP interface (Ethernet, loopback, or embedded N_port) has gone down and is not available.

linkUp This trap indicates that an IP interface (Ethernet, loopback, or embedded N_port) has become available.

Note: linkUp and linkDown traps are not associated with removing or adding an Ethernet cable. This is strictly a driver indication that the interface is configured, operational, and available and does not necessarily mean that the physical network cable is affected.

authenticationFailure
This trap indicates that the agent has received a protocol message that is not properly authenticated. By default, this trap is disabled but can be enabled using the **agtcfgSet**, **MIB-II support**, or **snmpEnableAnotherTrap** commands. The latter two commands are StorWatch commands and are not listed in this book.

Enterprise specific traps

The following enterprise-specific traps are supported:

swFault This trap indicates that the diagnostics detect a fault with the switch.

swSensorScn
This trap indicates that an environment sensor changed its operational state. For example, a fan stops working. The VarBind in the Trap Data Unit contains the corresponding instance of the sensor status.

swFCPortScn
This trap is a notification that a fibre-channel port has changed its operational state. For instance, the fibre-channel port goes from online to offline. The VarBind in the Trap Data Unit contains the corresponding instance of the operational status of the port.

Note: SNMP swFCPortScn traps are generated on GBIC insertion and removal even though the state remains offline.

swEventTrap
This trap is a notification that an event has occurred and its event severity level is at or below the value set in the variable, *swEventTrapLevel* (see “Agent configuration”). The VarBind in the Trap Data Unit contains the corresponding instance of the event index, time information, event severity level, the repeat count, and description.

The parameters can be configured using the SNMPv1 **set** command with an appropriate community. These parameters can also be configured using a Telnet connection, using the **agtcfgSet** command.

Agent configuration

The parameters that can be configured include:

- SNMPv1 communities (up to six)
- trap recipients (one per community)
- sysName
- sysContact
- sysLocation

authenticationFailure
This trap Indicates that the agent has received a protocol message that is not properly authenticated. This trap, by default, is disabled.

swEventTrap Level

This trap Indicates the swEventTrap severity level in conjunction with an event's severity level. When an event occurs and if its severity level is at or below the set value, the SNMP trap (swEventTrap) is sent to configured recipients. By default, this value is set at 0, implying that no swEventTrap is sent. Possible values are as follows:

0 – none

1 – critical

2 – error

3 – warning

4 – informational

5 – debug

See "errShow" on page 130 for more information about detected errors. See "Port error messages" on page 129 for more information about error messages.

These parameters can be changed using the **agtcfgSet** Telnet command, StorWatch Specialist, or SNMP.

Available MIB and trap files

You can download the MIB definitions and enterprise trap definitions.

1. From a Web browser, connect to the Web site at:

   www.ibm.com/storage/fchub/

2. Click on **firmware**. The following MIB files are displayed:
   - Fabric Element MIB definition file
   - Enterprises MIB definition file
   - Enterprise Specific Trap definitions

Note: The term port number is used to number the fibre-channel ports on a hub. The value is 0 - 7. In the various MIB definition files, there is the notion of port index, which by convention forbids the use of 0 as its value. For the hub, the port index for fibre-channel ports range from 1 - 8.

syslog daemon

A UNIX-style syslog daemon (syslogd) process is supported. Syslogd reads system events and forwards system messages to users or writes the events to log files, according to your system configuration.

System events are categorized by facility and severity. Refer to your UNIX documentation for a list of facilities and severity levels. The log process is used to log errors and system events on the local machine and are sent to a user or system administrator. The daemon is constantly running and is ready to receive messages from system processes. The events are logged according to the statements in the configuration file. In addition, syslogd is enabled to receive messages from a remote machine. Syslogd monitors UDP port 514 system events. A remote machine does not have to be running UNIX to forward messages to syslogd, but it must follow the basic syslog message format standard.

The first two items in the log are the date and time of the event (as known by the machine where syslogd is running) and the machine name that issued the error. This is the local machine, if the message is generated by a task running on the same machine as syslogd, or a remote machine, if the message was received on UDP port 514. The first two items are always present, all other entries are message specific.

Note: The log file can be located on a different machine and be remotely mounted. Therefore, a local error is an error that occurred where syslogd is running, not on the machine where the error log physically resides.

syslogd applications for Windows NT and Windows 95 are available at no charge on several FTP servers on the Internet.

syslogd support

Switch firmware maintains an internal log of all error messages. The log is implemented as a circular buffer, with a storage capability of 64 errors. After 64 errors have been logged, the next error message overwrites the messages at the beginning of the buffer.

If configured, the switch sends internal error messages to syslogd by sending a UDP packet to port 514 on the syslogd machine. This allows the storage of switch errors on a syslogd-capable machine and avoids the limitations of the circular buffer.

syslogd provides system error support using a single log file and can notify a system administrator in real time of error events. Additionally, the daemon provides dial-home capability.

Error message format

Each error message that is logged sends the following information:

- Error number (1 for the first error after start up, the number increments by one with each new error).
- The error message, exactly as it is stored in the error log (and printed using the **errShow** command).

The error message includes the switch that reported the error with the following event information:

- The ID of the task that generated the error.
- The name of the task that generated the error.
- The date and time when the error occurred, as seen by the switch. This can be different from the first item in the log file, which is the time as seen by the syslogd machine. These two time values are different if the clocks in the switch and in the syslogd machine are not in sync.
- The error identifier consisting of a module name, a dash, and an error name.
- The error severity.
- The optional informational.
- The optional stack trace.

Example:

syslogd running on switch sw9 is sending log events to the UNIX machine called *example*. The following is an example of a No memory error message that is generated by the shell. This is a severity 1 (LOG_CRITICAL) error. syslogd is configured to store the errors in the /var/adm/silkworm file.

```
example% egrep sw9 /var/adm/silkworm
Jul 11 16:48:25 sw9 1 0x103d8620 (tShell): Jul 11 16:48:19
Jul 11 16:48:25 sw9 Error SYS-NOMEM, 1, No memory
Jul 11 16:48:25 sw9 Traceback:
Jul 11 16:48:25 sw9 _tl+0x40 (0x103a2030)
Jul 11 16:48:25 sw9 _yystart+0x95c (0x1017128c)
Jul 11 16:48:25 sw9 _yyparse+0x694 (0x10172dc4)
Jul 11 16:48:25 sw9 _execute+0xdc (0x1014c06c)
Jul 11 16:48:25 sw9 _shellTask+0x964 (0x1003aea4)
Jul 11 16:48:25 sw9 _shellTask+0x198 (0x1003a6d8)
Jul 11 16:48:25 sw9 _vxTaskEntry+0x10 (0x10114d14)
Jul 11 16:48:25 sw9
```

Message classification

syslogd messages are classified according to facility and priority (severity code), thus allowing a system administrator to take different actions depending on the error. The action taken, based on the facility and priority of the message, is defined in the syslog configuration file. Example configurations are provided in “Switch configuration” on page 127 and “syslogd configuration” on page 128.

The switch uses the facility local7 for all error messages that are sent to the syslogd.

UNIX provides eight priorities, whereas the switch provides five severity codes (code LOG_PANIC [0] causes a restart and is not sent to the syslogd). The mapping between the severity codes of the switch and UNIX syslogd priorities is shown in Table 12 (in order of decreasing priorities).

Table 12. syslog message classification

Switch	**UNIX**
LOG_CRITICAL (1)	alert
LOG_ERROR (2)	err
LOG_WARNING (3)	warning
LOG_INFO (4)	info
LOG_DEBUG (5)	debug

Switch configuration

To start the syslogd, type the following command:

```
syslogdIp <IP address of the syslogd machine>
```

The command with no parameter prints the IP address of the current target syslogd machine. An IP address of `0.0.0.0` disables the forwarding of error messages to syslogd. In this case, error messages are still logged internally to the switch, but they are not forwarded to the syslogd.

Examples:

Enable and verify syslogd support:

```
=> syslogdIp “10.0.0.1”
=> syslogdIp
syslog daemon’s address: 10.0.0.1
```

Disable syslogd support:

```
=> syslogdIp “0.0.0.0”
=> syslogdIp
syslog daemon’s address: 0.0.0.0
```

syslogd configuration

The syslog configuration provides the syslogd with instructions for handling different messages. The following are example entries in a syslog configuration file (/etc/syslog.conf) for storing switch error messages that are stored in different files. See your UNIX documentation for a full description of the syslog configuration file.

The following entry in /etc/syslog.conf causes all messages from the silkworm of UNIX priority warning or higher (switch severity LOG_WARNING or higher) to be stored in the file /var/adm/silkworm.

```
local7.warning         /var/adm/silkworm
```

The following entries in /etc/syslog.conf causes the messages from the silkworm of UNIX priority alert (switch severity LOG_CRITICAL) to be stored in the file /var/adm/alert, and all other messages from the switch to be stored in the file /var/adm/silkworm.

```
local7.alert        /var/adm/alert
local7.debug        /var/adm/silkworm
```

The local7 prefix identifies the message from a switch. Note that usually a file must exist and have the proper permission in order for the syslogd to write to it.

Appendix A. Error messages

This appendix explains the error message format and possible errors. This section includes:

- Fan error message
- Port error messages
- Thermometer error message

The error messages are shown in bold font. Following the error message is the suggested action or actions to be taken.

Fan error message

Fan has stopped spinning
Check the fans inside the hub box.

Port error messages

The GBIC was removed from this port (solid black LED)
Check the hub front panel for GBIC.

Port is receiving no light (solid black LED)
There is no G_port board or no GBIC module for this port. Check the hub front panel.

Port is receiving light, but not yet online (solid amber LED)
A cable is partially inserted in the port, or the device at the other end of the cable is not functioning properly. Check the hub front panel or check the device on the other end of the cable.

Port is disabled (slow flashing amber LED)
The port was manually disabled by an administrator using the front panel or using one of the management tools.

Port has a fault (fast flashing amber LED)
One or more faulty conditions have occurred:

Laser_Flt
The LED is signaling a laser fault (defective GBIC or embedded optic)

Port_Flt
The port has been marked faulty (defective GBIC, embedded optic, cable, or device)

Diag_Flt
The port failed diagnostics (defective G_port card or system board)

Port is OK (solid green LED)
The port is online and connected to a device over the cable.

Port is segmented (slow flashing green LED)

Port is online but segmented. Check for loopback cable or incompatible hub.

Port has an internal loopback (fast flashing green LED)

The port is configured as a loopback port by diagnostics to verify the proper functioning of the internal fibre-channel port logic and paths between the interface and the central memory. portEnable will put the port back online again.

Port is sending data (flickering green LED)

The port is online and transmitting and receiving frames.

Thermometer error message

Temperature out of range

One or more temperature sensors have exceeded the minimum or maximum allowed temperature reading (Minimum temperature is 0°C [32°F], maximum is 75°C [167°F]). Check the temperature sensors inside the hub box.

Appendix B. Commands

Appendix B provides command descriptions and examples to help you manage and monitor the 3534 Managed Hub. Use these commands and settings to configure and operate the 3534 Managed Hub through the Telnet interface. The commands are listed in alphabetical order for easier reference.

agtcfgDefault

The **agtcfgDefault** command resets the configuration of the SNMP agent to the default values.

Syntax

```
agtcfgDefault
```

Availability

Administrator

Description

Use the **agtcfgDefault** command and the following variables to reset the configuration of the SNMP agent to default values:

sysDescr

The default value is Fibre Channel Switch.

sysLocation

The default value is End User Premise.

sysContact

The default value is Field Support.

swEventTrapLevel

The default value is 0 (off).

authTraps

The default value is 0 (off).

IP addresses

The trap recipient for each community defaults to 0.0.0.0 or no trap recipient.

- Community 1, Secret C0de: the default value is no trap recipient.
- Community 2, OrigEquipMfr: the default value is no trap recipient.
- Community 3, private: the default value is no trap recipient.
- Community 4, public: the default value is no trap recipient.

- Community 5, common: the default value is no trap recipient.
- Community 6, Fibre Channel: the default value is no trap recipient.

Note: For more information about these SNMP configuration parameters refer to the **agtcfgSet** command.

Operands

None

Example

In the following example, the **agtcfgDefault** command is run to set the SNMP agent configuration parameters to the default values. Then the **agtcfgShow** command is run again to verify that the default values are set.

```
sw5:admin> agtcfgDefault
Committing configuration...done.
agent configuration reset to factory default
sw5:admin> agtcfgShow
Current SNMP Agent Configuration
Customizable MIB-II system variables:
Committing configuration...done.
agent configuration reset to factory default
sw5:admin> agtcfgShow
Current SNMP Agent Configuration
Customizable MIB-II system variables:
        sysDescr = Fibre Channel Switch.
        sysLocation = End User Premise
        sysContact = Field Support.
swEventTrapLevel = 0
authTraps = 0 (OFF)
SNMPv1 community and trap recipient configuration:
Community 1: Secret C0de (rw)
   No trap recipient configured yet
Community 2: OrigEquipMfr (rw)
   No trap recipient configured yet
Community 3: private (rw)
   No trap recipient configured yet
Community 4: public (ro)
   No trap recipient configured yet
Community 5: common (ro)
   No trap recipient configured yet
Community 6: FibreChannel (ro)
   No trap recipient configured yet
sw5:admin>
```

See also

agtcfgSet
agtcfgShow

agtcfgSet

The **agtcfgSet** command modifies the configuration of the SNMP agent.

Syntax

```
agtcfgSet
```

Availability

Administrator

Description

Use this command to modify the configuration of the SNMP agent in the switch. Set the values for the following items:

sysDescr

Specify the switch description (in MIB-II definition). The default value is Fibre Channel Switch.

sysLocation

Specify the location of the switch (in MIB-II). The default value is End User Premise.

sysContact

Specify the contact information for this switch. The default value is Field Support.

swEventTrapLevel

Specify the event trap level in conjunction with an event severity level. When an event occurs, and if its severity level is at or below the set value (that is, more critical), the SNMP trap, swEventTrap, is sent to configured trap recipients. The default value is 0, which means that no swEventTrap is sent. The event trap levels are:

0	none
1	critical
2	error
3	warning
4	informational
5	debug

See the **errShow** command for more information.

authTrapsEnabled

Specify whether authorization traps are passed to the trap recipient. The default value is false (off), meaning no messages are sent. A value of true (on) means that authorization trap messages are sent to the community IP addresses. For SNMPv1 and SNMPv2c, this indicates that a request containing a community string is not known to the agent.

IP addresses

There are six communities, each with a respective trap recipient, supported by the agent. The first three communities are for read-write (rw) access and the last three are for read-only (ro) access. The trap recipient for each community defaults to 0.0.0.0 or no trap recipient.

Specify the IP address for each management station:

- Community 1, Secret C0de: the default value is 0.0.0.0.
- Community 2, OrigEquipMfr: the default value is 0.0.0.0.
- Community 3, private: the default value is 0.0.0.0.
- Community 4, public: the default value is 0.0.0.0.
- Community 5, common: the default value is 0.0.0.0.
- Community 6, FibreChannel: the default value is 0.0.0.0.

Example

```
sw5:admin> agtcfgSet

Customizing MIB-II system variables ...

At each prompt, do one of the following:
    o <Return> to accept current value,
    o enter the appropriate new value,
    o <Ctrl+D> to skip the rest of configuration, or
    o <Ctrl+C> to cancel any change.
To correct any input mistake:

    <
> erases the previous character,
    <Ctrl+U> erases the whole line,

    sysDescr: [FC Switch]
    sysLocation: [End User Premise]
    sysContact: [Field Support]
    swEventTrapLevel: (0..5) [3] 4
    authTrapsEnabled (true, t, false, f): [true]

SNMP community and trap recipient configuration:

Community (rw): [Secret C0de]
    Trap Recipient’s IP address in dot notation: [192.168.1.51]
Community (rw): [OrigEquipMfr]
    Trap Recipient’s IP address in dot notation: [192.168.1.26]
Community (rw): [private]
    Trap Recipient’s IP address in dot notation: [0.0.0.0]
192.168.64.88
Community (ro): [public]
    Trap Recipient’s IP address in dot notation: [0.0.0.0]
Community (ro): [common]
    Trap Recipient’s IP address in dot notation: [0.0.0.0]
Community (ro): [FibreChannel]
    Trap Recipient’s IP address in dot notation: [0.0.0.0]

value = 1 = 0x1
sw5:admin>
```

See also

agtcfgDefault
agtcfgShow
errShow

agtcfgShow

The **agtcfgShow** command displays the SNMP agent configuration.

Syntax

```
agtcfgShow
```

Availability

All users

Description

Use this command to display the configuration of the SNMP agent in the switch. The following information is displayed:

sysDescr

Displays the switch description.

sysLocation

Displays the location of the switch.

sysContact

Displays the contact information for this switch.

swEventTrapLevel

Displays the event trap level. Possible values are:

0 none

1 critical

2 error

3 warning

4 informational

5 debug

For more information about the event trap level, see the **errShow** command.

authTraps

Displays whether authorization traps are passed to the trap recipient. The default value is 0 (off), meaning no messages are sent. A value of 1 (on) means that authorization trap messages are sent to the community IP addresses that have been configured. For SNMPv1 and SNMPv2c, this indicates that a request containing a community string is not known to the agent.

trap recipient

There are six communities, each with a respective trap recipient, supported by the agent. The first three communities are for read-write (rw) access and the last three are for read-only (ro) access.

Before an SNMP management station can receive a trap that is generated by the agent, the administrator must configure a trap recipient IP address of the management station.

Community 1: Secret C0de

Displays the IP address for this trap recipient.

Community 2: OrigEquipMfr

Displays the IP address for this trap recipient.

Community 3: private

Displays the IP address for this trap recipient.

Community 4: public

Displays the IP address for this trap recipient.

Community 5: common

Displays the IP address for this trap recipient.

Community 6: FibreChannel

Displays the IP address for this trap recipient.

For more information about these SNMP configuration parameters, see the **agtcfgset** command.

Operands

None

Example

```
sw5:admin> agtcfgShow

Current SNMP Agent Configuration

Customizable MIB-II system variables:
    sysDescr = FC Switch
    sysLocation = End User Premise
    sysContact = Field Support.
    swEventTrapLevel = 3
    authTraps = 1 (ON)

SNMPv1 community and trap recipient configuration:

Community 1: Secret COde (rw)
    Trap recipient: 192.168.1.51

Community 2: OrigEquipMfr (rw)
    Trap recipient: 192.168.1.26

Community 3: private (rw)
    No trap recipient configured yet

Community 4: public (ro)
    No trap recipient configured yet

Community 5: common (ro)
    No trap recipient configured yet

Community 6: FibreChannel (ro)
    No trap recipient configured yet
```

See also

agtcfgDefault
agtcfgSet

aliasShow

The **aliasShow** command displays the alias server information.

Syntax

```
aliasShow
```

Availability

All users

Description

Use this command to display local alias server information. If there is no local alias group, a message is displayed. If there are multiple entries in the local alias group, they are displayed.

The following fields are displayed:

Alias ID

The multicast address presented in format FFFB*xx*, where *xx* is the name of the multicast group.

Creator

The fibre-channel address ID of the Nx_port that created alias group.

Creator token

The alias token that is provided to map to the alias group; it consists of the following entries:

rb	Routing bits.
type	The upper level application type.
grptype	Alias group type; must be 10 for multicast.
qlfr	The alias group qualifier.

Member list

A list of member address IDs.

Operands

None

Example

```
switch:admin> aliasShow
The Local Alias Server has 1 entry
Alias ID Creator Token [rb, type, grptype, qlfr] Member List
fffb01 fffffd [40, 05, 10, 60000010 12000069] {021200 0208e2}
```

backspace

The **backspace** command sets or clears the alternate backspace character.

Syntax

```
backSpace [0 | 1]
```

Availability

All users (display)

administrator (set or clear)

Description

Use this command to change the backspace character that is used by the shell from the default value of `BACKSPACE` (hex 08) to an alternate value of `DEL` (hex 7F).

Operands

This command has the following operand:

[0 | 1] Specify 0 to use the standard backspace character (BACKSPACE). Specify 1 to use the alternate backspace character (DEL). This operand is optional.

Specify the command with no operand to display the current setting.

Examples

The following example shows displaying the current backspace character and then how to change it to DEL.

```
switch:admin> backSpace
BackSpace character is BACKSPACE (hex 08)
switch:admin> backSpace 1
Committing configuration...done.
BackSpace character is DEL (hex 7F)
```

bcastShow

The **bcastShow** command displays broadcast routing information.

Syntax

```
bcastShow
```

Availability

All users

Description

Use this command to display the broadcast routing information for all ports in the switch that are known to the FSPF path selection/routing task. The broadcast routing information indicates all ports that are members of the broadcast distribution tree (that is, ports that are able to send and receive broadcast frames).

Normally, all F_ports and FL_ports are members of the broadcast distribution tree. The broadcast path selection protocol selects the E_ports that are part of the broadcast distribution tree. The E_ports are chosen in such a way as to prevent broadcast routing loops.

The broadcast routing information displays as a set of bit maps. Each bit in a bit map represents a port, with the least significant bit representing port 0. If a bit is set to 1, that port is part of the broadcast distribution tree. The following describes the fields.

Group

Displays the multicast group ID of the broadcast group.

Member ports

Displays a map of all ports in the broadcast tree.

Member ISL ports

Displays a map of all E_ports in the broadcast tree.

Static ISL ports

Reserved.

Operands

None

Examples

```
switch:admin> bcastShow
Group Member Ports Member ISL Ports Static ISL Ports
-----------------------------------------------------------
-----
256 0x00012083 0x00002080 0x00000000
```

See also

mcastShow

portRouteShow

camTest

The **camTest** commands tests the function of the CAM memory.

Syntax

```
camTest [passCount]
```

Availability

Administrator

Description

Use this command to verify that content addressable memory (CAM) is functionally correct. The CAM is used by QuickLoop to translate the SID.

The following are possible error messages if failures are detected:

DIAG-CAMINIT DIAG-XMIT DIAG-CAMSID

Operands

This command has the following operand:

passCount

Specify the number of times to run this test. The default value is 1. This operand is optional.

Example

```
sw7:admin> camTest 2
Running CAM Test .............. passed.
```

See also

centralMemoryTest

cmemRetentionTest

cmiTest

crossPortTest

portLoopbackTest

portRegTest

ramTest

spinSilk

sramRetentionTest

centralMemoryTest

The **centralMemoryTest** command tests the bit write/read test of the ASIC central memory.

Syntax

```
centralMemoryTest [passCount, dataType, dataSeed]
```

Availability

Administrator

Description

Use this command to verify the address and data bus of the ASIC SRAMs that serve as the central memory.

The following are possible error messages if failures are detected:

DIAG-TIMEOUT DIAG-BADINT DIAG-CMERRTYPE DIAG-CMERRPTN

Operands

This command has the following operands. If all are omitted, the default values used are 1 for passCount, QUAD_RAMP for dataType, and a random value for dataSeed.

passCount
The number of times to run this test

dataType
The data type to use when writing the central memory. The **dataTypeShow** command lists data types allowed.

dataSeed
The initial seed value used in generating the data pattern. For example, a QUAD_RAMP pattern with a seed value of 0xdead is as follows: 0xdead, 0xdeae, 0xdeaf, 0xdeb0, ...

Example

```
sw7:admin> centralMemoryTest
Running Central Memory Test ... passed.
```

See also

camTest

cmemRetentionTest

cmiTest

crossPortTest

portLoopbackTest

portRegTest

ramTest

spinSilk

sramRetentionTest

cmemRetentionTest

The **cmemRetentionTest** command tests the data retention of the central memory SRAMs.

Syntax

```
cmemRetentionTest [passCount]
```

Availability

Administrator

Description

Use this command to verify for data retention in the central memory SRAMs in the ASIC.

The following are possible error messages if failures are detected:

DIAG-LCMRS

DIAG-LCMTO

DIAG-LCMEM

Operands

This command has the following operand:

passCount
: Specify the number of times to run this test. The default value is 1. This operand is optional.

Example

```
sw7 :admin> cmemRetentionTest
Running CMEM Retention Test ...
passed.
```

See also

camTest

centralMemoryTest

cmiTest

crossPortTest

portLoopbackTest

ramTest

spinSilk

cmiTest

The **cmiTest** command tests the connection of ASIC to ASIC for the CMI bus.

Syntax

```
cmiTest [passCount]
```

Availability

Administrator

Description

Use this command to verify that the multiplexed 4-bit control message interface (CMI) point-to-point connection between two ASICs is functioning properly. Also use it to verify that a message with a bad checksum sets the error and interrupt status bits of the destination ASIC and that a message with a good checksum does not set an error or interrupt bit in any ASIC.

The test method is displayed below. Complete the following for each source ASIC X and each destination ASIC Y in the switch. Do not complete this test if ASIC X = ASIC Y.

1. Generate the CMI data D.
2. Send data from source X to destination Y.
3. Check destination Y for the following:
   - The capture flag is set.
   - The data is received as expected (D).
   - If the checksum test is good, the CMI error bit and the EMI error interrupt status bit are not set.
   - If the checksum test is bad, the CMI error bit and the CMI error interrupt status bit are set.
4. Check that all ASICs (other than Y) do not have:
   - The capture flag set.
   - The CMI error bit set.
   - The CMI error interrupt status bit set.

The following are possible error messages if failures are detected:

DIAG-CMISA1

DIAG-CMINOCAP

DIAG-CMICKSUM

DIAG-CMIINVCAP

DIAG-CMIDATA

DIAG-INTNIL

DIAG-BADINT

Operands

This command has the following operand:

passCount
Specify the number of times to run this test. The default value is 1. This operand is optional.

Example

```
sw7:admin> cmiTest
Running CMI Test .............. passed.
```

See also

camTest

centralMemoryTest

cmemRetentionTest

crossPortTest

portLoopbackTest

portRegTest

ramTest

spinSilk

sramRetentionTest

configDefault

The **configDefault** command restores the system configuration to the default settings.

Syntax

```
configDefault
```

Availability

Administrator

Description

Use this command to reset the system configuration to default values. All configuration parameters, with the following exceptions, are reset to default values:

- Ethernet MAC address, IP address, and subnetmask
- IP gateway address
- License keys
- OEM customization
- SNMP configuration
- System name
- World-wide name
- Zoning configuration

Note: See the **configure** command for more information about the default values for configuration parameters.

Attention: Do not run this command on an enabled system; first disable the system using the **switchDisable** command.

Some configuration parameters are cached by the system. To avoid unexpected switch behavior, restart the system after running this command.

Operands

None

Example

```
switch:admin> configDefault
Committing configuration...done.
```

See also

agtcfgDefault
configure
switchDisable
switchEnable

configDownload

The **configDownload** command downloads the switch configuration from a host file.

Syntax

```
configDownload [“host”,“user”,“file”[,passwd]]
```

Availability

Administrator

Description

Use this command to download the switch configuration file from a host system. The configuration file is an ASCII text file. The file might have been generated using the **configUpload** command, or it might have been created by the user to download specific configuration changes.

The download process uses either FTP or the RSHD protocol (TCP service 514). On Windows NT, the FTP server might have to be installed from the distribution media and enabled. On Windows NT or Windows 9x, there are several good freeware and shareware FTP servers available. To use RSHD on Windows NT or Windows 9 x, two utilities are supplied, RSHD.EXE and CAT.EXE, together with instructions on how to install and run them. The FTP server or RSHD must be running before a download can be initiated.

If the **configDownload** command is invoked without any operands, you are prompted for input, including whether you want to use FTP or RSHD. If you use three operands, RSHD is used. Otherwise, if you enter a password operand, FTP is used.

Note that the identity of the switch cannot be changed by the **configDownload** command. Parameters, such as the name and IP address of the switch, are ignored. These are the lines in the configuration file that begin with “boot”.

Also note that the download process is additive; that is, the lines that are read from the file are added to the current switch configuration. This enables you to change a single configuration variable by downloading a file with a single line. All other variables remain unchanged.

This is particularly important when downloading a zoning configuration. Because the new zoning information is added to the current configuration, there might not be any conflicts. Typically, this command is used to either add a consistent change to the current zoning configuration or to replace the current zoning configuration. In these cases, the **cfgClear** command must be invoked before the **configDownload** command.

Operands

This command has the following operands:

“host”

Specify a host name or IP address in quotation marks; for example, `"citadel" or "192.168.1.48"`. The configuration file is downloaded from this host system. This operand is optional.

“user”

Specify a user name in quotation marks; for example, `"jdoe"`. This user name is used to gain access to the host. This operand is optional.

“file”

Specify a file name in quotation marks; for example, `“config.txt”`. Absolute path names can be specified using the forward slash (/). Relative path names create the file in your home directory on UNIX hosts, and in the directory where the FTP server is running on Windows hosts. This operand is optional.

passwd

Specify a password. If present, the command uses FTP to transfer the file. This operand is optional.

Example

```
switch:admin> configDownload “citadel”,“jdoe”,“config.txt”
Committing configuration...done.
download complete
```

Errors

The following are possible reasons for a failure of this command:

- The host name is not known to the switch.
- The host IP address cannot be contacted.
- The user does not have permission on the host.
- The user runs a script that prints something at login.
- The file does not exist on the host.
- The file is not a switch configuration file.

- The RSHD or FTP server is not running on the host.
- The configuration data contains errors.

See also

configDefault
configUpload
configShow
configure

configShow

The **configShow** command displays the system configuration settings.

Syntax

```
configShow [“filter”]
```

Availability

All users

Description

Use this command to view system configuration settings that have been set by the **configure** command, as well as to view the following:

- Ethernet MAC address
- NVRAM start up settings

Operands

This command has the following operand:

“filter”

Specify a text string, in quotation marks, that limits the output of the command to only those entries that contain the text string. The filter does not apply to the Ethernet MAC address and NVRAM data display settings.

Example

```
switch:admin> configShow
Ethernet address: 0:60:69:0:60:10
Nvram data: fei(0,0)host:/usr/switch/firmware
e=192.168.1.62 g=192.168.1.254 u=user tn=switch
Type <CR> to continue, Q<CR> to stop:
diag.postDisable: 0
fabric.domain: 1
fabric.ops.BBCredit: 16
fabric.ops.E_D_TOV: 2000
fabric.ops.R_A_TOV: 10000
fabric.ops.dataFieldSize: 2112
fabric.ops.mode.fcpProbeDisable: 0
fabric.ops.mode.isolate: 0
fabric.ops.mode.tachyonCompat: 0
fabric.ops.mode.unicastOnly: 0
fabric.ops.mode.useCsCtl: 0
fabric.ops.mode.vcEncode: 0
fabric.ops.vc.class.2: 2
fabric.ops.vc.class.3: 3
fabric.ops.vc.config: 0xc0
fabric.ops.vc.linkCtrl: 0
fabric.ops.vc.multicast: 7
fc4.fcIp.address: 192.168.65.62
fc4.fcIp.mask: 255.255.255.0
fcAL.fanFrameDisable: 0
fcAL.useAltBBCredit: 0
lcdContrast: 128
licenseKey: none
rpc.rstatd: 1
rpc.rusersd: 1
```

See also

agtcfgShow
configure
diagDisablePost
diagEnablePost
ipAddrShow
licenseShow

configUpload

The **configUpload** command uploads the switch configuration to a host file.

Syntax

```
configUpload [“host”,“user”,“file”[,passwd]]
```

Availability

Administrator

Description

Use this command to upload the switch configuration to a host file. The upload process uses either FTP or the RSHD protocol (TPC service 514). Both of these services are widely available on UNIX hosts, but less so on Windows hosts. On Windows NT, the FTP server might have to be installed from the distribution media and enabled. On Windows NT or Windows 9x, there are several freeware and shareware FTP servers available.

The two utilities supplied (for RSHD.EXE and CAT.EXE) currently do not support uploads, only downloads. Therefore, in a Windows environment, FTP must be used, and the FTP server must be running before an upload can occur.

If you enter the **configUpload** command, you are prompted for input, including whether you want to use FTP or RSHD. If you use three operands, RSHD is used. Otherwise, if you enter a password operand, FTP is used.

Operands

This command has the following operands:

“host”

Specify a host name or IP address in quotation marks; for example, `“citadel”` or `“192.168.1.48”`. The configuration file is downloaded from this host system. This operand is optional.

“user”

Specify a user name in quotation marks; for example, `“jdoe”`. This user name is used to gain access to the host. This operand is optional

“file”

Specify a file name in quotation marks; for example, `“config.txt”`. Absolute path names can be specified using the forward slash (/). Relative path names create the file in the your home directory on UNIX hosts, and in the directory where the FTP server is running on Windows hosts. This operand is optional.

passwd

Specify a password. If present, the command uses FTP to transfer the file. This operand is optional.

Example

The following example shows uploading the configuration file `"config.txt"` using FTP from the host `“citadel”` and account `“jdoe”:`

```
swd5:admin> configUpload “citadel”,“jdoe”,“config.txt”,“passwd”
upload complete
```

If you upload the configuration file from the switch to a host, you are prompted to enter the correct responses to the parameters, as shown in the following example:

```
swd154:admin> configUpload
Server Name or IP Address [citadel]: 192.168.15.42
User Name [none]: user21
File Name [config.txt]: config-swd154.txt
Protocol (RSHD or FTP) [FTP]: ftp
Password:
upload complete
swd154:admin>
```

Errors

The upload can fail for several reasons:

- The host name is not known to the switch.
- The host IP address cannot be contacted.
- The user does not have permission on the host.
- The user runs a script that prints something at login.
- The RSHD or FTP server is not running on the host.

See also

configDefault
configDownload
configShow
configure

configure

The **configure** command changes the system configuration settings.

Syntax

```
configure
```

Availability

Administrator

Description

Use this command to change the following system configuration settings:

- Arbitrated loop settings
- Switch fabric settings
- System services settings
- Virtual channel settings

Attention: Do not run the **configure** command on an enabled system; first disable the system using the **switchDisable** command.

You use the **configure** command to navigate a series of menus. Top level menus and associated submenus consist of a text prompt, a list of acceptable values, and a default value (in brackets).

Use the following options to control input:

Return

When entered at a prompt with no preceding input, accepts the default value (if applicable) and moves to the next prompt.

Interrupt (Ctrl+C)

Ends the command immediately and ignores all changes made.

End-of-file (Ctrl+D)

When entered at a prompt with no preceding input, ends the command and saves changes made.

Note: You can use (Ctrl+D) on most computers; however, your settings could be different.

Arbitrated loop settings

Table 13 describes the arbitrated loop settings that can be changed.

Table 13. Arbitrated loop settings

Field	Type	Default	Range
Send FAN frames?	Boolean	1	0 or 1
Always send RSCN?	Boolean	0	0 or 1

Send FAN frames?

Specifies that the fabric address notification (FAN) frames be sent to public loop devices to notify them of their node ID and address. When set to 1, frames are sent. When set to 0, frames are not sent.

Always send RSCN?

Following the completion of loop initialization, a remote state change notification (RSCN) is issued when the FL_ports detect the presence of new devices or the absence of preexisting devices. When set, an RSCN is issued upon completion of loop initialization, regardless of the presence or absence of new or preexisting devices.

Switch fabric settings

There are a number of settings that control the overall behavior and operation of the fabric. Some of these values, such as the domain, are assigned automatically by the fabric and can differ from one switch to another in the fabric. Other parameters, such as the buffer-to-buffer credit or the timeout values, can be changed for specific applications or operating environments, but must be in agreement among all switches to allow formation of the fabric.

Table 14 defines the settings that can be changed.

Table 14. Switch fabric settings

Field	Type	Default	Range
Domain	Number		
BB credit	Number		
R_A_TOV	Number	10000	E_D_TOV *2 to 120000
E_D_TOV	Number		
Data field size	Number		
Non-SCSI Tachyon mode	Boolean		
Disable device probing	Boolean		
Unicast-only operation			
VC encoded address mode	Boolean		
Disable translative mode	Boolean		
Per-frame route priority	Boolean		

The following is a description of the switch fabric settings:

Domain The domain number uniquely identifies the switch in a fabric. This value is automatically assigned by the fabric. The range of allowed values varies depending on the switch model and other system settings. See VC encoded address mode.

BB credit

This specifies the largest possible value, in bytes, and advertises this value to other switches in the fabric during construction of the fabric, as well as to other devices when they connect to the fabric. Setting this to a value smaller than 2112 can result in decreased performance.

R_A_TOV

The resource-allocation timeout value (R_A_TOV) is displayed in milliseconds. This variable works with the variable E_D_TOV to determine switch actions when presented with an error condition.

Allocated circuit resources with detected errors are not released until the time value has expired. If the condition is resolved prior to the timeout, the internal timeout clock resets and waits for the next error condition.

E_D_TOV

The error detect timeout value (E_D_TOV) is displayed in milliseconds. This timer is used to flag a potential error condition when an expected response is not received (for example, an acknowledgment or reply in response to packet receipt) within the set time limit. If the time for an expected response exceeds the set value, an error condition occurs.

Data field size

This specifies the largest possible value, in bytes, and advertises this value to other switches in the fabric during construction of the fabric, as well as to other devices when they connect to the fabric. Setting this to a value smaller than 2112 can result in decreased performance.

Non-SCSI Tachyon mode

When set, multiple sequences from different sources are interleaved to Tachyon-based controllers at sequence boundaries rather than at frame boundaries, resulting in better performance from Tachyon-based controllers. Set this mode when there are no Tachyon-based SCSI host adapters connected to the fabric.

Disable device probing

When this is set, devices that do not register with the name server are not present in the name server database. Set this mode only if the switch N_port discovery process (PLOGI, PRLI, INQUIRY) causes an attached device to fail.

VC encoded address mode

When this mode is set, frame source and destination address utilize an address format compatible with some first-generation switches. Set this mode only if the fabric includes this type of switch.

Disable translative mode

The setting applies only if VC encoded address mode is also set. This value, when set, disables translative addressing to achieve explicit address compatibility with some first-generation switches. Set this value only if hardware or software systems are attached to the fabric that explicitly rely on a specific frame address format.

Per-frame route priority

In addition to the eight virtual channels used in frame routing priority, support is also available for per-frame based prioritization when this value is set. When set, the virtual channel ID is used in conjunction with a frame header to form the final virtual channel ID.

System service settings

Table 15 describes the system services settings that can be changed.

Table 15. System service settings

Field	**Type**	**Default**	**Range**
rstatd	Boolean	Off	On/Off
rusersd	Boolean	Off	On/Off

The following is a description of the system service settings:

rstatd Dynamically enables or disables a server that returns information about system operation through remote procedure calls (RPC). The protocol provides for a wide range of system statistics; however, only Ethernet interface statistics (see **ifShow**) and system up time (see **uptime**) are supported.

Retrieving this information is supported by a number of operating systems which support RPC. On most UNIX-based systems (for example, HP-UX, Irix, Linux, Solaris, and others), the commands to retrieve the information are **rup** and **rsysinfo**. See your local system documentation for the appropriate usage of these or equivalent commands.

rusersd Dynamically enables or disables a server that returns information about the user logged into the system through remote procedure calls (RPC). The information returned includes user login name, the system name, login protocol or type, login time, idle time, and remote login location (if applicable).

Retrieving this information is supported by a number of operating systems which support RPC. On most UNIX-based systems (for example, HP-UX, Irix, Linux, Solaris, and others) the command to retrieve the information is **rusers**. See your local system documentation for the appropriate usage of this or equivalent commands.

Virtual channel settings

The switch provides you with the ability to tune a specific application by configuring the parameters for its eight virtual channels. Note that the first two virtual channels are reserved for switch internal functions and are not user-configurable.

The default virtual channel settings have already been optimized for switch performance. Changing the default values can improve switch performance, but it can also degrade performance. Do not change these settings without fully understanding the effects of the changes.

Table 16 shows the type, default, and range of the virtual channel settings fields.

Table 16. Virtual channel settings

Field	Type	Default	Range
VC link control	Number	0	0 - 1
VC class 2	Number	2	2 - 5
VC class 3	Number	3	2 - 5
VC multicast	Number	7	6 - 7
VC priority 2	Number	2	2 - 3
VC priority 3	Number	2	2 - 3
VC priority 4	Number	2	2 - 3
VC priority 5	Number	2	2 - 3
VC priority 6	Number	3	2 - 3
VC priority 7	Number	3	2 - 3

The following is a description of the virtual channel settings.

VC link control

Specifies the virtual channel used for N_port-generated, class 2 link control frames (ACKS, P_BSYs, P_RJTs). This setting forces N_port-generated link control frames to be sent using a class 2 data virtual channel when set to 0. When set to 1, the control frames are sent using a virtual channel that is normally reserved for fabric-internal traffic.

This setting is configurable only when the VC encoded address mode is set.

VC class 2

Specifies the virtual channel used for class 2 frame traffic.

VC class 3
Specifies the virtual channel used for class 3 frame traffic. This setting is configurable only when the VC encoded address mode is set.

VC multicast
Specifies the virtual channel used for multicast frame traffic. This setting is configurable only when the VC encoded address mode is set.

VC priority
Specifies the class of frame traffic given priority for a virtual channel.

Operands

None

Example

```
switch:admin> configure
Configure...
Fabric parameters (yes, y, no, n): [no] yes
Domain: (1..239) [1]
BB credit: (1..16) [16]
R_A_TOV: (4000..120000) [10000]
E_D_TOV: (1000..5000) [2000] 5000
Data field size: (256..2112) [2112]
Non-SCSI Tachyon Mode: (0..1) [0] 1
Disable Device Probing: (0..1) [0]
VC Encoded Address Mode: (0..1) [0] 1
Disable Translative Mode: (0..1) [0]
Per-frame Route Priority: (0..1) [0]
Virtual Channel parameters (yes, y, no, n): [no] yes
VC Link Control: (0..1) [0]
VC Class 2: (2..5) [2]
VC Class 3: (2..5) [3]
VC Multicast: (6..7) [7]
VC Priority 2: (2..3) [2]
VC Priority 3: (2..3) [2]
VC Priority 4: (2..3) [2]
VC Priority 5: (2..3) [2]
VC Priority 6: (2..3) [3]
VC Priority 7: (2..3) [3]
Arbitrated Loop parameters (yes, y, no, n): [no] yes
Send FAN frames?: (0..1) [1]
Always send RSCN?: (0..1) [0]
System services (yes, y, no, n): [no] yes
rstatd (on, off): [off] on
rusersd (on, off): [off] on
Committing configuration...done.
```

See also

agtcfgDefault
agtcfgSet
agtcfgShow
configDefault
configShow
ifShow
ipAddrSet
switchDisable
switchEnable
uptime

crossPortTest

The **crossPortTest** command tests the function of the port M-N path.

Syntax

```
crossPortTest [passCount, singlePortAlso]
```

Availability

Administrator

Description

Use this command to verify the functional operation of the switch. This command verifies operation by sending frames from port M's transmitter and looping the frames back through an external fiber cable into another port N receiver. This exercises all the switch components from the main board to the GBIC, from the GBIC to the fiber cable, from the fiber cable to the GBIC, and from the GBIC back to the main board.

The cables can be connected to any port combination as long as the cables and GBICs connected are of the same technology. A short wavelength GBIC port is connected to another short wavelength GBIC port using a short wavelength cable, a long wavelength port is connected to a long wavelength port, and a copper port is connected to a copper port.

For complete testing, ports connected should be from different ASICs. Ports 0 - 3 are assigned to ASIC 0, ports 4 - 7 are assigned to ASIC 1, and so on. A connection from port 0 to port 15 exercises the transmit path between ASICs. A connection from port 0 to port 3 tests only the internal transmit path in ASIC 0.

Only one frame is transmitted and received at a given time, and the port LEDs flicker green while the test is running.

Test method:

1. Determine the port connections.
2. Enable the ports for cabled loopback mode.
3. Create a frame F with a maximum data size (2112 bytes).
4. Transmit frame F through port M.
5. Pick up the frame from its cross connected port N. Complain if port other than N actually received the frame.

6. Pick up the frame from its cross connected port N. Complain if port other than N actually received the frame.

   ENC_in, CRC_err, TruncFrm, FrmTooLong, BadEOF, Enc_out, BadOrdSet, DiscC3

7. Check the transmit, receive or class 3 receiver counters to see if they are stuck at some value.
8. Check that the number of frames received is equal to the number of frames transmitted.
9. Repeat steps 3 through 8 for all ports present until the number of frames (or passCount) requested is reached or all ports are marked bad.

At each pass, the frame is created from a different data type. If seven passes are requested, seven different data types are used in the test. If eight passes are requested, the first seven frames use unique data types, and the eighth is the same as the first. The seven data types are:

1. CUSPID: axel axel axel axel ...
2. Bottlefuls: axel axel axel axel ...
3. Chaffiest: axial axial axial axial ...
4. Quotient: axel axon axel axon ...
5. Catchers: axel axel axel axel ...
6. CREPT: oxbow oxbow axel axel ...
7. RANDOM: axel axon axel axial ...

Modes

One of three following modes can be activated. The test produces different results for each mode:

- switchEnable/switchDisable mode
- singlePortAlso mode
- GBIC mode

switchEnable/switchDisable mode

This mode can be run in one of two states, online or offline.

In the online state, the switch is enabled prior to executing the test. In this state, only ports that are cable loopbacked to ports from the same switch are tested. Ports connected outside of the switch are ignored.

To run, at least one port (if the singlePortAlso is active) or two ports (if singlePortAlso is not active) must be cable loopbacked to each other. If this criteria is not met, the following messages are sent to the Telnet shell:

```
Need at least one port(s) connected to run this test
(singlePortAlso active)
```

or

```
Need at least two port(s) cross-connected to run this test
(singlePortAlso not active)
```

The following message appears in the front panel display:

```
Need at least one port(s) connected first (singlePortAlso
active)
```

or

```
Need at least two port(s) cross-connected first.
(singlePortAlso not active)
```

In the offline state, the switch is disabled prior to executing the test. In this state, it is assumed that all ports (see GBIC mode) are cable loopbacked to similar ports in the same switch. If one or more ports are not connected, the test aborts.

The test determines which port is connected to which port transmitting frames. If any ports are not properly connected (improperly seated GBICs or cables, bad GBICs or cables, or improper connection of SWL to LWL), the following message is sent to the Telnet shell:

```
One or more ports is not active, please double check fibres
on all ports.
```

The following message displays on the front panel:

```
One or more ports not cabled.
```

singlePortAlso mode

Specify **singlePortAlso** mode by executing the **crossPortTest** command with a value of 1 for the second argument:

```
sw:admin> crossPortTest 0, 1
```

In this mode, a port can be cable loopbacked to itself (port M is connected to port M) in addition to being cross connected (port M is connected to port N). This mode can be used to isolate improperly functioning ports.

GBIC mode

Activate GBIC mode by running the **sw:admin> setGbicMode 1** command before running the **crossPortTest** command.

When activated, only ports with GBICs present are tested by the **crossPortTest** command. For example, if only port 0 and port 3 contain GBICs, the **crossPortTest** test limits testing to port 0 and port 3.

The state of GBIC mode is saved in flash memory and it remains active (even after restarts or power cycles) until it is disabled as follows:

```
sw:admin> setGbicMode 0
```

For example, disable the switch, set the GBIC mode to 1, and run the

crossPortTest command with **singlePortAlso** activated and the crossPortTest to limit testing to only ports containing GBICs that _all_ GBIC ports that are cable loopbacked ports connected to themselves (single port connections) Because this test includes the GBIC and the fiber cable in the test path, use the results from this test, in conjunction with the results from the **portLoopbackTest** and the spinSilk test to determine those switch components that are not functioning properly.

The following are possible error messages, if failures are detected:

DIAG-INIT

DIAG-PORTDIED

DIAG-XMIT

DIAG-TIMEOUT

DIAG-ERRSTAT

DIAG-STATS

DIAG-PORTWRONG

DIAG-DATA

Operands

This command has the following operands:

passCount
Specify the number of times (or number of frames per port) to run this test. If omitted, the default value is `0xfffffffe`.

singlePortAlso
Specify `1` to connect port N to itself (port N->N).

Example

```
sw7:admin> crossPortTest 100
Running Cross Port Test .......
One moment please ...
switchName: sw7
switchType: 2.2
switchState: Testing
switchRole: Disabled
switchDomain: 1 (unconfirmed)
switchId: fffc01
switchWwn: 10:00:00:60:69:00:73:71
port 0: cu Testing Loopback->15
port 1: sw Testing Loopback->11
port 2: sw Testing Loopback->6
port 3: lw Testing Loopback->4
port 4: lw Testing Loopback->3
port 5: sw Testing Loopback->8
port 6: sw Testing Loopback->2
port 7: sw Testing Loopback->12
port 8: sw Testing Loopback->5
port 9: sw Testing Loopback->14
port 10: sw Testing Loopback->13
port 11: sw Testing Loopback->1
port 12: sw Testing Loopback->7
port 13: sw Testing Loopback->10
port 14: sw Testing Loopback->9
port 15: cu Testing Loopback->0
passed.
```

See also

camTest

centralMemoryTest

cmemRetentionTest

cmiTest

portLoopbackTest

portRegTest

ramTest

spinSilk

sramRetentionTest

date

The **date** command displays or sets the system date and time.

Syntax

```
date [“newDate”]
```

Availability

All users (display)

Administrator (set)

Description

Use this command with no operands to display the date and time. Use the **newdate** operand to set the date and time. Date and time are specified as a quoted string in the format:

```
“mmddhhmmyy”
```

where:

mm is the month	01 - 12
dd is the date	01 - 31
hh is the hour	00 - 23
mm is minutes	00 - 59
yy is the year	00 - 99

The firmware is year 2000 compliant. Year values greater than 69 are interpreted as 1970 - 1999, year values less than 70 are interpreted as 2000 - 2069.

The date function does not support daylight savings time or time zones.

All switches maintain the current date and time in nonvolatile memory. Date and time are used for logging events. Switch operation does not depend on the date and time; a switch with an incorrect date value still functions properly.

Operands

The **date** command has the following operand:

New Date

Specify the new date and time in quotation marks. This operand is optional.

Example

The following example shows displaying the current date and time, then changing the date and time to Feb 27 15:31:00 2001:

```
sw5:admin> date
Fri Jan 29 17:01:48 1999
sw5:admin> date “0227153101”
Thu Feb 27 15:31:00 2001
```

See also

portLogShow
uptime

diagClearError

The **diagClearError** command clears the diag software flag to allow for retest.

Syntax

```
diagClearError [port]
```

Availability

Administrator

Description

Use this command to clear the diag software flag that indicates whether a port is BAD or OK. The current flag settings are displayed by using the **doggish** command. This command resets the flag to allow the bad port to be retested; otherwise, the test skips the port.

When the command is used with no operand, the current level is displayed.

This command does not clear the error log entry. Instead, it generates the DIAG-Clear_ERR message for each port software flag cleared. For example:

```
0x10f9d560 (tShell): Apr 9 08:35:50
Error DIAG-CLEAR_ERR, 3, Pt13 (Lm3) Diagnostics Error
Cleared Err# 0001 0x10f9d560 (tShell): Apr 9 08:35:50
Error DIAG-CLEAR_ERR, 3, Pt13 (Lm3) Diagnostics Error
Cleared Err# 0001
```

Operands

This command has the following operand:

port Specify the port where you want to reset the diag software flag. The default (if no operand is specified) is to clear all bad port flags. This operand is optional.

Example

```
sw7:admin> diagClearError
0x10f9d5e0 (tShell): Apr 6 13:25:36
  Error DIAG-CLEAR_ERR, 3,
Pt7 (Lm1) Diagnostics Error Cleared
Err# 0001
```

See also

diagShow

diagDisablePost

The **diagDisablePost** command disables the execution at restart.

Syntax

```
diagDisablePost
```

Availability

Administrator

Description

Use this command to disable the power-on self-test (POST) execution at switch restart. This mode is saved in flash memory and POST remains disabled until it is enabled using the **diagEnablePost** command.

A switch restarted without POST enabled issues a diag-postskipped error message:

```
0x10fc0c10 (tSwitch): Apr 6 13:24:42
Error DIAG-POST_SKIPPED, 3,
Skipped POST tests: assuming all ports are healthy,
Err# 0004
```

POST includes the following tests:

- ramTest - Bit write / read test of SDRAMS in the switch.
- portRegTest - Bit write / read test of the ASIC SRAMs and registers.
- centralMemoryTest - Bit write / read test of the ASIC central memory.
- cmiTest - ASIC to ASIC connection test of the CMI bus.
- camTest - Functional test of the CAM memory.
- portLoopbackTest - Functional test of switch by sending and receiving frames from the same port.

For more information about these tests, refer to the individual command descriptions.

Note: The cold restart (power reset) runs the long ramTest while the warm restart (software reset) runs the short ramTest.

Operands

None

Example

```
sw7:admin> diagDisablePost
Committing configuration...done.
On next restart, POST will be skipped.
```

See also

diagEnablePost

diagEnablePost

The **diagEnablePost** command enables POST execution at the next restart.

Syntax

```
diagEnablePost
```

Availability

Administrator

Description

Use this command to enable the power-on self-test (POST) execution at the next switch restart. This mode is saved in flash memory and POST remains enabled until it is disabled using the **diagDisablePost** command.

POST includes the following tests:

- ramTest - Bit write / read test of SDRAMS in the switch.
- portRegTest - Bit write / read test of the ASIC SRAMs and registers.
- centralMemoryTest - Bit write / read test of the ASIC central memory.
- cmiTest - ASIC to ASIC connection test of the CMI bus.
- camTest - Functional test of the CAM memory.
- portLoopbackTest - Functional test of switch by sending and receiving frames from the same port.

For more information about these tests, refer to the individual command descriptions.

Note: The cold startup (power reset) runs the long ramTest while the warm startup (software reset) runs the short ramTest.

Operands

None

Example

```
sw7:admin> diagEnablePost
Committing configuration...done.
On next restart, POST will be executed.
```

See also

camTest

centralMemoryTest

cmiTest

diagDisablePost

portLoopbackTest

portRegTest

ramTest

diagHelp

The **diagHelp** command displays the available diagnostic help commands.

Syntax

```
diagHelp
```

Availability

All users

Description

Use this command to display a list of the diagnostic help commands for diagnosing switch problems.

Operands

None

Example

```
Sr99:admin> diaghelp

ramTest                 System DRAM diagnostic
portRegTest             Port register diagnostic
centralMemoryTest       Central memory diagnostic
cmiTest                 CMI bus connection diagnostic
camTest                 Quickloop CAM diagnostic
portLoopbackTest        Port internal loopback diagnostics
ramRetentionTest SRAM Data Retention diagnostic
cmemRetentionTest       Central Mem Data Retention diagnostic
crossPortTest           Cross-connected port diagnostic
spinSilk                Cross-connected line-speed exerciser
diagClearError          Clear diag error on specified port
diagDisablePost         Disable Power-On-Self-Test
diagEnablePost          Enable Power-On-Self-Test
setGbicMode             Enable tests only on ports with GBICs
setSplbMode             Enable 0=Dual, 1=Single port LB mode
supportShow             Print version, error, portLog, etc.
diagShow                Print diagnostic status information
parityCheck             Dram Parity 0=Disabled,1=Enabl

Sr99:admin>
```

diagShow

The **diagShow** command prints the diagnostic results that were generated since the last restart.

Syntax

```
diagShow [nSeconds]
```

Availability

All users

Description

Use this command to print the following information generated since the last switch restart:

- State of all ports in the switch resulting from diagnostics run since the last restart. Ports that passed diagnostic testing are marked OK. Ports that failed one or more diagnostic tests are marked BAD.
- Current state of ports. Active ports are UP and inactive ports are DN.
- Frame counts for active ports - the number of frames transmitted is frTx and the number of frames received is frRx.

The “LLI_errs” is the total of the port’s 8 statistic error counters: ENC_in, CRC_err, TruncFrm, FrmTooLong, BadEOF, Enc_out, BadOrdSet, DiscC3.

- State of central memory based on the results of diagnostics run since the last restart. OK if previous centralMemoryTest executions passed; FAULTY if the switch failed the centralMemoryTest.
- Total diagnostic frames transmitted and received since the last restart. The totals represent the cumulative number of frames transmitted and received by the diagnostic functional tests (portLoopbackTest, crossPortTest,or spinSilk for the transmitted count only) for all ports since the last restart. (If the switch is restarted with POST disabled, diagShow indicates the total as 0.) The transmitted and received values may not always be the same; for example, they may not be the same if an error occurred in one of the ports during one of the tests above.

The **diagShow** command may also be run by using the s (Stats) option of the QCSL diag prompt which is generated when a diagnostic test is keyboard interrupted.

It can also be looped by specifying the nseconds operand. This operand enables you to specify a repeat interval for this command. If a repeat interval is specified the command continues to run until interrupted. For example, **diagShow 4** runs **diagShow** every four seconds unless stopped by a keyboard interrupt.

Also use this command to isolate a bad GBIC. A changing “LLI_errs” value prefixed by “**” indicates a port is continuing to detect errors.

Operands

The following operand can be used with this command:

nSeconds

Specify the repeat interval (in seconds) between executions of the **diagShow** command. If a repeat interval is specified the command continues to run until interrupted. If this operand is not used the default is to print the information once. Valid values are from 1 - 2**32. This operand is optional.

Example

```
sw7:admin> diagShow
Diagnostics Status: Wed Apr 5 03:09:20 2000
port#: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
diags: OK OK OK OK OK OK OK OK OK OK OK OK OK OK OK OK
state: UP UP UP UP UP UP UP UP UP UP UP UP UP UP UP UP
lm0:   100 frTx 100 frRx 0 LLI_errs. <looped-15>
lm1:   100 frTx 100 frRx 0 LLI_errs. <looped-11>
lm2:   100 frTx 100 frRx 0 LLI_errs. <looped-6>
lm3:   100 frTx 100 frRx 0 LLI_errs. <looped-4>
lm4:   100 frTx 100 frRx 0 LLI_errs. <looped-3>
lm5:   100 frTx 100 frRx 0 LLI_errs. <looped-8>
lm6:   100 frTx 100 frRx 0 LLI_errs. <looped-2>
lm7:   100 frTx 100 frRx 0 LLI_errs. <looped-12>
lm8:   100 frTx 100 frRx 0 LLI_errs. <looped-5>
lm9:   100 frTx 100 frRx 0 LLI_errs. <looped-14>
lm10:  100 frTx 100 frRx 0 LLI_errs. <looped-13>
lm11:  100 frTx 100 frRx 0 LLI_errs. <looped-11>
lm12:  100 frTx 100 frRx 0 LLI_errs. <looped-1>
lm13:  100 frTx 100 frRx 0 LLI_errs. <looped-10>
lm14:  100 frTx 100 frRx 0 LLI_errs. <looped-9>
lm15:  100 frTx 100 frRx 0 LLI_errs. <looped-0>
Central Memory OK
Total Diag Frames Tx: 131696
Total Diag Frames Rx: 136112
```

dlsReset

The **dlsReset** command turns off the dynamic load sharing option.

Syntax

```
dlsReset
```

Availability

Administrator

Description

Use this command to disable dynamic load sharing when a fabric change occurs. See the **dlsSet** command for a full description of load sharing.

Operands

None

Example

The following example shows turning off the dynamic load sharing option.

```
switch:admin> dlsReset
```

Note: Use this command only if the devices that are connected to the fabric cannot handle occasional routing changes.

See also

dlsSet
dlsShow

dlsSet

The **dlsSet** command turns on the dynamic load sharing option.

Syntax

```
dlsSet
```

Availability

Administrator

Description

Use this command to enable dynamic load sharing when a fabric change occurs.

Routing is done on a per source-port basis. This means that all the traffic coming in from a port (either E_port or Fx_port) that is directed to the same remote domain is routed through the same output E_port.

To optimize fabric usage, when there are multiple equivalent paths to a remote switch, traffic is shared among all the paths. Load sharing takes place when a switch restarts. In addition, if dynamic load sharing is enabled, the optimal load sharing is recomputed every time a change in the fabric occurs. A change in the fabric is defined as an E_port going up or down, or an Nx_port going up or down.

If dynamic load sharing is turned off, load sharing is performed only at startup time or when an Nx_port comes up. Optimal load sharing is rarely achieved with this setting.

Dynamic load sharing is enabled by default.

Note: When dynamic load sharing is set, routing changes can affect working ports. For example, if an Fx_port goes down, another Fx_port can be rerouted from one E_port to a different E_port. The switch minimizes the number of routing changes, but some are necessary in order to achieve optimal load sharing. These changes can affect the application, especially if the in-order delivery option is set. With the in-order delivery option (see **iodSet**), routes are not available for a few seconds after a fabric change. In addition, some frame loss can occur. No frame loss occurs if in-order delivery option is off, but there is still a short period of time when traffic is not forwarded. This period of time is significantly shorter than when in-order delivery is on, and is usually less than 1 second.

Operands

None

Example

The following example shows turning on the dynamic load sharing option.

```
switch:admin> dlsSet
```

See also

dlsReset
dlsShow
iodReset
iodSet
topologyShow
uRouteShow

dlsShow

The **dlsShow** command displays the state of the dynamic load sharing option.

Syntax

```
dlsShow
```

Availability

All users

Description

Use this command to display whether dynamic load sharing is on or off.

Operands

None

Example

```
switch:admin> dlsShow
DLS is set
```

See also

dlsSet
dlsReset

errDump

The **errDump** commands displays the error log without page breaks.

Syntax

```
errDump
```

Availability

All users

Description

Use this command to display the error log without page breaks. This command displays the same information as the **errShow** command, but **errShow** enables you to scroll through the entries using the Enter key.

See the **errShow** command for a description of the error log.

Operands

None

Example

The following example shows a log with two entries. The first entry is the most recent; it is a diagnostic failure. The second entry is the oldest; it displays the switch restart reason. See the **uptime** command for a description of restart reasons.

```
sw5:admin> errDump

Error 02
--------
0x103e9500 (tSwitch): Feb 5 16:59:09
      Error DIAG-TIMEOUT, 1, portLoopbackTest: pass 1,
      Port 1 receive timeout.
Error 01
--------
0x103e9500 (tSwitch): Feb 5 16:58:39
      Error SYS-BOOT, 3, Restart reason: Reboot
```

See also

errShow
uptime

errShow

The **errShow** command scrolls through the error log.

Syntax

```
errShow
```

Availability

All users

Description

Use this command to display the error log. This command enables you to scroll through the entries using the Enter key. Use the **errDump** command to display the same information without line breaks.

Each entry in the log follows this format:

```
Error Number
------------
taskId (taskName): Time Stamp (count)
Error Type, Error Level, Error Message
Diag Err#
```

The following is a description of the error log fields:

Error number
Beginning at one. If the number of errors exceeds the size of the log, the most recent errors are shown.

Task ID (task name)
The ID and name of the task recording the error.

Time stamp
The date and time of the first occurrence of the error.

Error count
Error count. For errors that occur multiple times, the repeat count is shown in parenthesis. The maximum count is 999.

Error type
An uppercase string showing the firmware module and error type. The switch documentation contains a detailed explanation of error types.

Error level
Error Level

0 = panic (the switch restarts)

1 = critical

2 = error

3 = warning

4 = information

5 = debug

Error message

Additional information about the error.

Diag error number

A hexadecimal 4-digit code representing the error type that is generated by a diagnostic test. The error numbers are shown in Table 17 on page 192.

Table 17. Diagnostic error numbers

Error number	Test	Error type
0001		DIAG-CLEAR_ERR
0002		DIAG-BURNIN_START
0003		DIAG-BURNIN_STOP
0004		DIAG-POST_SKIPPED
0110	ramTest	DIAG-MEMORY
0111	ramTest	DIAG-MEMSZ
0112	ramTest	DIAG-MEMNULL
040F	portRegTest	DIAG-BUS_TIMEOUT
0415	portRegTest	DIAG-REGERR
0416	portRegTest	DIAG-REGERR_UNRST
0B0F	sramRetentionTest	DIAG-BUS_TIMEOUT
0B0F	sramRetentionTest	DIAG-REGERR
0B16	sramRetentionTest	DIAG-REGERR_UNRST
1020	centralMemoryTest	DIAG-CMBISRTO
1021	centralMemoryTest	DIAG-CMBISRF
1025	centralMemoryTest	DIAG-LCMRS
1026	centralMemoryTest	DIAG-LCMTO
1027	centralMemoryTest	DIAG-LCMEM
1028	centralMemoryTest	DIAG-LCMEMT
1029	centralMemoryTest	DIAG-CMNOBUF

Table 17. Diagnostic error numbers

Error number	Test	Error type
102A	centralMemoryTest	DIAG-CMERRTYPE
102B	centralMemoryTest	DIAG-CMERRPTN
102C	centralMemoryTest	DIAG-INTNOTCLR
1030	centralMemoryTest	DIAG-BADINT
106F	centralMemoryTest	DIAG-TIMEOUT
1F25	cmemRetentionTest	DIAG-LCMRS
1F26	cmemRetentionTest	DIAG-LCMTO
1F27	cmemRetentionTest	DIAG-LCMEM
2030	cmiTest	DIAG-BADINT
2031	cmiTest	DIAG-INTNIL
2032	cmiTest	DIAG-CMISA1
2033	cmiTest	DIAG-CMINOCAP
2034	cmiTest	DIAG-CMIINVCAP
2035	cmiTest	DIAG-CMIDATA
2036	cmiTest	DIAG-CMICKSUM
223B	camTest	DIAG-CAMINIT
223C	camTest	DIAG-CAMSID
2271	camTest	DIAG-XMIT
2640	portLoopbackTest	DIAG-ERRSTAT (ENCIN)
2641	portLoopbackTest	DIAG-ERRSTAT (CRC)
2642	portLoopbackTest	DIAG-ERRSTAT (TRUNC)
2643	portLoopbackTest	DIAG-ERRSTAT (2LONG)
2644	portLoopbackTest	DIAG-ERRSTAT (BADEOF)
2645	portLoopbackTest	DIAG-ERRSTAT (ENCOUT)
2646	portLoopbackTest	DIAG-ERRSTAT (BADORD)
2647	portLoopbackTest	DIAG-ERRSTAT (DISCC3)
264F	portLoopbackTest	DIAG-INIT
265F	portLoopbackTest	DIAG-PORTDIED
2660	portLoopbackTest	DIAG-STATS (FTX)
2661	portLoopbackTest	DIAG-STATS (FRX)
2662	portLoopbackTest	DIAG-STATS (C3FRX)
266E	portLoopbackTest	DIAG-DATA

Table 17. Diagnostic error numbers

Error number	Test	Error type
266F	portLoopbackTest	DIAG-TIMEOUT
2670	portLoopbackTest	DIAG-PORTABSENT
2671	portLoopbackTest	DIAG-XMIT
3040	crossPortTest	DIAG-ERRSTAT (ENCIN)
3041	crossPortTest	DIAG-ERRSTAT (CRC)
3042	crossPortTest	DIAG-ERRSTAT (TRUNC)
3043	crossPortTest	DIAG-ERRSTAT (2LONG)
3044	crossPortTest	DIAG-ERRSTAT (BADEOF)
3045	crossPortTest	DIAG-ERRSTAT (ENCOUT)
3046	crossPortTest	DIAG-ERRSTAT (BADORD)
3047	crossPortTest	DIAG-ERRSTAT (DISCC3
304F	crossPortTest	DIAG-INIT
305F	crossPortTest	DIAG-PORTDIED
3060	crossPortTest	DIAG-STATS (FTX)
3061	crossPortTest	DIAG-STATS (FRX)
3062	crossPortTest	DIAG-STATS (C3FRX)
306E	crossPortTest	DIAG-DATA
306F	crossPortTest	DIAG-TIMEOUT
3070	crossPortTest	DIAG-PORTABSENT
3071	crossPortTest	DIAG-XMIT
3078	crossPortTest	DIAG-PORTWRONG
3840	spinSilk	DIAG-ERRSTAT (ENCIN)
3841	spinSilk	DIAG-ERRSTAT (CRC
3842	spinSilk	DIAG-ERRSTAT (TRUNC)
3843	spinSilk	DIAG-ERRSTAT (2LONG)
3844	spinSilk	DIAG-ERRSTAT (ENCOUT)
3845	spinSilk	DIAG-ERRSTAT (BADORD)
3846	spinSilk	DIAG-ERRSTAT (DISCC3)
3847	spinSilk	DIAG-INIT
384F	spinSilk	DIAG-PORTDIED
385F	spinSilk	DIAG-PORTABSENT
3870	spinSilk	DIAG-XMIT
3871	spinSilk	DIAG-XMIT
3874	spinSilk	DIAG-PORTSTOPPED

Operands

None

Example

The following example shows a log with two entries. The first entry is the most recent; it is a diagnostic failure. The second entry is the oldest; it displays the switch restart reason. See the **uptime** command for a description of restart reasons.

```
sw5:admin> errShow
Error 02
--------
0x103e9500 (tSwitch): Feb 5 16:59:09
    Error DIAG-TIMEOUT, 1, portLoopbackTest: pass 1,
    Port 1 receive timeout.
Type <CR> to continue, Q<CR> to stop:
Error 01
--------
0x103e9500 (tSwitch): Feb 5 16:58:39
    Error SYS-BOOT, 3, Restart reason: Restart
```

See also

errDump
firmwareDownload
reboot
uptime

fabricShow

The **fabricShow** command displays the fabric membership information.

Syntax

```
fabricShow
```

Availability

All users

Description

Use this command to display information about switches and multicast alias groups in the fabric. Multicast alias groups are created on demand by request from N_ports that are attached to the alias server; typically no groups are listed.

If the switch is initializing or disabled, the message `no fabric` is displayed. If the fabric is reconfiguring, some or all switches might not be shown. Otherwise, the following fields are shown:

Switch ID
The switch Domain_ID and embedded port D_ID.

World-wide name
The switch world-wide name.

Enet IP Addr
The switch Ethernet IP address.

FC IP Addr
The switch FC IP address.

Name
The switch symbolic name (“>” indicates the principal switch).

If multicast alias groups exist, the following fields are shown:

Group ID
The alias group number and D_ID.

Token
The alias group token (assigned by the N_port).

Operands

None

Example

The following example shows a fabric of four switches. “sw180” is the principal switch. Three of the switches are configured to run IP over fibre channel. There is one multicast alias group.

```
sw5:admin> fabricShow
Switch ID Worldwide Name Enet IP Addr FC IP Addr Name
-------------------------------------------------------------------------
0: fffc40 10:00:00:60:69:00:06:56 192.168.64.59 192.168.65.59 “ sw5”
1: fffc41 10:00:00:60:69:00:02:0b 192.168.64.180 192.168.65.180 “sw180”
2: fffc42 10:00:00:60:69:00:05:91 192.168.64.60 192.168.65.60 “sw60”
3: fffc43 10:00:00:60:69:10:60:1f 192.168.64.187 0.0.0.0 “sw187”
The Fabric has 4 switches
Group ID Token
-----------------
0: fffb01 40:05:00:00:10:00:00:60:69:00:00:15
```

See also

switchShow

fanShow

The **fanShow** command displays the fan status.

Syntax

```
fanShow
```

Availability

All users

Description

Use this command to display the current status of the switch fans. The format of the display varies depending on the switch model and number of fans. Some switch models show fan speed measured in RPM.

Fan status is shown as:

OK

The fan is functioning correctly.

Absent

The fan is not present.

Below minimum

The fan is present but is rotating too slowly or has stopped.

Operands

None

Example

```
sw5:admin> fanShow
Fan 1 is OK, speed is 8460 RPM
Fan 2 is OK, speed is 8220 RPM
Fan 3 is OK, speed is 8340 RPM
Fan 4 is OK, speed is 8850 RPM
```

See also

psShow
tempShow

fastboot

The **fastboot** command restarts the switch, bypassing POST.

Syntax

```
fastboot
```

Availability

Administrator

Description

Use this command to restart the switch, bypassing POST. The restart takes effect immediately as the switch resets and runs the normal start sequence. However, power-on self-test (POST) is skipped. This reduces start time significantly.

If POST has been disabled using the **diagDisablePost** command, then **fastboot** is the same as **reboot**. However, **fastboot** skips POST on the current restart, while **diagDisablePost** skips POST on all future restarts until cancelled by the **diagEnablePost** command.

While the switch is restarting, the Telnet session is closed and all fibre-channel ports are inactive. If the switch is part of a fabric, the remaining switches are reconfigured.

Operands

None

Example

The following example shows restarting the switch:

```
sw5:admin> fastboot
Rebooting...
```

See also

diagDisablePost
diagEnablePost
reboot

firmwareDownload

The **firmwareDownload** command downloads a switch firmware file from a host.

Syntax

```
firmwareDownload [“host”,“user”,“file” [,passwd]]
```

Availability

Administrator

Description

Use this command to download a switch firmware file from a host into the switch flash memory.

The download process uses either FTP (file transfer protocol) or the RSHD protocol (TCP service 514). Both of these services are widely available on UNIX hosts, but less so on Windows hosts.

On Windows NT, the FTP server might have to be installed from the distribution media and enabled. On Windows NT or Windows 9x, there are several good freeware and shareware FTP servers available. To use RSHD on Windows NT or 9x, two utilities are supplied with the firmware file, RSHD.EXE and CAT.EXE, together with instructions on how to install and run them. The FTP server or RSHD must be running before a firmware download can occur.

If the **firmwaredownload** command is invoked without operands, you are prompted for input, including the choice of FTP or RSHD. If it is invoked with three operands, RSHD is used; the addition of the fourth operand (password) selects FTP.

After the download begins, numbers are displayed (size of .text, .data, and .bss sections, and the file checksum) followed by status lines indicating the progress of the download. This display varies depending on switch model, but all displays print a period “.” per page of firmware read or written.

The following can cause the download to fail:

- The host name is not known to the switch.
- The host IP address cannot be contacted.
- The user does not have permission on the host.
- The user runs a script that prints something at login.
- The file does not exist on the host.
- The file is not a switch firmware file.

- The file is corrupted.
- The RSHD or FTP server is not running on the host.
- No host connection (Ethernet)

After a download successfully completes, the switch must be restarted to activate the new firmware.

You can also download firmware through the switch world-wide Web interface.

Operands

This command has the following operands:

“host” Specify a host name or IP address in quotation marks; for example, `“citadel”` or `“192.168.1.48”`. The configuration file is downloaded from this host system. This operand is optional.

“user” Specify a user name in quotation marks; for example, `“jdoe”`. This user name is used to gain access to the host. This operand is optional.

“file” Specify a file name in quotation marks; for example, `“firmware.txt”`. Absolute path names can be specified using the forward slash (/). Relative path names create the file in your home directory on UNIX hosts, and in the directory where the FTP server is running on Windows hosts. This operand is optional.

passwd Specify a password. If present, the command uses FTP to transfer the file. This operand is optional.

Example

```
An example download of a firmware file:
sw5:admin> firmwareDownload “citadel”,“jdoe”,“/home/jdoe/firmware”
55696+6984+133172, csum 7eca
writing flash 0 ..................
writing flash 1 ..................
download complete
```

See also

reboot
version

fspfShow

The **fspfShow** command displays FSPF protocol information.

Syntax

```
fspfShow
```

Availability

All users

Description

Use this command to display the fibre-channel shortest path first (FSPF) protocol information, and internal data structures. FSPF is implemented by a single task, called tFspf.

The display shows the following fields:

version
The version of FSPF protocol.

domainID
The domain number of the local switch.

isl_ports
The bit map of all E_ports.

minLSArrival
FSPF constant.

minLSInterval
FSPF constant.

LSoriginCount
The internal variable.

startTime
The start time of the tFspf task (milliseconds from startup).

fspfQ FSPF input message queue.

fabP The pointer-to-fabric data structure.

agingTID Ager timer ID.

agingTID Ager timeout value, in milliseconds.

lsrDlyTID
The link state record delay timer ID.

lsrDelayTo
The link state record delay timeout value, in milliseconds.

lsrDelayCount

The counter of delayed link state records.

ddb_sem

FSPF semaphore ID.

event_sch

FSPF scheduled events bit map.

lsrRefreshCnt

The internal variable.

Operands

None

Example

```
switch:admin> fspfShow
version = 2
domainID = 2
isl_ports = 0x00000002
minLSArrival = 3
minLSInterval = 5
LSoriginCount = 0
startTime = 41776
fspfQ = 0x10f79660
fabP = 0x10f9b3c0
agingTID = 0x10f6d120
agingTo = 10000
lsrDlyTID = 0x10f6ce40
lsrDelayTo = 5000
lsrDelayCount = 0
ddb_sem = 0x10f79630
fabP:event_sch= 0x0
lsrRefreshCnt = 0
```

See also

bcastShow
mcastShow
topologyShow

fwClassInit

The **fwClassInit** command initializes all classes under Fabric Watch.

Syntax

```
fwClassInit
```

Availability

Administrator

Description

Use to initialize all classes under Fabric Watch. This command should only be used after installing a Fabric Watch license, to initialize the licensed Fabric Watch classes.

Operands

None

Example

The following example shows initializing all classes under Fabric Watch:

```
sw:admin> fwClassInit
gbicRegister: re-register 0x0 0x10f6c260 fwClassInit:
Fabric Watch initialized
```

See Also

fwConfigReload

fwConfigure

fwShow

fwConfigReload

The **fwConfigReload** command reloads the Fabric Watch configuration.

Syntax

```
fwConfigReload
```

Availability

Administrator

Description

Use to reload the Fabric Watch configuration. This command should only be used after downloading a new Fabric Watch configuration file from a host.

Operands

None

Example

The following example shows reloading the Fabric Watch configuration:

```
sw:admin> fwConfigReload
fwConfigReload: Fabric Watch configuration reloaded
```

See also

configUpload

configDownload

fwClassInit

fwConfigure

fwShow

fwConfigure

The **fwConfigure** command displays and allows modification of the Fabric Watch configuration and status.

Syntax

```
fwConfigure
```

Availability

Administrator

Description

Use to allow the admin account to display and modify threshold information and the Fabric Watch configuration. Switch elements monitored by Fabric Watch are divided into classes, which are further divided into areas. In addition, each area can include from 0 to 16 thresholds. The Fabric Watch classes and areas are provided in the following list.

Fabric

- Loss of E_port
- Fabric reconfigure
- Segmentation changes
- Domain ID changes
- Zoning changes
- Fabric to QuickLoop changes
- Fabric logins
- GBIC state change

Environmental

- Temperature
- Fan
- Power supply

Port

- Link failure count
- Loss of synchronization count
- Loss of signal count
- Primitive sequence protocol error
- Invalid transmission word
- Invalid CRC count
- Receive performance

Transmit performance

State changes

E_port

Link failure count

Loss of synchronization count

Loss of signal count

Primitive sequence protocol error

Invalid transmission word

Invalid CRC count

Receive performance

Transmit performance

State changes

F/FL_port (optical)

Link failure count

Loss of synchronization count

Loss of signal count

Primitive sequence protocol error

Invalid transmission word

Invalid CRC count

Receive performance

Transmit performance

State changes

F/FL_port (copper)

Link failure count

Loss of synchronization count

Loss of signal count

Primitive sequence protocol error

Invalid transmission word

Invalid CRC count

Receive performance

Transmit performance

State changes

GBIC

Temperature

Received power

Transmitted power

Current

Operands

None

Example

The following example shows displaying the Fabric Watch configuration and status:

```
sw:admin> fwConfigure
1 : Environment class
2 : GBIC class
3 : Port class
4 : Fabric class
5 : E-Port class
6 : F/FL Port (Copper) class
7 : F/FL Port (Optical) class
8 : quit
Select a class => : (1..8) [8] 1
1 : Temperature
2 : Fan
3 : Power Supply
4 : return to previous page
Select an area => : (1..4) [4] 1
Index ThresholdName Status CurVal
LastEvent LastEventTime LastVal
LastState
================================================================
1 envTemp001 enabled 33 C
started 10:28:59 on 02/01/2000 0 C Informative
2 envTemp002 enabled 34 C
started 10:28:59 on 02/01/2000 0 C Informative
3 envTemp003 enabled 36 C
started 10:28:59 on 02/01/2000 0 C Informative
4 envTemp004 enabled 35 C
started 10:28:59 on 02/01/2000 0 C Informative
5 envTemp005 enabled 36 C
started 10:28:59 on 02/01/2000 0 C Informative
1 : refresh
2 : disable a threshold
3 : enable a threshold
4 : advanced configuration
5 : return to previous page
Select choice => : (1..5) [5]
```

See also

fwClassInit

fwConfigReload

fwShow

fwShow

The **fwShow** command displays the thresholds monitored by Fabric Watch.

Syntax

```
fwShow
```

Availability

Administrator

Description

Use to display the thresholds monitored by Fabric Watch. If no parameters are entered, a summary of all thresholds is displayed and printed. If a valid threshold name is entered as a parameter, detailed information pertaining only to that threshold is displayed and printed.

Operands

None

Example

The following example shows displaying the thresholds monitored by Fabric Watch:

```
sw:root> fwShow
===========================================================
Name Label Last Value
---------------- ------------------------ ---------------
envTemp001 Env Temperature 1 33 C
envTemp002 Env Temperature 2 33 C
envTemp003 Env Temperature 3 36 C
envTemp004 Env Temperature 4 35 C
envTemp005 Env Temperature 5 36 C
envFan001 Env Fan 1 5070 RPM
envFan002 Env Fan 2 3090 RPM
envFan003 Env Fan 3 3150 RPM
envFan004 Env Fan 4 5130 RPM
envPS002 Env Power Supply 2 0 (1 OK/0 FAULT
sw:admin> fwShow "envTemp001"
Env Temperature 1:
Monitored for: 1283 (21 mins)
Last checked: 10:50:21 on 02/01/2000
Lower bound: 0 C
Upper bound: 75 C
Buffer Size: 10
Value history: 33 C
Disabled? No
Locked? No
```

See also

fwClassInit

fwConfigReload

fwConfigure

gbicShow

The **gbicShow** command displays the serial ID GBIC information.

Syntax

```
gbicShow [port_number]
```

Availability

All users

Description

Use this command to display information about serial identification GBICs (also known as module definition “4” GBICs). These GBICs provide extended information that describes the capabilities, interfaces, manufacturer, and other information about the GBICs.

Use this command with no operand to display a summary of all GBICs in the switch. The summary shows the GBIC type (see switchShow for an explanation of the two letter codes) and, for Serial ID GBIC, the vendor name and GBIC serial number.

Use this command with a port number operand to display detailed information about the Serial ID GBIC in that port.

For Finisar “smart” GBICs, four additional fields are displayed: module temperature, received optical power, transmitted optical power (long wavelength only), and laser diode drive current.

Operands

This command has the following operand:

port_number

Specify the port number to be displayed: 0 - 7 or 0 - 15. This operand is optional.

Example

The following example shows summary information for an eight-port switch, followed by detailed information for a Finisar “smart” GBIC:

```
sw5:admin> gbicShowport 0: id Vendor: FINISAR CORP. Serial No: 103980
port 1: id Vendor: HEWLETT-PACKARD Serial No:9809100953460702
port 2: id Vendor: FINISAR CORP. Serial No: 103960
port 3: sw
port 4: sw
port 5: cu
port 6: sw
port 7: sw

sw5:admin> gbicShow 2
Identifier: 1 GBIC
Connector: 1 SC
Transceiver: 010d102202000000 100_MB/s SM M5 M6 Longwave Inter_dist

Encoding: 1 8B10B
Baud Rate: 12 (units 100 megabaud)
Length 9u: 100 (units 100 meters)
Length 50u: 55 (units 10 meters)
Length 625u: 55 (units 10 meters)
Length Cu: 0 (units 1 meter)

Vendor Name: FINISAR CORP.
Vendor OUI: 00:5a:41
Vendor PN: FTR 1319
Vendor Rev: S
Options: 001a Loss_of_Sig Tx_Fault Tx_Disable
BR Max: 0
BR Min: 0
Serial No: 103960
Date Code: 990119
Temperature: 39 Centigrade
RX Power: 0 uWatts
TX Power: 289 uWatts
Current: 15 mAmps
```

See also

switchShow

h

The **h** command displays the shell history.

Syntax

```
h
```

Availability

All users

Description

The shell history mechanism is similar to the UNIX Korn shell history facility. It has a built-in line-editor similar to UNIX vi that allows previously typed commands to be edited. The **h** command displays the 20 commands most recently typed into the shell; old commands fall off the top as new ones are entered.

To edit a command, press Esc to access edit mode, then use vi commands. The Esc key switches the shell to edit mode. The Enter key gives the line to the shell from either editing or input mode.

Basic vi commands:

k	Get the previous shell command
j	Get the next command
h	Move the cursor left
l	Move the cursor right
a	Append
i	Insert
x	Delete
u	Undo

Operands

None

Example

The following example displays the previous shell commands:

```
sw5:admin> h
1 version
2 switchShow
3 portDisable 2
4 portEnable 2
5 switchShow
```

help

The **help** command displays help information for commands.

Syntax

```
help [command]
```

Availability

All users

Description

Use this command without an operand to display an alphabetical list of all commands that provide help information. At the end of the list are additional commands that display groups of commands; for example, the **diagHelp** command displays a list of diagnostic commands.

The lists only show commands that are available to the current user; this can vary according to:

- Login user level
- License key
- Switch model

To access help information for a specific command, enter the command name as an operand.

Operands

This command has the following operand:

command
Specify the command name, with or without quotation marks.

Example

In the following example, the first line provides help information for the **login** command. The second line provides help information for the **configure** command.

```
sw5:admin> help login ...
sw5:admin> help “configure” ...
```

i

The **i** command displays the task summary.

Syntax

```
i [taskId]
```

Availability

All users

Description

Use this command to display a Synopsis of all tasks in the switch or for a specific task if a task ID is supplied. One line is displayed for each task; it contains the following fields:

NAME Task name.

ENTRY Symbol name or address where the task started running.

TID Task ID.

PRI Priority.

STATUS
Task status.

PC Program counter.

SP Stack pointer.

ERR
Most recent error code for this task.

DELAY
If the task is delayed, the number of clock ticks remaining.

The following shows the task status:

READY Task is not waiting for any resource other than the CPU.

PEND Task is blocked because a resource is unavailable.

DELAY Task is asleep for a duration.

SUSPEND
Task is unavailable for running (but not delayed or ended).

DELAY+S
Task is both delayed and suspended.

PEND+S
Task is both pended and suspended.

PEND+T

Task is pended with a timeout.

PEND+S+T

Task is pended with a time out and also suspended.

DEAD

Task no longer exists.

Operands

This command has the following operand:

taskId Specify the task name or task ID for the task to be displayed.

Example

```
sw5:admin> i tFcp

NAME       ENTRY       TID    PRI STATUS    PC        SP    ERR DELAY
---------- --------- -------- --- ------- ------- -------- ----- -
tFcp      _fcpTask   103ad660 150 PEND+T 10191b78 103ad9e0 3d0004 32

sw5:admin> i

NAME       ENTRY       TID    PRI STATUS    PC       SP     ERR DELAY
---------- ---------- -------- --- ------ -------  -------- ----- -
tExcTask  _excTask    103f7eb0   0 PEND   10191b78 103f8200 3d0001 0
tLogTask  _logTask    103f5f30   0 PEND   10191b78 103f6280      0 0
tShell    _shellTask  103b8970   1 READY  10177460 103b8be0 1c0001 0
tRlogind  _rlogind    103de0e0   2 PEND   10173e80 103de7d0      0 0
tTelnetd  _telnetd    103dc150   2 PEND   10173e80 103dc5c0      0 0
tTimers   _timerTask  103cf270  10 PEND   10191b78 103cf5f0      0 0
tErrLog   _errLogTask 103d0810  20 PEND   10191b78 103d0b90      0 0
tNetTask  _netTask    103f0370  50 READY  10174f20 103f0740      0 0
tSwitch   _switchTask 103d1db0  80 PEND+T 10191b78 103d21b0 3d0004 9
tPBmenu   _menuTask   103c8e30  90 PEND   10191b78 103c91f0      0 0
tReceive  _portRxTask 103c5690 100 PEND   10191b78 103c5a10      0 0
tTransmit _portTxTask 103c40f0 100 PEND   10191b78 103c4470      0 0
tFabric   _fabricTask 103aae20 100 PEND   10191b78 103ab1e0      0 0
tFspf     _fspfTask   103a8c70 100 PEND   10191b78 103a8ff0      0 0
tFcph     _fcphTask   103af890 120 PEND   10191b78 103afc10 3d0004 2
tFcp      _fcpTask    103ad660 150 READY  10191b78 103ad9e0 3d0004 0
tNSd      _ns_svr     10397050 150 PEND   10191b78 103973e0      0 0
tASd      _as_svr     1036f5b0 150 PEND   10191b78 1036f930      0 0
```

See also

ifModeSet
ifShow

ifModeSet

The **ifModeSet** command sets the link operating mode for a network interface.

Syntax

```
ifModeSet [“interface”]
```

Availability

Administrator

Description

Use this command to set the link operating mode for a network interface.

Use the **ifShow** command to list the network interfaces that are available on the system.

An operating mode is confirmed with a “y” or “yes” at the prompt. If the operating mode that is selected differs from the current mode, the change is saved and the command is ended.

Operands

This command has the following operand:

“interface”

Specify the name of the interface in quotation marks. For example, “`fei0`”, where `fei` is the network interface, and `0` is the physical unit.

Example

The following example forces the link for the `“fei0”` Ethernet interface from auto-negotiate operation to 10 Mbps per half duplex operation.

```
sw5:admin> ifModeSet “fei0”
Auto-negotiate (yes, y, no, n): [no]
100 Mbps / Full Duplex (yes, y, no, n): [no]
100 Mbps / Half Duplex (yes, y, no, n): [no]
10 Mbps / Full Duplex (yes, y, no, n): [no]
10 Mbps / Half Duplex (yes, y, no, n): [no] yes
Committing configuration...done.
```

See also

ifModeShow
ifShow

Notes

The system must be restarted for changes to take effect.

Changing the link mode is not supported for all network interfaces or for all Ethernet network interfaces. Currently, this command is only functional for “fei” interfaces.

Exercise care when using this command. Forcing the link to an operating mode that is not supported by the network equipment to which it is attached can result in an inability to communicate with the system through its Ethernet interface.

ifModeShow

The **ifModeShow** command displays the link operating mode for a network interface.

Syntax

```
ifModeShow [“interface”]
```

Availability

All users

Description

Use this command to display the link operating mode for a network interface.

Operands

This command has the following operand:

“interface”

Specify the name of the interface in quotation marks. For example, `“fei0”`, where `fei` is the network interface and `0` is the physical unit.

Example

The following example displays the link operating mode for the “fei0” Ethernet interface.

```
sw5:admin> ifModeShow “fei0”
fei (unit number 0):
Link mode: Auto-negotiate
```

See also

ifModeSet
ifShow

ifShow

The **ifShow** command displays the network interface information.

Syntax

```
ifShow [“ifName”]
```

Availability

All users

Description

Use this command to display network interface status. If the `ifName` operand is provided, only that interface is displayed. If `ifName` is omitted, all interfaces are displayed.

Each switch has three interfaces:

- “ei” or “fei” is the 10BASE-T or 100BASE-T Ethernet interface
- “lo” is the loopback interface
- “fc” is the fibre-channel interface

The “fc” interface is displayed for switches running IP over fibre channel that have been assigned an FC-IP address.

For each interface that is selected, the following information is displayed:

- Flags (for example, loopback, broadcast, arp, running, debug)
- Internet address
- Broadcast address
- Netmask and subnetmask
- Ethernet address
- Route metric
- Maximum transfer unit
- Number of packets received and sent
- Number of input errors, output errors, and collisions

Operands

This command has the following operand:

“**ifName”**

Specify the name of an interface, in quotation marks. This operand is optional.

Example

The following example shows Ethernet interface information for a switch with a 10BASE-T connection:

```
sw5:admin> ifShow “ei”
ei (unit number 0):
Flags: (0x63) UP BROADCAST ARP RUNNING
Internet address: 192.168.1.65
Broadcast address: 192.168.1.255
Netmask 0xffffff00 Subnetmask 0xffffff00
Ethernet address is 00:60:69:00:00:8a
Metric is 0
Maximum Transfer Unit size is 1500
42962 packets received; 127 packets sent
0 input errors; 0 output errors
7 collisions
```

See also

ipAddrSet
ipAddrShow

interfaceShow

The **interfaceShow** command displays the FSPF interface information.

Syntax

```
interfaceShow [port_number]
```

Availability

All users

Description

Use this command to display data structures that are associated with FSPF interfaces (E_ports) on the switch.

There are two data structures: the permanently allocated interface descriptor block (IDB) and the neighbor data structure that is allocated when a switch port becomes an E_port. The neighbor data structure contains all the information relating to the switch that is connected to a local interface, also known as the adjacent switch. The **interfaceShow** command displays the content of both data structures, if they have been allocated.

Used without specifying the port number, this command displays the interface information for all ports on the switch (including non-E_ports).

The following fields are displayed:

idbP Pointer to IDB.

nghbP Pointer to neighbor data structure.

ifNo Interface number.

cost Cost of sending a frame over the ISL connected to this interface. The value 1000 indicates a 1 Gbps link.

delay Conventional delay incurred by a frame that is transmitted on this ISL. A fixed value that is required by the FSPF protocol.

lastScn Type of the last state change notification received on this interface.

lastScnTime
Time the last state change notification was received on this interface.

upCount Number of times this interface came up, with respect to FSPF.

lastUpTime
Last time this interface came up.

downCount
Number of times this interface failed.

lastDownTime
Last time this interface failed.

downReason
Type of last state change notification that caused this interface to fail.

iState Current state of this interface. The state can be UP or DOWN. An interface in DOWN state does not have an allocated neighbor data structure and cannot be used to route traffic to other switches.

state Current state of this interface. This E_port is used to route traffic to other switches only if the state is ‘NB_ST_FULL’.

nghbCap
Neighbor capabilities. Should be 0.

nghbId
Domain ID of the neighbor (adjacent) switch.

idbNo
IDB number. Should be equal to port_number.

remPort Port number on the remote switch connected to this port.

nflags Internal FSPF flags.

initCount
Number of times this neighbor was initialized, without the interface going down.

dbRetransList
Pointer to the database retransmission list.

lsrRetransList
Pointer to the link state records (LSR) retransmission list.

lsrAckList
Pointer to the link state acknowledgements (LSA) retransmission list.

inactTID
Inactivity timer ID.

helloTID
Hello timer ID.

dbRtxTID
Database retransmission timer ID.

lsrRtxTID
LSR retransmission timer ID.

inactTo

Inactivity timeout value, in milliseconds. When this timeout expires, the adjacency with the neighbor switch is broken and new paths are computed to all possible destination switches in the fabric.

helloTo

Hello timeout value, in milliseconds. When this timeout expires, a Hello frame is sent to the neighbor switch through this port.

rXmitTo

Retransmission timeout value, in milliseconds. It is used to transmit topology information to the neighbor switch. If no acknowledgement is received within rXmitTo, the frame is retransmitted.

nCmdAcc

Total number of commands accepted from the neighbor switch. Number includes hellos, link state updates (LSU), and link state acknowledgements.

nInvCmd

Number of invalid commands received from the neighbor switch. Usually commands with an FSPF version number higher than the one running on the local switch.

nHloIn

Number of hello frames received from the neighbor switch.

nInvHlo

Number of invalid hello frames (hello frames with invalid parameters) received from the neighbor switch.

nLsuIn

Number of LSUs received from the neighbor switch.

nLsaIn

Number of LSAs received from the neighbor switch.

attHloOut

Number of attempted transmissions of hello frames to the neighbor switch.

nHloOut

Number of hello frames transmitted to the neighbor switch.

attLsuOut

Number of attempted transmissions of LSUs to the neighbor switch.

nLsuOut

Number of LSUs transmitted to the neighbor switch.

attLsaOut

Number of attempted transmissions of LSAs to the neighbor switch.

nLsaOut

Number of LSAs transmitted to the neighbor switch.

Operands

This command has the following operand:

port_number

Specify the port number you want to display the interface data structures for.

Example

```
switch:admin> interfaceShow 4
idbP = 0x10f61f40
Interface 4 data structure:

nghbP           = 0x10f61d90
ifNo            = 4
cost            = 1000
delay           = 1
lastScn         = 5
lastScnTime     = Mar 29 12:57:52.833
upCount         = 2
lastUpTime      = Mar 29 12:57:52.833
downCount       = 1
lastDownTime    = Mar 29 12:57:47.566
downReaso       = 2
iState          = UP
Type <CR> to continue, Q<CR> to stop:

Neighbor 4 data structure:
state           = NB_ST_FULL
nghbCap         = 0x0
nghbId          = 2
idbNo           = 4
remPort         = 1
nflags          = 0x3
initCount       = 1
dbRetransList   = 0x10f61db0
lsrRetransList  = 0x10f61dc0
lsrAckList      = 0x10f61dd0
inactTID        = 0x10f61d40
helloTID        = 0x10f61cf0
dbRtxTID        = 0x10f61ca0
lsrRtxTID       = 0x10f61c50
inactTo         = 80000
helloTo         = 20000
rXmitTo         = 5000
nCmdAcc         = 11464
nInvCmd         = 0
nHloIn          = 11209
nInvHlo         = 0
nLsuIn          = 128
nLsaIn          = 127
attHloOut       = 11209
nHloOut         = 11209
attLsuOut       = 128
nLsuOut         = 128
attLsaOut       = 128
nLsaOut         = 128
```

See also

portShow
switchShow

iodReset

The **iodReset** command turns off the in-order delivery option.

Syntax

```
iodReset
```

Availability

Administrator

Description

Use this command to allow out-of-order delivery of frames during fabric topology changes.

This is the default behavior, and allows fast rerouting after a fabric topology change.

Operands

None

Example

The following example shows turning off the in-order delivery options:

```
switch:admin> iodReset
```

See also

iodSet

iodSet

The **iodSet** command turns on the in-order delivery option.

Syntax

```
iodSet
```

Availability

Administrator

Description

Use this command to enforce in-order delivery of frames during a fabric topology change.

In a stable fabric, frames are always delivered in order, even when the traffic between switches is shared among multiple paths. However, when topology changes occur in the fabric (for instance, a link goes down), traffic is rerouted around the failure. Generally, when topology changes occur, some frames are delivered out-of-order. This command ensures that frames are not delivered out-of-order, even during fabric topology changes.

The default is for the in-order delivery option to be off.

The **iodSet** command should be used with care, because it can cause a delay in establishing a new path when a topology change occurs. Use this command only if there are devices connected to the fabric that do not tolerate occasional out-of-order delivery of frames.

Operands

None

Example

The following example shows turning on the in-order delivery option:

```
switch:admin> iodSet
```

See also

iodReset
iodShow

iodShow

The **iodShow** command displays the state of the in-order delivery option.

Syntax

```
iodShow
```

Availability

All users

Description

Use this command to display whether the in-order delivery option is on or off.

Operands

None

Example

```
switch:admin> iodShow
IOD is not set
```

See also

iodSet
iodReset

ipAddrSet

The **ipAddrSet** command sets the Ethernet and FC-IP addresses.

Syntax

```
ipAddrSet
```

Availability

Administrator

Description

Use this command to set Ethernet and FC-IP addresses. You are prompted for:

Ethernet IP Address

The IP address of the Ethernet port.

Ethernet Subnetmask

The IP subnetmask of the Ethernet port.

Fibre Channel IP Address

The IP address of the fibre-channel ports.

Fibre Channel Subnetmask

The IP subnetmask of the fibre-channel ports.

Gateway Address

The IP address of the gateway.

After each prompt the current value is shown. You can:

- Press Enter to retain the current value
- Enter an IP address in conventional dot (‘.’) notation
- Enter none
- Press Ctrl+C to cancel changes
- Press Ctrl+D to accept changes and end input

The final prompt allows you to set the new IP addresses immediately. Type y to set new addresses immediately; type `n` to delay the changes until the next switch restart. (Typing y closes the Telnet session.)

A change to these values issues a domain address format RSCN (see FC-FLA for a description of RSCNs).

Operands

None

Example

The following example shows enabling IP over fibre channel:

```
sw5:admin> ipAddrSet
Ethernet IP Address [192.168.1.65]:
Ethernet Subnetmask [none]:
Fibre Channel IP Address [none]: 192.168.65.65
Fibre Channel Subnetmask [none]:
Gateway Address [192.168.1.1]:
Committing configuration...done.
Set IP addresses now?
[y = set now, n = next reboot]: y
```

See also

ifShow
ipAddrShow

ipAddrShow

The **ipAddrShow** command displays the Ethernet and FC IP addresses.

Syntax

```
ipAddrShow
```

Availability

All users

Description

Use this command to display the Ethernet and fibre-channel IP addresses. The following are shown:

Ethernet IP address

The IP address of the Ethernet port.

Ethernet subnetmask

The IP subnetmask of the Ethernet port.

Fibre-channel IP address

The IP address of the fibre-channel ports.

Fibre-channel subnetmask

The IP subnetmask of the fibre-channel ports.

Gateway address

The IP address of the gateway.

EIP addresses are displayed in conventional dot (".") notation. All fibre-channel ports on a switch have the same IP address and subnetmask. The fibre-channel IP address displays `none` if the switch is not configured to run IP over fibre-channel.

Operands

None

Example

The following example shows displaying the switch IP addresses:

```
sw5:admin> ipAddrShow
Ethernet IP Address: 192.168.1.65
Ethernet Subnetmask: none
Fibre Channel IP Address: 192.168.65.65
Fibre Channel Subnetmask: none
Gateway Address: 192.168.1.1
```

See also

ifShow
ipAddrSet

licenseAdd

The **licenseAdd** command adds a license key to the switch.

Syntax

```
licenseAdd “license”
```

Availability

Administrator

Description

Use this command to add a license key to a switch. The license key string is case sensitive; it must be entered exactly as issued.

When the key has been entered, use the **licenseShow** command to check that the key has been correctly entered and the licensed product is installed. Once the key has been installed, the product is immediately available.

Note: A QuickLoop only switch (2109 switch) must be restarted after adding a fabric license.

Operands

This command has the following operand:

“license”

Specify the license key, in quotation marks. This operand is required.

Example

The following example shows adding a license key to the switch:

```
sw5:admin> licenseAdd “bQebzbRdScRfc0iK”
adding license key “bQebzbRdScRfc0iK”
Committing configuration...done.
```

See also

licenseRemove
licenseShow

licenseHelp

The **licenseHelp** command displays the commands that are used to administer license keys.

Syntax

```
licenseHelp
```

Availability

Administrator

Description

Use this command to display the commands that are available to administer license keys. Each switch can save one license key to enable one or more optionally licensed products. This license key is unique for each switch.

Operands

None

Example

```
switch:admin> licenseHelp
licenseAdd Add a license key to this switch
licenseRemove Remove a license key from this switch
licenseShow Show current license key
```

licenseRemove

The **licenseRemove** command removes the license key from a switch.

Syntax

```
licenseRemove “license”
```

Availability

Administrator

Description

Use this command to remove an existing license key from a switch. The existing license key is case-sensitive and must be entered exactly as shown by the **licenseShow** command.

When the key has been entered, use the **licenseShow** command to check that the key has been removed and the licensed product uninstalled. Once the license key has been removed, the switch must be restarted.

With no license keys installed, **licenseShow** displays `“No licenses”`.

Operands

The following operand is required:

“license”
Specify the license key, in quotation marks. This operand is required.

Example

The following example shows removing a license key from the switch:

```
sw5:admin> licenseRemove “bQebzbRdScRfc0iK”
removing license key “bQebzbRdScRfc0iK”
Committing configuration...done.
```

See also

licenseAdd
licenseShow

licenseShow

The **licenseShow** command displays the current license keys.

Syntax

```
licenseShow
```

Availability

All users

Description

Use this command to display the current license keys along with a list of the licensed products that are enabled by these keys; `none` is displayed if no license keys are installed.

Operands

None

Example

In the following example, the switch has two keys, the first key enables two licensed products and the second key enables a third:

```
sw5:admin> licenseShow
bQebzbRdScRfc0iK:
   Web license
   Zoning license
SybbzQQ9edTzcc0X:
   Fabric license
```

See also

licenseAdd
licenseRemove

linkCost

The **linkCost** command sets or prints the FSPF cost of a link.

Syntax

```
linkCost [port_number], [cost]
```

Availability

Administrator

Description

Use this command to set or display the cost of an inter-switch link (ISL). The cost of a link is a dimensionless positive number. It is used by the FSPF path selection protocol to determine the path that a frame takes going from the source to the destination switch. The chosen path is the path with minimum cost. The cost of a path is the sum of the costs of all the ISLs traversed by the path. The cost of a path is also known as the *metric*.

FSPF supports load sharing over a number of equal cost paths.

Every ISL has a default cost that is inversely proportional to the bandwidth of the ISL. For a 1 Gbps ISL, the default cost is 1000.

The **linkCost** command changes the actual link cost only, it does not affect the default cost. The **interfaceShow** command displays both the default and the actual cost.

Without operands, this command displays the actual cost of all the ISLs. With one operand, it displays the actual cost of a specific ISL. With two operands, it sets the cost of a specific ISL.

Operands

This command has the following operands:

port_number

Specify the interface cost to be set or printed.

cost

Specify the new cost of the link connected to the interface port_number.

Example

```
switch:admin> linkCost 1
Interface: 1 cost 1000
switch:admin> linkCost 1,2000
Committing configuration...done.
switch:admin> linkCost 1
Interface: 1cost 2000
```

See also

interfaceShow
LSDbShow
topologyShow
uRouteShow

login

The **login** command logs in as a new user.

Syntax

```
login
```

Availability

All users

Description

Use this command to log in to the switch with another user name and password, without first logging out from the original session. If the user was originally connected using a Telnet or login session, that session is left open.

This command allows you to access commands that you cannot access at your current user level.

Operands

None

Example

The following example shows changing the login from “user” to “admin”:

```
sw5:user> login
login: admin
Password:
sw5:admin>
```

See also

logout

logout

The **logout** command lets you log out from a Telnet, login, or serial port session.

Syntax

```
logout
```

Availability

All users

Description

Use this command to logout from a Telnet, login, or serial port session. Telnet and login connections are closed, the serial port returns to the `“login:”` prompt.

The **exit** and **quit** commands are accepted as synonyms for **logout**, as is Ctrl+D entered at the beginning of a line.

Operands

None

Example

The following example shows logging out from a login session:

```
sw5:admin> logout
Connection closed.
```

See also

login

loopdiagClear

The **loopdiagClear** command clears information from management layers.

Syntax

```
loopdiagClear port
```

Availability

Administrator

Description

This command cleans any residual information from a previous failed session in management layer. It releases all the resources that were created for the specified port.

Operands

This command has the following operand:

port The physical port number where the loopdiag runs. This operand is required.

Example

The followig example shows completing loopdiag at port 5:

```
switch:admin> loopdiagClear 5
```

See also

loopdiagDone

loopdiagStart

loopdiagStop

loopdiagDone

The **loopdiagDone** command completes the loopdiag application.

Syntax

```
loopdiagDone port
```

Availability

Administrator

Description

This command completes the loopdiag application at the port specified. It releases all the resources that were created for loopdiag and sets the port online before resetting the loop.

Operands

This command has the following operands:

port The physical port number where loopdiag runs. This operand is required.

Example

The following example shows completing loopdiag at port 5:

```
switch:admin> loopdiagDone 5
```

See also

loopdiagClear

loopdiagStart

loopdiagStop

LSDbShow

The **LSDbShow** command displays the FSPF link state database (LSD).

Syntax

```
LSDbShow [domain_number]
```

Availability

All users

Description

Use this command to display a link state database record for switches in the fabric. There are two data structures, the permanently allocated link state database entry and the link state record (LSR) that is allocated when a switch is connected to the fabric. The LSR for domain ‘n’ describes the links between the switch with domain number ‘n’ and its neighbor switches. For a link to be reported in the LSR, the neighbor for that link must be in NB_ST_FULL state.

This command displays the content of both data structures, if the LSR is present.

Without operands, this command displays the whole link state database.

The display shows the following fields:

Domain The domain number described by this LSR. A (self) keyword after the domain number indicates LSR describes the local switch.

lsrP The pointer to LSR.

earlyAccLSRs
The number of LSRs accepted even though they were not sufficiently spaced apart.

ignoredLSRs
The number of LSRs not accepted because they were not sufficiently spaced apart.

lastIgnored
The last time an LSR was ignored.

installTime
The time this LSR was installed in the database, in seconds, since a restart.

lseFlags Internal variable.

uOutIfs Internal variable.

uPathCost
Internal variable.

uHopsFromRoot
Internal variable.

mOutIfs Internal variable.

parent Internal variable.

mPathCost
Internal variable.

mHopsFromRoot
Internal variable.

lsAge The age, in seconds, of this LSR. An LSR is removed from the database when its age exceeds 3600 seconds.

reserved Reserved for future use.

type The type of the LSR. Always 1.

options Always 0.

lsId The ID of this LSR. It is identical to the domain number.

advertiser
The ID (domain number) of the switch that originated this LSR.

incarn The incarnation number of this LSR.

length The total length (in bytes) of this LSR. Includes header and link state information for all links.

chksum The checksum of total LSR, with exception of lsAge field.

linkCnt The number of links in this LSR. Each link represents a neighbor in NB_ST_FULL state.

flags Always 0.

LinkId The ID of this link. It is the domain number of the switch on the other side of the link.

out port The port number on the local switch.

rem port The port number of the port on the other side of the link.

cost The cost of this link. The default cost for a 1 Gbps link is 1000.

costCnt Always 0.

type Always 1.

Operands

This command has the following operand:

domain_number

Specify the domain number of the LSR to be displayed.

Example

The following example shows displaying the link state record for the local switch, as indicated by (self) keyword. The local switch has four links in NB_ST_FULL state; three of them connected to switch 5, and one connected to switch 4.

```
switch:admin> LSDbShow
Domain     = 7 (self), Link State Database Entry pointer = 0x103946a0

lsrP          = 0x1035bb30
earlyAccLSRs  = 1
ignoredLSRs   = 0
lastIgnored   = Never
installTime   = 0x4f20a (324106)
lseFlags      = 0xa
uOutIfs       = 0x0
uPathCost = 0
uHopsFromRoot = 0
mOutIfs = 0x20
parent = 0x4
mPathCost = 2000
mHopsFromRoot = 2
Link State Record:
Link State Record pointer = 0x1035bb30
lsAge = 138
reserved = 0
type = 1
options = 0x0
lsId = 7
advertiser = 7
incarn = 0x80000217
length = 92
chksum = 0x2fdd
linkCnt = 4, flags = 0x0
LinkId = 4, out port = 3, rem port = 2, cost = 1000, costCnt = 0, type = 1
LinkId = 5, out port = 5, rem port = 5, cost = 1000, costCnt = 0, type = 1
LinkId = 5, out port = 6, rem port = 3, cost = 1000, costCnt = 0, type = 1
LinkId = 5, out port = 7, rem port = 4, cost = 1000, costCnt = 0, type = 1
```

See also

interfaceShow
nbrStateShow

mcastShow

The **mcastShow** command displays multicast routing information.

Syntax

```
mcastShow [group_ID]
```

Availability

All users

Description

Use this command to display the multicast routing information, as it is known by the FSPF path selection/routing task, for all ports in the switch. For each multicast group, the multicast routing information indicates all the ports that are members of that group (that is, ports that are able to send and receive multicast frames on that group).

The multicast routing information is shown for all the multicast groups, or for a specific group if a group ID is supplied.

Normally, an F_port or FL_port is a member of the multicast group only if it has joined the group using the alias server protocol. On the other hand, E_ports that are part of the multicast group are selected by the multicast path selection protocol. They are chosen in a way that prevents multicast routing loops.

The multicast paths are active for all the multicast groups at all times, regardless of whether a multicast group contains any members.

The multicast routing information is shown as a set of bit maps. Each bit in the bit map represents a port, with the least significant bit representing port 0. A bit set to 1 indicates that a port is part of the multicast distribution tree.

The following fields are displayed:

Group The multicast group ID.

Member ports
The bit map of all ports in the multicast tree for that multicast group.

Member ISL ports
The bit map of all E_ports in the multicast tree for that multicast group.

Static ISL ports
Reserved. It should be all zeroes.

Operands

This command has the following operand:

group_ID

Specify the multicast group to be displayed.

Example

```
switch:admin> mcastShow 9
Group Member Ports Member ISL Ports Static ISL Ports
---------------------------------------------------------
9     0x00002083   0x00002080       0x00000000
```

See also

bcastShow
portRouteShow

msConfigure

The **msConfigure** command configures the management server.

Syntax

```
msConfigure
```

Availability

Administrator

Description

Use this command to configure parameters that are used to access the management server. The management server allows a storage area network (SAN) management application to retrieve and administer fabric and interconnect elements such as switches. It is located at the fibre-channel address FFFFFAh.

If the management server access control list (ACL) is empty (default), the management server is accessible to all systems that are connected in-band to the fabric. To restrict access, specify the world-wide name (WWN) for one or more management applications; access is then restricted to those WWNs.

The ACL is implemented on a per-switch basis and should be configured on the switch to which the management application station is directly connected.

This command is interactive and provides the following choices:

0 Done (with the administration)

1 Display the access list (ACL)

2 Add member based on its port or node WWN

3 Delete member based on its port or node WWN

If a change is made, you are prompted to save the changed ACL to the flash memory. The saved ACL is restored on future restart.

Operands

None

Example

```
sw5:admin> msConfigure
0            Done
1            Display the access list
2            Add member based on its Port/Node WWN
3            Delete member based on its Port/Node WWN
select : (0..3) [1]
MS Access List consists of (5): {
20:01:00:60:69:00:60:10
20:02:00:60:69:00:60:10
20:03:00:60:69:00:60:10
20:02:00:60:69:00:60:03
20:02:00:60:69:00:60:15
}
0            Done
1            Display the access list
2            Add member based on its Port/Node WWN
3            Delete member based on its Port/Node WWN
select : (0..3) [1] 0
done ...
sw5>
```

msPlatShow

The **msPlatShow** command displays the Management Server Platform database.

Syntax

```
msPlatShow
```

Availability

Administrator

Description

Use this command to display the Management Server Platform database. It displays the platform name and the attributes that are associated with each platform object in the database.

Platform database management is available in firmware v2.3 and above. Lower level firmware releases do not support platform database management.

Operands

None

Example

The following example displays the Management Server Platform database for a fabric:

```
switch:admin> msPlatShow
-------------------------------------------------------
Platform Name: [9] "first obj"
Platform Type: 5 : GATEWAY
Number of Associated M.A.: 1
Associated Management Addresses:
[35] "http://java.sun.com/products/plugin"
Number of Associated Node Names: 1
Associated Node Names:
10:00:00:60:69:20:15:71
-------------------------------------------------------
Platform Name: [10] "second obj"
Platform Type: 7 : HOST_BUS_ADAPTER
Number of Associated M.A.: 1
Associated Management Addresses:
[30] "http://java.sun.com/products/1"
Number of Associated Node Names: 2
Associated Node Names:
10:00:00:60:69:20:15:79
10:00:00:60:69:20:15:75
```

See also

msPlCapabilityShow

msPlMgmtActivate

msPlMgmtDeactivate

msPlClearDB

msPlCapabilityShow

The **msPlCapabilityShow** command displays the platform database management capability.

Syntax

```
msPlCapabilityShow
```

Availability

Administrator

Description

Use this command to query a fabric for the platform database management capability. Based on the result of this command, you can decide if you can activate platform database management on all switches in the fabric.

When this command is issued, information is gathered from every switch of the fabric and the ability of each switch to handle the platform database management is displayed.

Platform database management is available in firmware v2.3 and above. Lower level firmware releases do not support platform database management.

Operands

None

Example

The following example shows displaying the platform database management capability on a fabric:

```
switch:admin> msPlCapabilityShow
Platform
Switch WWN Service Capable Capability Name
======================= ============== ==========
=======
10:00:00:60:69:20:15:71 Yes 0X0000000B "swd156"
10:00:00:60:69:00:30:05 Yes 0X0000000B "swd158"
Capability Bit Definitions:
Bit 0: Basic Configuration Service Supported.
Bit 1: Platform Management Service Supported.
Bit 2: Topology Discovery Service Supported.
Bit 3: Unzoned Name Server Service Supported.
Bit 4: M.S. Fabric Zone Service Supported.
Bit 5: Fabric Lock Service Supported.
Others: Reserved.
Done.
```

See also

msPlMgmtActivate

msPlMgmtDeactivate

msPlatShow

msPlClearDB

msPlClearDB

The **msPlClearDB** command clears the Management Server Platform database on all switches in the fabric.

Syntax

```
msPlClearDB
```

Availability

Administrator

Description

Use this command to clear the entire management server platform database on all switches in the fabric. Because this operation is nonrecoverable (that is, after the command is issued, the database is erased), it should not be used unless it is intended to resolve a database conflict between two joining fabrics or to establish an entire new fabric with an empty database.

Platform database management is available in firmware v2.3 and above. Lower level firmware releases do not support platform database management.

Operands

None

Example

The following example shows clearing the Management Server Platform database on all switches in the fabric:

```
switch:admin> msPlClearDB
Fabric-wise Platform DB Delete operation in progress...
switch:admin>Done...
```

See also

msPlMgmtDeactivate

msPlatShow

msPlCapabilityShow

msPlMgmtActivate

The **msPlMgmtActivate** command displays the network interface information and activates platform database management on all switches in the fabric.

Syntax

```
msPlMgmtActivate
```

Availability

Administrator

Description

Use this command to activate Management Server platform database management on all switches in the fabric. IBM recommends that the you run the **msPlCapabilityShow** command before issuing this command. If any switch within the fabric is not capable of handling platform database management, this command is rejected. When the **msPlMgmtActivate** command is issued, all the switches in the fabric have platform database management enabled.

The activation is saved to the nonvolatile storage of each switch, so that even after a reboot, a switch will boot up with Platform Management service enabled. By default, the Platform Management service is disabled.

Platform database management is available in firmware v2.3 and above. Lower level firmware releases do not support platform database management.

Operands

None

Example

The following example shows activating platform database management on all switches in the fabric:

```
switch:admin> msPlMgmtActivate
Request Fabric to activate Platform Management
services.... Done.
switch:admin>
```

See also

msPlMgmtDeactivate

msPlatShow

msPlCapabilityShow

msPlClearDB

msPlMgmtDeactivate

The **msPlMgmtDeactivate** command deactivates platform database management on all switches in the fabric.

Syntax

```
msPlMgmtDeactivate
```

Availability

Administration

Description

Use this command to deactivate the platform database management. This command deactivates platform database management from each switch in the fabric and commits the changes to the nonvolatile storage of each switch.

After platform database management is deactivated, even in the event of a restart, the switch will initialize with the service disabled.

By default, platform database management is disabled.

Platform database management is available in firmware v2.3 and above. Lower level firmware releases do not support platform database management.

Operands

None

Example

The following example shows deactivating the platform database management on all switches in the fabric:

```
switch:admin> msPlMgmtDeactivate
Request Fabric to Deactivate Platform Management
services....
Done.
switch:admin>
```

See also

msPlatShow

msPlCapabilityShow

msPlMgmtActivate

msPlClearDB

nbrStatsClear

The **nbrStatsClear** command resets the FSPF interface counters.

Syntax

```
nbrStateShow [port_number]
```

Availability

All users

Description

Use this command to reset the counters of FSPF frames that are transmitted and received on an interface.

Use this command with no operand to reset the counters on all interfaces.

Operands

This command has the following operand:

port_number
Specify the port number for the counters to be reset.

Example

```
switch:admin> nbrStatsClear 4
switch:admin> interfaceShow 4
idbP                  = 0x10f61f40
Interface 4 data structure:
nghbP                 = 0x10f61d90
ifNo                  = 4
defaultCost           = 1000
cost                  = 1000
delay                 = = 1
lastScn               = 5
lastScnTime           = Mar 29 12:57:52.833
upCount               = 2
lastUpTime            = Mar 29 12:57:52.833
downCount             = 1
lastDownTime          = Mar 29 12:57:47.566
downReason            = 2
iState                = UP
Type <CR> to continue, Q<CR> to stop:
Neighbor 4 data structure:
state                 = NB_ST_FULL
lastTransition        = Mar 29 12:57:52.865
nghbCap               = 0x0
nghbId                = 2
idbNo                 = 4
remPort               = 1
nflags                = 0x3
initCount             = 1
lastInit              = Mar 29 12:57:52.849
&dbRetransList        = 0x10f61db0
&lsrRetransList       = 0x10f61dc0
&lsrAckList           = 0x10f61dd0
inactTID              = 0x10f61d40
helloTID              = 0x10f61cf0
dbRtxTID              = 0x10f61ca0
lsrRtxTID             = 0x10f61c50
inactTo               = 80000
helloTo               = 20000
rXmitTo               = 5000
nCmdAcc               = 0
nInvCmd               = 0
nHloIn                = 0
nInvHlo               = 0
nLsuIn                = 0
nLsaIn                = 0
attHloOut             = 0
nHloOut                 = 0
attLsuOut               = 0
nLsuOut                 = 0
attLsaOut               = 0
nLsaOut                 = 0
```

See also

interfaceShow
portShow
switchShow

nbrStateShow

The **nbrStateShow** command displays the state of the FSPF neighbor.

Syntax

```
nbrStateShow [port_number]
```

Availability

All users

Description

Use this command to display information about neighbors to the local switch, or information about a specific neighbor if a port number is supplied. A neighbor is a switch that is directly attached to the local switch.

The display shows the following fields:

Local port
The domain number of the remote switch.

Local domain ID
E_port (interface) on the local switch.

Domain The domain number of the local switch.

Remote port
The state of the neighbor. The E_port is used to route frames only if the neighbor is in NB_ST_FULL state.

Operands

This command has the following operand.

port_number
Specify the port on the local switch that connects to the neighbor being displayed.

Example

The following example shows how to display information about switches directly connected to the local switch:

```
switch:admin> nbrStateShow
Local Domain ID: 15
Local Port   Domain    Remote Port State
---------------------------------------------------
2            13        13          NB_ST_FULL
6            13         9          NB_ST_FULL
7            13         8          NB_ST_FULL
13            3         7          NB_ST_FULL
```

See also

interfaceShow

nsAllShow

The **nsAllShow** command displays global name server information.

Syntax

```
nsAllShow [type]
```

Availability

All users

Description

Use this command to display the 24-bit fibre-channel addresses of all devices in all switches in the fabric. If the operand `type` is supplied, only devices of the specified FC-PH type are displayed. If `type` is omitted, all devices are displayed.

Operands

This command has the following operand:

type

Specify the FC-PH type code.

Example

The following example shows displaying all devices in the fabric, followed by all type 8 (SCSI-FCP) devices.

```
sw5:admin> nsAllShow
     12 Nx_Ports in the Fabric {
     011000 011200 0118e2 0118e4 0118e8 0118ef 021200 021300
     0214e2 0214e4 0214e8 0214ef
               }
sw5:admin> nsAllShow 8
     8 FCP Ports {
     0118e2 0118e4 0118e8 0118ef 0214e2 0214e4 0214e8 0214ef
      }
sw5:admin> nsAllShow 5
      2 FC-IP Ports in the Fabric {
      011200 021200}
```

See also

nsShow
switchShow

nsShow

The **nsShow** command displays the local name server information.

Syntax

```
nsShow
```

Availability

All users

Description

Use this command to display the local name serve information, including information about devices that are connected to this switch, and cached information about devices that are connected to other switches in the fabric.

The following message is displayed if there is no information in this switch:

```
There is no entry in the Local Name Server
```

There still can be devices connected to other switches in the fabric. The **nsAllShow** command displays information from all switches.

The display shows the following fields:

***** Indicates a cached entry from another switch.

Type `U` for unknown, `N` for N_port, `NL` for NL_port.

Pid 14-bit fibre-channel address.

COS The list of classes of service supported by the device.

PortName
The device port world-wide name.

NodeName
The device node world-wide name.

TTL (sec) Time-to-live (in seconds) for cached entries, or `na` (not applicable) if the entry is local.

There can be additional lines in the display if the device has registered any of the following information (the switch automatically registers SCSI inquiry data for FCP target devices):

- FC4s supported
- IP address
- IPA

- Port and node symbolic names
- Fabric port name
- Hard address and/or the port IP address

Operands

None

Example

The following example shows displaying one cached entry and 6 local entries: two local entries support FC-IP and four support SCSI-FCP:

```
    sw5:admin> nsShow
The Local Name Server has 7 entries {
Type Pid    COS  PortName        NodeName                TTL(sec)

*N   011200;  2,3;10:00:00:60:69:00:ab:ba;10:00:00:60:69:00:ab:ba;60

    FC4s: FCIP
N    021200;  2,3;10:00:00:60:69:00:03:19;30:00:00:60:69:00:03:19;na

    FC4s: FCIP
N    021300;  3;10:00:00:60:69:00:02:d6;20:00:00:60:69:00:02:d6; na

NL   0214e2;  3;21:00:00:fa:ce:00:21:1e;20:00:00:fa:ce:00:21:1e; na

    FC4s: FCP [STOREX RS2999FCPH3 MT09]

NL   0214e4;  3;21:00:00:fa:ce:00:21:e1;20:00:00:fa:ce:00:21:e1; na

    FC4s: FCP [STOREX RS2999FCPH3 CD09]

NL 0214e8; 3;21:00:00:fa:ce:04:83:c9;20:00:00:fa:ce:04:83:c9; na

    FC4s: FCP [STOREX RS2999FCPH3 NS09]

NL 0214ef; 3;21:00:00:ad:bc:04:6f:70;20:00:00:ad:bc:04:6f:70; na

FC4s: FCP [STOREX RS2999FCPH3 JB09]
}
```

See also

nsAllShow
switchShow

parityCheck

The **parityCheck** command enables or disables DRAM parity checking.

Syntax

```
parityCheck [ mode ]
```

Availability

Administrator

Description

Use this command to enable DRAM parity checking. The mode is saved in flash memory and remains in that mode until **parityCheck** is run again.

The mode becomes active as soon as this command is run. It does not require a restart to take effect.

DRAM parity checking, when enabled, causes **ramTest** to perform several additional tests of the parity memory. It also enables the parity checking hardware to verify proper parity on all DRAM read operations. DRAM parity checking is only available on specific switch models. If the current switch does not support parity checking, an error is displayed.

Operands

This command has the following operand:

mode Specify a `1` to enable DRAM parity checking or specify a `0` to disable it. The default (if no operand is specified) is to disable parity checking.

Example

The following example shows enabling and disabling DRAM parity checking:

```
switch:admin> parityCheck 1
Committing configuration...done.
Parity check is now ON.
switch:admin> parityCheck 0
Committing configuration...done.
Parity check is now OFF.
switch:admin> parityCheck 0
Parity not supported on system model: 4
Parity check already OFF.
```

See also

ramTest

passwd

The **passwd** command changes the system login name and password.

Syntax

```
passwd [“user”]
```

Availability

All users

Description

Use this command to change the system login name and password.

To change the login name and password for a specific user, enter the command with the optional `“user”` operand.

To change the login names and passwords for all users up to and including the current user’s security level, enter the command without the `“user”` operand.

In either case, you are first prompted to change the login name. The current login name is shown in brackets. Enter a new login name on this line or enter a carriage return to retain the previous login name. If the login name that is supplied is not already in use by another user, you are then prompted for the old password. If the password you enter matches the current password, you are prompted twice for the new password. If the two versions do not match, the process is repeated at most two more times until the command fails.

The password must have from 8 to 40 characters. You can change the login name without changing the associated password.

Use the following keyboard controls for input:

Return When entered at a prompt with no preceding input, accepts the default value (if applicable) and moves to the next prompt.

Ctrl+C (Interrupt)
Ends the command immediately and ignores all changes made. (See note.)

Ctrl+D (end of file)
When entered at a prompt with no preceding input, ends the command and saves the changes made. (See note.)

Note: On most computers; however, your settings could be different.

Operands

This command has the following operand:

“user”

Specify the name of the user, in quotation marks, for whom the login name and password are to be changed. This operand is optional.

Example

```
switch:admin> passwd “admin”
New username [admin]: maint
Old password: ********
New password: ********
Re-enter new password: ********
Committing configuration...done.
```

Diagnostics

All error messages are preceded by the command name. The following is a description of the error messages:

Table 18. Error message description

Error Message	Explanation
“user” is not a valid user name.	You have not specified a user name that is a valid, recognized user name on the system.
Permission denied.	You do not have permission to change the login name or password specified.
That user name is already being used.	You cannot change the user name to that of a previously existing user.
Incorrect password.	You have not entered the correct password when prompted for the old password.
Password unchanged.	You have not entered the correct password when prompted for the old password.
Number of failure attempts exceeded.	You have made three unsuccessful attempts to enter and verify a new password.
Passwords do not match; try again.	You have not correctly verified the new password.

See also

login
logout

portCfgEport

The **portCfgEport** command enables or disables a port from becoming an E_Port.

Syntax

```
portCfgEport [<port_number>, <mode>]
```

Availability

Administrator

Description

Use this command to enable or disable a port from becoming an E_port. The E_port capability is enabled by default unless this command is used to disable it.

When the **portCfgEport** command is a non-E_port, an ISL that is connected to this port is segmented. No data traffic between two switches is routed through this port. Also, fabric management data, such as zoning information, is not be exchanged through this port.

The configuration is saved in the nonvolatile memory and is persistent acrossa switch restart or a power cycle.

Operands

This command has the following operands:

port_number
Specify the port number to be configured. Valid values are 0 - 7 or 0 - 15 depending on the switch type.

mode Specify `1` or `0` to enable or disable a port as an E_port. Specify `1` to enable the port to become an E_port. This is the default port state. Specify `0` to disable the port from becoming an E_port. When the port_number operand is used, the mode operand must also be used. This operand is optional.

When no operand is specified, the command reports a list of ports that are disabled from becoming E_ports.

Example

The following example shows disabling port 3 from becoming an E_port:

```
switch:admin> portCfgEport 3, 0
Committing configuration...done.
switch:admin> portCfgEport
Ports: 0 1 2 3 4 5 6 7
--------------------------------
- - - NO - - - -
```

See also

portShow

switchShow

portCfgGport

The **portCfgGport** command designates a port as a locked G_port.

Syntax

```
portCfgGport [port_number, mode]
```

Availability

Administrator

Description

Use this command to designate a port as a locked G_port. After this is done, the switch attempts to initialize that port as an F_port only, and does not attempt loop initialization (FL_port) on the port. However, if the device that is attached to the port initiates loop communication, the switch responds accordingly and the port can become an FL_port. Similarly, a port designated as a G_port can become an E_port.

Locking a port as a G_port only changes the actions that are initiated by the switch; it does not change how the switch responds to initialization requests.

The configuration is saved in the nonvolatile memory and is persistent across a switch restart or a power cycle.

Operands

This command has the following operands:

port_number
Specify the port number to be configured. Valid values are 0 - 7 or 0 - 15, depending on the switch type. This operand is required.

mode Specify a value of `1` to designate the port as a G_port. Specify a value of `0` to remove the G_port designation from the port. This is the default port state. This operand is required.

Example

The following example shows configuring switch port 3 as a locked G_port:

```
switch:admin> portCfgGport 3, 1
Committing configuration...done.
```

See also

configure
portShow
switchShow

portCfgLport

The **portCfgLport** command locks a port as an L_port.

Syntax

```
portCfgLport [port_number mode]
```

Availability

Administrator

Description

Use this command to designate a port as an L_port. The switch then only attempts to initialize that port as an FL_port. The switch never attempts point-to-point (F_port) initialization on the port. However, if the device that is attached to the port initiates point-to-point communication, the switch responds accordingly, and the port can become an F_port.

Similarly, being locked as an L_port does not prevent the port from becoming an E_port.

Locking a port as an L_port only affects the actions that are initiated by the switch. It does not change how the switch responds to initialization requests.

Operands

The following operands are required:

port_number
Specify the port number to be configured. Valid values are 0 - 7 or 0 - 15, depending on the switch type. This operand is required.

mode Specify a value of `1` to designate the port as a locked L_port. Specify a value of `0` to remove the locked L_port designation from this port. This operand is required.

Example

The following example shows configuring switch port 3 as a locked L_port:

```
switch:admin> portCfgLport 3, 1
Committing configuration...done.
```

See also

configure
portShow
switchShow

portCfgLongDistance

The **portCfgLongDistance** command configures a port to support long distance links.

Syntax

```
portCfgLongDistance port_number [0|1|2]
```

Availability

Administrator

The Extended Fabrics license key is required to use this command.

Description

Use this command to specify the allocation of enough full-size frame buffers on a particular port to support a long distance link of up to 100 km (62 mi). The port can be used as either an Fx_port or an E_port. The configuration is saved in the nonvolatile memory and is persistent across switch restart or a power cycle.

When this command is invoked without the optional operand, you are prompted to enter the long distance level number. The level number must be one of the following:

0 Reconfigures the port as a regular switch port. The number of buffers reserved for the port supports links up to 10 km.

1 Level 1 long distance, up to 50 km (31 mi). A total of 27 full-size frame buffers are reserved for the port.

2 Level 2 long distance, up to 100 km (62 mi). A total of 60 full-size frame buffers are reserved for the port.

You can cancel the configuration update by pressing Ctrl+D.

When a port is configured to be a long distance port, the output of the **portShow** and **switchShow** commands displays the long distance level. In the **portShow** command output, the long distance level is indicated as `medium` for level 1 long distance, and `long` for level 2 long distance. In the **switchShow** command output, the format is Lx, where x is the long distance level number, except for level 0, which is not displayed by **switchShow**.

A group of four adjacent ports that share a common pool of frame buffers (for example, ports 0 - 3 or 4 - 7) are called a *quad*. Because the total number of frame buffers in a quad is limited, if one of the ports in the quad is configured as a long distance port, none of the remaining ports in the quad can be a long distance port; they must all be level 0 ports.

In order to have a long distance port take effect, all switches in the fabric must be configured to run in long distance fabric mode (in other words, the long distance fabric mode bit must be *on*, or set to 1). Otherwise, the fabric will be segmented. A long distance port cannot be configured in a switch unless the long distance fabric mode is on for that switch.

If all ports are reconfigured back to nonlong distance ports, the long distance fabric mode must be set to off for that switch.

Operands

This command has the following operands:

port_number
Specify the port number to be configured. Valid values are 0 - 7 or 0 - 15. This operand is required.

0|1|2
Specify the distance to the connected port. This operand is optional. The valid values for this operand are:

0 = Reconfigure port to be regular switch port

1 = Level 1 long distance (up to 50 km [31 mi])

2 = Level 2 long distance (up to 100 km [62 mi])

Example

The following example shows configuring switch port 3 to support a 100 km (62 mi) link:

```
switch:admin> portCfgLongDistance 3
Please enter the long distance level -- : (0..2) [0] 2
Committing configuration...done.
```

See also

configure

portShow

switchShow

portcfgMcastLoopback

The **portcfgMcastLoopback** command configures a port to receive multicast frames.

Syntax

```
portCfgMcastLoopback port_number, mode
```

Availability

Administrator

Description

This command allows you to dedicate an unused port in a leaf (edge) switch with no F_port belonging to a multicast group, to receive multicast frames.

When multicast frames are received at an edge switch with no member port, traffic throttles down in the KBps range as embedded processor intervention is required to process it.

However when a port is assigned as the multicast loopback port, frames that are destined for any multicast group are routed to that multicast loopback port where it is loopbacked to the port's receiver, which is turned off. This effectively sends the frames to an unused port. Because an embedded processor is not involved, traffic moves at normal (and full) speed.

Running this command on a branch (middle) switch does not affect traffic. It can be configured for future use as an edge switch. The disadvantage is that the port cannot be used to connect to other devices.

The configuration is saved in the nonvolatile memory and is persistent across switch restarts or power cycles.

You are prompted if:

- The selected port is already in use as an E_port or an Fx_port.
- The switch is a branch (middle) switch.

A warning message is printed if another port is already configured as the multicast loopback.

When a port is configured as multicast loopback port:

- Its port LED blinks a slow green, indicating a loopback state. Its laser, if optical GBICed, is disabled. It does not respond to any attempt to connect it to any device.

- The comment field of the **switchShow** command shows that it is looped back to itself, as in the following example:

```
“port 3: sw No_Light Loopback->3”
```

- The portFlags line of the **portShow** command displays the “F_PORT” and “INT_LB” flags, as in the following example:

```
“portFlags: 0x20249 PRESENT F_PORT U_PORT INT_LB LED”
```

- The **mcastShow** command shows the port as a member in its Member Ports column.

Operands

The following operands are required:

port_number

The port number to be configured: 0 - 7.

mode

A value of `1` means the “port_number” specified will be dedicated as a multicast loopback port. A value of `0` means the “port_number” specified will be deconfigured from its previous role as a multicast loopback port.

Example

The following example shows configuring switch port 3 as a multicast loopback port:

```
sw5:admin> portCfgMcastLoopback 3, 1
Committing configuration...done.
```

See also

portShow
switchShow
mcastShow
configure

portDisable

The **portDisable** command disables a switch port.

Syntax

```
portDisable port_number
```

Availability

Administrator

Description

Use this command to disable a switch port. If the port is connected to another switch, the fabric might reconfigure. If the port is connected to one or more devices, the devices can no longer communicate with the fabric.

If the port was online before being disabled, the following indicate a state transition: RSCN, SNMP trap, Web pop-up window.

The front panel LED of a disabled port flashes yellow with a two-second cycle.

Operands

This command has the following operand:

port_number
Specify the port number to be disabled. Valid values are 0 - 7. This operand is required.

Example

The following example shows disabling port 4:

```
sw5:admin> portDisable 4
```

See also

portEnable
portShow
switchShow

portEnable

The **portEnable** command enables a switch port.

Syntax

```
portEnable port_number
```

Availability

Administrator

Description

Use this command to enable a switch port. If the port is connected to another switch, the fabric might reconfigure. If the port is connected to one or more devices, the devices can communicate with the fabric.

For ports that come online after being enabled, the following indications can be sent to indicate a state transition: RSCN, SNMP trap, Web pop-up window.

The front panel LED of an enabled and online port is green.

Operands

This command has the following operand:

port_number

Specify the port number to be enabled. Valid values are 0 - 7. This operand is required.

Example

The following example shows enabling port 4:

```
sw5:admin> portEnable 4
```

See also

portDisable
portShow
switchShow

portErrShow

The **portErrShow** command displays a port error summary.

Syntax

```
portErrShow
```

Availability

All users

Description

Use this command to display an error summary for all ports. The display contains one output line per port and shows error counters in units, thousands (K), or millions (M).

The following fields are displayed:

frames tx
The number of frames transmitted.

frames rx
The number of frames received.

enc in The number of encoding errors inside frames.

crc err The number of frames with CRC errors.

too shrt The number of frames shorter than minimum.

too long The number of frames longer than maximum.

bad eof The number of frames with bad end-of-frame delimiters.

enc out The number of encoding error outside of frames.

disc c3 The number of class 3 frames discarded.

link fail The number of link failures (LF1 or LF2 states).

loss sync
Loss of synchronization.

loss sig Loss of signal.

frjt The number of frames rejected with F_RJT.

fbsy The number of frames busied with F_BSY.

Operands

None

Example

The following example shows an eight-port switch. Notice in the example that port 6 has a high number of errors and should be examined:

```
sw5:admin> portErrShow
frames      enc  crc  too    too   bad  enc  disc   link   loss   loss   frjt fbsy
tx   rx     in   err  shrt   long  eof  out  c3     fail   sync   sig
--------------------------------------------------------------------------
0:   0      0    0    0      0     0    0    0      0      0      0 1    0    0
1:   2.5m   38   0    0      0     0    0    2      0      0      1 1    0    0
2:   0      0    0    0      0     0    0    0      0      0      0 1    0    0
3:   95k    15k  0    0      0     0    0    3      0      0      1 0    0    0
4:   0      0    0    0      0     0    0    0      0      0      0 1    0    0
5:   0      0    0    0      0     0    0    0      0      0      0 1    0    0
6:   61k    48   2    15     0     0    0    3k     0      0      2 0    0    0
7:   0      0    0    0      0     0    0    0      0      0      0 1    0    0
```

See also

portShow
portStatsShow

portLogClear

The **portLogClear** command clears the port log.

Syntax

```
portLogClear
```

Availability

Administrator

Description

Use this command to clear the port log.

You might want to clear the port log before triggering an activity so that the log displays only the information that is related to that activity. See the **portLogShow** command for a description of the port log.

If the port log is disabled, the **portLogClear** command enables it. Certain errors automatically disable the port log to preserve information needed to understand the error (new events are not collected so that existing information is not overwritten).

The following errors disable the port log:

FCIU,	IUBAD
FCIU,	IUCOUNT
FCPH,	EXCHBAD
FCPH,	EXCHFREE
NBFSM,	DUPEPORTSCN
UCAST,	RELICPDB

Operands

None

Example

The following example shows clearing the port log:

```
sw5:admin> portLogClear
sw5:admin> portLogShow
port log is empty
```

See also

portLogDump
portLogShow

portLogDump

The **portLogDump** command displays the port log without page breaks.

Syntax

```
portLogDump [count[, saved]]
```

Availability

All users

Description

Use this command to display the port log, listing all entries in the log without page breaks. This command displays the same information as the **portLogShow** command, but the **portLogShow** command prompts you to enter “returns” between each page.

See the **portLogShow** command for a description of the port log.

If the port log is disabled, the following message is displayed as the first line:

```
WARNING: port log is disabled
```

See the **portLogClear** command for details.

Operands

This command has the following operands:

count Specify the maximum number of lines to be displayed. Only the most recent count entries are displayed. This operand is optional.

saved Specify a nonzero value to display the saved port log from the last switch fault. See **uptime** for conditions that cause a fault. `count` is ignored when displaying the saved log. This operand is optional.

Example

The following example shows displaying of the port log:

```
Sr99:admin> portlogdump 10
May  1       task   event port cmd args
----------------------------------------------
16:51:15.499 tShell ioctl    7  de 10f9bb90,0
16:51:15.499 tShell ioctl    8  de 10f9bb90,0
16:51:15.499 tShell ioctl    9  de 10f9bb90,0
16:51:15.499 tShell ioctl   10  de 10f9bb90,0
16:51:15.499 tShell ioctl   11  de 10f9bb90,0
16:51:15.499 tShell ioctl   12  de 10f9bb90,0
16:51:15.499 tShell ioctl   13  de 10f9bb90,0
16:51:15.499 tShell ioctl   14  de 10f9bb90,0
16:51:15.499 tShell ioctl   15  de 10f9bb90,0
16:58:28.383 tShell  create        tSyslog
Sr99:admin>
```

See also

portLogClear
portLogShow
uptime

portLogShow

The **portLogShow** command displays the port log.

Syntax

```
portLogShow [count[, saved]]
```

Availability

All users

Description

Use this command to display the port log; 22 entries are displayed at a time.

The **portLogShow** command displays the same information as the **portLogDump** command, but it allows you to enter a “return” after each page of output.

If the port log is disabled, the following message is displayed as the first line:

```
WARNING: port log is disabled
```

See the **portLogClear** command for details.

Table 19 gives a description of the **portLogShow** fields.

Table 19. Description of the portlogShow fields

Field	Description	
time	The date and time of the event. Clock resolution is 16 ms.	
task	The name of the task that logged the event, “interrupt” if the event was logged in interrupt context, or “unknown” if the task no longer exists.	
event	Possible events are:	
	start	Switch start or restart event.
	disable	Port is disabled.
	enable	Port is enabled.
	ioctl	Port I/O control is run.
	Tx	Frame is transmitted (class is indicated).
	Rx	Frame is received (class is indicated).
	scn	State change notification is posted.
	pstate	Port changes physical state.
	rejec	Received frame is rejected.
	busy	Received frame is busied.

	ctin	CT-based request is received.	
	ctout	CT based response is transmitted.	
	errlog	Message is added to the error log.	
	loopscn	Loop state change notification is posted.	
	create	Task is created.	
port	The port number of the affected port.		
cmd	Command value - description depends on event type:		
	ioctl	I/O control command code.	
	Tx & Rx	Frame payload size.	
	scn	New state (see state codes).	
	pstate	New physical state (see pstate codes).	
	ctin	CT-subtype: fc = simple name server, f8 = alias server.	
	ctout	Same as ctin.	
	errlog	Error level (see **errShow**).	
	loopscn	Current loop state during loop initialization. Possible values are:	
		OLP	Offline (disconnected or nonparticipating).
		LIP	FL_port entered INITIALIZING or OPEN_INIT state.
		LIM	LISM completed, FL_port became the loop master.
		BMP	Loop initialization completed, FL_port in MONITORING state.
		OLD	Port transited to the old_port state.
		TMO	Loop initialization times out.
args	The command arguments - description depends on event type:		
	star	Start type: 0 = enable ports, 100 = disable ports	
	disable	State (See state codes.)	
	enable	Mode: 0 = normal, non-zero = loopback.	
	ioctl	I/O control arguments.	
	Tx & Rx	First two header words and first payload word.	
	reject	FC-PH reject reason.	
	busy	FC-PH busy reason.	
	ctin	Argument 0 is divided into two 16-bit fields:	
		[A]	Bit map indicating validity of subsequent arguments (0001 = argument 1 is valid, 0003 = arguments 1 and 2 are valid).
		[B]	ct-based service command code. Argument 1 = first word of the CT payload, if applicable (as specified in [A]). Argument 2 = second word of the CT payload, if applicable (as specified in [A]).

	ctout	Argument 0 is divided into two 16-bit fields:	
		[A]	Bit map indicating validity of subsequent arguments (0001 = argument 1 is valid, 0003 = arguments 1 and 2 are valid).
		[B]	CT command code indicating an accept (8002) or a reject (8001). If [B] is an accept, argument 1 and 2 represents the first and second words of the CT payload, if applicable (as specified in [A]).
			If [B] is a reject, argument 1 contains the CT reject reason and explanation code.
	errlog	Error type (see **errShow**) create - name of the task being created.	
	loopscn	Description depends on loop state:	
		OLP	Offline reason code, usually zero.
		LIP	Reason code for LIPs initiated by FL_port, if the code value is 800x (x = [1,0xc], see below), or the lower two bytes of the LIP received, if the code value is other than 800x.
		LIM	Usually zero BMP, memory address for the loop bitmap.
		OLD	Usually zero.
		TMO	Encoded value of state when loop initialization timed out.
Codes:			
state	1	Online	
	2	Offline.	
	3	Testing.	
	4	Faulty.	
	5	E_port.	
	6	F_port.	
	7	Segmented.	
pstate	AC	Active state	
	LR1	Link reset: LR transmit state.	
	LR2	Link reset: LR receive sate.	
	LR3	Link reset: LRR receive state.	
	LF1	Link failure: NOS transmit state.	
	LF2	Link failure: NOS receive state.	
	OL1	Offline: OLS transmit state.	
	OL2	Offline: OLS receive state.	
	OL3	Offline: wait for OLS state.	
ioctl	90	Get virtual channel credits.	

	91	Set virtual channel credits.
	a1	Port is an E_port.
	a2	Port is an F_port.
	a3	Port is segmented.
	a4	Domain name is known.
	a5	Port enable.
	a6	Port disable.
	a7	Link reset.
	a8	Add unicast route.
	a9	Delete unicast route.
	aa	Add multicast route.
	ab	Delete multicast route.
	ac	Unicast path selection done.
	ad	Multicast path selection done.
LIP	8001	Retry loop initialization.
reason	8002	Start loop after gaining sync.
	8003	Restart loop after port reset.
	8004	LIP when a loop hangs.
	8005	Restart loop if LIP received when sending out ARB(F0).
	8006	LIP when an OPN returns.
	8007	Restart loop when LIPs received in OLD_PORT AC state.
	8008	Restart loop if loop not empty but E_port loopback.
	8009	LIP as requested by the LINIT ELS received.
	800a	LIP as requested by the LPC ELS received.
	800b	Restart loop for QuickLoop looplet setup.
	800c	Restart loop for QuickLoop looplet reinitialization.

Operands

This command has the following operands:

count Specify the maximum number of lines to display. Only the most recent count entries are displayed. This operand is optional.

saved Specify the maximum number of lines to display. Only the most recent count entries are displayed. This operand is optional.

Example

The following example shows a section of the port log with an E_port coming online. The ELP and EFP exchanges are shown; a name service request was processed.

```
sw5:admin> portLogShow 5
May 1        task      event port  cmd args
----------------------------------------------
06:48:01.623  interrupt scn    13  2
06:48:02.359  tFspf     ioctl  13  ab  ffffff,10
06:48:04.699  tReceive  Rx     13  0   c0fffffd,00fffffd,00bb0045
06:48:07.616  tReceive  Rx     13  40 4002fffffd,00fffffd,0046ffff,14000000
06:48:07.616 tTransmit Tx 13 0 c0fffffd,00fffffd,004600bc
```

See also

portLogClear
portLogDump
uptime

portLoopbackTest

The **portLoopbackTest** command tests the function of the port N to port N path.

Syntax

```
portLoopbackTest
```

Availability

Administrator

Description

Use this command to verify the functional operation of the switch by sending frames from the port N transmitter, and looping the frames back into the same port N receiver. The loopback is done at the parallel loopback path. The path exercised in this test does not include the GBIC nor the fiber cable.

Only one frame is transmitted and received at any one time. No external cable is required to run this test. The port LEDs flicker green rapidly while the test is running.

Below is the test method:

1. Set all ports for parallel loopback
2. Create a frame F of maximum data size (2112 bytes).
3. Transmit frame F through port N.
4. Pick up the frame from the same port N.
5. Check the 8 statistic error counters for nonzero values:

ENC_in, CRC_err, TruncFrm, FrmTooLong, BadEOF, Enc_out, BadOrdSet, DiscC3

6. Check if the transmit, receive, or class 3 receiver counters are stuck at some value.
7. Check if the number of frames transmitted is not equal to the number of frames received.
8. Repeat steps 2 - 7 for all ports present until:
   - The number of frames (or passCount) requested is reached.
   - All ports are marked bad.
   - At each pass, the frame is created from a different data type. If seven passes are requested, seven different data types are used in the test. If eight passes are requested, the first seven frames use unique data types, and the eighth is the same as the first. The seven data types are:

```
1. CSPAT:       0x7e, 0x7e, 0x7e, 0x7e, ...
2. BYTE_LFSR:   0x69, 0x01, 0x02, 0x05, ...
3. CHALF_SQ:    0x4a, 0x4a, 0x4a, 0x4a, ...
4. QUAD_NOT:    0x00, 0xff, 0x00, 0xff, ...
5. CQTR_SQ:     0x78, 0x78, 0x78, 0x78, ...
6. CRPAT:       0xbc, 0xbc, 0x23, 0x47, ...
7. RANDOM:      0x25, 0x7f, 0x6e, 0x9a, ...
```

Because this test does not include the GBIC and the fiber cable in its test path, use the results from this test in conjunction with the results from the crossPortTest and the spinSilk test to determine those switch components that are not functioning properly.

If failures are detected, following are possible error messages:

DIAG-INIT

DIAG-PORTDIED

DIAG-XMIT

DIAG-TIMEOUT

DIAG-ERRSTAT

DIAG-STATS

DIAG-DATA

Operands

This command has the following operand:

passCount

Specify the number of times (or number of frames per port) to run this test. The default value is 0xfffffffe. This operand is optional.

Example

```
sw7:admin> portLoopbackTest 100
Running Port Loopback Test .... passed.
```

See also

camTest

centralMemoryTest

cmemRetentionTest

cmiTest

crossPortTest

portRegTest

ramTest

spinSilk

sramRetentionTest

camTest

centralMemoryTest

cmemRetentionTest

cmiTest

crossPortTest

portRegTest

ramTest

spinSilk

sramRetentionTest

portPerfShow

The **portPerfShow** command displays the port throughput performance in bytes, kilobytes, or megabytes.

Syntax

```
portPerfShow [interval]
```

Availability

All users

Description

Use this command to display the throughput information for all ports on the switch (8 or 16 columns depending on the switch model). One output line is displayed per interval (or second if no interval is specified) until Enter, Ctrl+C, or Ctrl+D are pressed.

The command displays the number of bytes received plus the number of bytes transmitted per interval. Throughput numbers are shown as either bytes, kilobytes (k), or megabytes (m).

Operands

This command has the following operand:

interval Specify the interval, in seconds, between each sample. This operand is optional.

Example

The following example shows throughput for an 8-port switch:

```
sw5:admin> portPerfShow

0      1      2      3      4      5      6      7
-----------------------------------------------
0      0      0      0      0      0      0      76m
96     0      96     0      0      96     0      76m
0      0      0      0      0      0      0      76m
```

See also

portStatsShow

portRegTest

The **portRegTest** command performs the bit write/read test of the ASIC SRAMs and registers.

Syntax

```
portRegTest
```

Availability

Administrator

Description

Use this command to verify that SRAM and register data bits in each ASIC can be independently written and read.

To verify the data bits, write a walking 1 pattern to each location - write a pattern of 0x00000001 to register N, read, and compare to be sure that the pattern is the same. Shift the pattern one bit to the left (to 0x00000002), repeat the write, read, and compare cycle. Shift again and repeat until the last writable bit in register N is reached (0x80000000 for a 32-bit register).

For example, use the following pattern to test a 6-bit register:

1. 0x0001
2. 0x0002
3. 0x0004
4. 0x0008
5. 0x0010
6. 0x0020
7. 0x0040
8. 0x0080
9. 0x0100

10.0x0200

11.0x0400

12.0x0800

13.0x1000

14.0x2000

15.0x4000

16.0x8000

Repeat the above steps until all ASIC SRAMs and registers have been tested.

If failures are detected, following are possible error messages:

DIAG-REGERR

DIAG-REGERR_UNRST

DIAG-BUS_TIMEOUT

Operands

None

Example

```
sw7:admin> portRegTest
Running Port Register Test .... passed.
```

See also

camTest
centralMemoryTest
cmemRetentionTest
cmiTest crossPortTest

portLoopbackTest
ramTest
spinSilk
sramRetentionTest

portRouteShow

The **portRouteShow** command displays the routing tables for a port.

Syntax

```
portRouteShow port_number
```

Availability

All users

Description

Use this command to display the port address ID and the contents of the following port routing tables:

External unicast routing table

Shows unicast frame routing to another switch element in the fabric. The output format is:

```
domain_number: ports_bitmap
```

where:

`domain_number` is the switch element number that a unicast frame reaches from the port_number port.

`ports_bitmap` contains all output ports, in bitmap hex format, that forwards unicast frames from port_number to domain_number.

There is at least one entry for each active port:

```
local_switch_domain_number: 0x10000
```

This is for routing unicast frames designated to the embedded port the local switch element.

Internal unicast routing table

Lists all ports in the local switch that a unicast frame can reach from port_number. The format is:

```
destination_port: output_ports_bitmap
```

Because the destination_port is in the local switch, `output_ports_bitmap` usually contains one bit with a bit position number representing the destination_port number.

Multicast routing table

Shows multicast frame routing to the destination multicast group. The output format is:

`mcast_group_number:` (mcast_group_id) `ports_bitmap`

where:

`mcast_group_number` is the multicast group number.

`mcast_group_id` is the multicast frame destination ID.

`ports_bitmap` is a hex bitmap of all output port numbers that can forward a multcast frame from the `port_number` to `mcast_group_id.`

Broadcast routing table

A bitmap containing all ports that are reachable by a received broadcast frame. Bit 16 of the bitmap is always set to allow the switch element to receive broadcast frames.

Operands

This command has the following operand:

port_number

Specify the port number to be displayed. Valid values are 0 - 7. This operand is required.

Example

```
JR-6910:other> portRouteShow 3
port address ID: 0x604300
external unicast routing table:
       0: 0x10000
       1: 0x2
internal unicast routing table:
       0: 0x1
       3: 0x4
       6: 0x40
multicast routing table:
broadcast routing table:
       0x10045
```

See also

bcastShow
mcastShow
switchShow
topologyShow
uRouteShow

portShow

The **portShow** command displays the port status.

Syntax

```
portShow port_number
```

Availability

All users

Description

Use this command to display status information for a port. Information varies with the switch model and port type. The following describes the fields that are displayed:

portFlags
The bit map of port status flags.

portType
The port type and revision numbers.

portState
The port SNMP state:

Online Up and running.

Offline Not online, portPhys gives details.

Testing Not online, portPhys gives details.

Faulty Failed diagnostics.

portPhys
The port physical state:

No_Card
No interface card present.

No_Module
No module (GBIC or other) present.

No_Light
Module is not receiving light.

No_Sync
Module is receiving light but is out of sync.

In_Sync Module is receiving light and is in sync.

Laser_Flt
Module is signaling a laser fault.

Port_Flt
Port marked faulty.

Diag_Flt
Port failed diagnostics.

Lock_Ref
Locking to the reference signal.

portScn Last state change notification for port.

portRegs
The address of the port hardware registers.

portData The address of the port driver private data.

portId 24-bit D_ID for port.

portWw Port world-wide name.

Distance The port’s long distance level.

Interrupts
The total number of interrupts.

Unknown
Interrupts that are not counted elsewhere.

Lli Low-level interface (physical state, primitive seqs).

Proc_rqrd
Frames delivered for embedded N_port processing.

Timed_out
Frames that have timed out.

Rx_flushed
Frames requiring translation.

Tx_unavail
Frames returned from an unavailable transmitter.

Free_buffer
Free buffer available interrupts.

Overrun Buffer overrun interrupts.

Suspended
Transmission suspended interrupts.

Parity_err
Central memory parity errors.

Operands

This command has the following operand:

port_number
Specify the port number to be displayed. Valid values are 0 - 7. This operand is required.

Example

The following example shows the status for a specified E_port:

```
Sr99:admin> portShow 1
portFlags: 0x20041       PRESENT U_PORT LED
portType: 3.1
portState: 2     Offline
portPhys: 4      No_Light
portScn: 0
portRegs: 0x80020000
portData: 0x10fa70a0
portId: 011100
portWwn: 20:01:00:60:69:00:73:71
Distance: normal
Interrupts:    0       Link_failure:   0       Frjt: 0
Unknown:       0       Loss_of_sync:   0       Fbsy: 0
Lli:           0       Loss_of_sig:    1
Proc_rqrd:     0       Protocol_err:   0
Timed_out:     0       Invalid_word:   0
Rx_flushed     0       Invalid_crc:    0
Tx_unavail:    0       Delim_err:      0
Free_buffer:   0       Address_err:    0
Overrun:       0       Lr_in:          0
Suspended:     0       0 Lr_out:       0
Parity_err:    0       Ols_in:         0
               0       Ols_out:        0


Sr99:admin>
```

See also

switchShow

portStatsShow

The **portStatsShow** command displays the port hardware statistics.

Syntax

```
portStatsShow port_number
```

Availability

All users

Description

Use this command to display the port hardware statistics counters. The first section is common to all hardware; one of the last two sections (depending on switch type) is shown for loop ports. The following describes the fields that are displayed:

stat_wtx 4-byte words transmitted.

stat_wrx 4-byte words received.

stat_ftx Frames transmitted.

stat_frx Frames received

stat_c2_frx
Class 2 frames received.

stat_c3_frx
Class 3 frames received.

stat_lc_rx
Link control frames received.

stat_mc_rx
Multicast frames received.

stat_mc_to
Multicast timeouts.

stat_mc_tx
Multicast frames transmitted.

tim_rdy_pri
Time R_RDY high priority.

tim_txcrd_z
Time BB_credit zero.

er_enc_in
Encoding errors inside frames.

er_crc Frames with CRC errors.

er_trunc Frames shorter than minimum.

er_toolong
Frames longer than maximum.

er_bad_eof
Frames with bad end-of-frame.

er_enc_out
Encoding error outside frames.

er_disc_c3
Class 3 frames discarded.

fl_open Number of OPNyx sent.

fl_opened
Number of OPNyx received.

fl_openfr
Number of OPNfr sent.

fl_cls_idle
CLS sent due to loop idle.

fl_cls_rx CLS received when open.

fl_bb_stall
OPN/CLS BB_Credit stalls.

fl_cf_alloc
Number of CFIFOs allocated.

fl_cf_opn
CFIFOs delivered when opened.

fl_cf_full
Number of CFIFOs full stalls.

fl_cf_na CFIFO not available stalls.

fl_trig_age
Number of age count triggers.

fl_trig_lp Number of loop not busy triggers.

open Number of times the FL_port entered open state.

transfer Number of times the FL_port entered transfer state

opened Number of times the FL_port entered opened state.

starve_stop
Loop tenancies stopped due to starvation.

fl_tenancy
Number of times FL_port had loop tenancy.

nl_tenancy
Number of times NL_port had loop tenancy.

frame_nozone
Frames rejected due to zone protection.

Operands

This command has the following operand:

port_number

Specify the port number to be displayed. Valid values are 0 - 7. This operand is required.

Example

The following example shows a port with only the basic set of statistics:

```
sw5:admin> portStatsShow 3
stat_wtx       1181994    4-byte words transmitted
stat_wrx       1188458    4-byte words received
stat_ftx       95830      Frames transmitted
stat_frx       15564      Frames received
stat_c2_frx    0          Class 2 frames received
stat_c3_frx    93         Class 3 frames received
stat_lc_rx     7735       Link control frames received
stat_mc_rx     0          Multicast frames received
stat_mc_to     0          Multicast timeouts
stat_mc_tx     0          Multicast frames transmitted
tim_rdy_pri    477        Time R_RDY high priority
tim_txcrd_z    0          Time BB_credit zero
er_enc_in      0          Encoding errors inside of frames
er_crc         0          Frames with CRC errors
er_trunc       0          Frames shorter than minimum
er_toolong     0          Frames longer than maximum
er_bad_eof     0          Frames with bad end-of-frame
er_enc_out     3          Encoding error outside of frames
er_disc_c3     0          Class 3 frames discarded
```

See also

portErrShow
portShow

psShow

The **psShow** command displays the power supply status.

Syntax

`psShow`

Availability

All users

Description

Use this command to display the switch power supply status.

The display format varies with switch model and number of power supplies present.

The status of each supply is shown as:

OK Power supply is present and functioning correctly.

absent Power supply is not present.

faulty Power supply is present but faulty (no power cable, power switch turned off, fuse blown, or other internal error).

After the status line, a power supply identification line can be shown. If present, this line contains manufacture date, part numbers, serial numbers, and other identification information.

Operands

None

Example

```
sw5:admin> psShow
Power Supply 1 is OK
9835,DH000000208,60-0000734-01, A,00001, E108302A,01, 803350
Power Supply 2 is OK
9839,DH000000253,60-0000734-01, A,00001, E108302A,01, 803522
```

See also

fanShow
tempShow

qlPartner

The **qlPartner** command sets or displays the quick loop partner.

Syntax

```
qlPartner[ 0 | worldwide Node Name ]
```

Availability

Administrator

Description

Use this command to set the quickLoop to single or dual switch mode or to display the quickLoop scope setting.

If no argument is specified, this command displays the current quickloop mode, which can be single or dual switch. When `0` is used as the argument, this command sets the quickloop to run in single switch mode, and restarts the switch if not already in this mode. If a non-zero and valid WWN (a WWN that is part of the fabric) for a switch is specified, that switch becomes the quickloop partner. The switch is then restarted to run in dual switch mode.

The partner setting is updated in flash memory.

If zoning is in use, this command is not in effect. Using it displays a message that refers you to the zoning commands.

Operands

The following operand is required:

`[0 | Worldwide Node Name]`

0 Clear quick loop partner. Change to single switch quick loop.

WWN Set quick loop partner. Change to dual switch quick loop.

No argument
Display current setting

Example

The following example shows setting `10:00:00:60:69:10:10:ec` as a quick loop partner switch:

```
sw5:admin> qlPartner "10:00:00:60:69:10:10:ec"
```

See also

qlShow,
configShow

qloopEnable

The **qloopShow** command enables quick loop mode.

Syntax

```
qlEnable
```

Availability

Administrator

Description

Use this command to enable QuickLoop mode on a switch. All devices connected to quickLoop ports are reinitialized to form a single loop.

If a partner switch is configured, the **qlEnable** command causes re-initialization of the partner, if it is in quickLoop mode. The devices on the two switches are then combined to form a single loop (using a single AL_PA space).

QuickLoop combines arbitrated loop and fabric topologies. It consists of multiple private arbitrated loops (looplets) interconnected by a fabric, with the existence of the fabric and the physical locations of the devices transparent. All NL_ports share a single AL_PA space and operate in accordance with FC-AL.

QuickLoop initialization includes the following two steps:

Pass 1: Sequential looplet initialization. Allows each device in a looplet to obtain a unique AL_PA.

Pass 2: Full quickLoop initialization. Brings the quickloop up to operation.

If zoning is in use, the **qlDisable**, **qlEnable**, and **qlPartner** commands are not in effect. In this case, entering these commands displays a message refering you to the zoning commands.

Operands

None

Example

The following command enables quick loop:

```
  sw5:admin> qlEnable
```

See also

qlDisable

qlPortEnable

qlShow

qloopShow

The **qloopShow** command displays quickloop information.

Synopsis

```
qlShow
```

Availability

All users

Description

This command displays the following quick loop information:

Self Worldwide name and domain ID of this switch.

Peer Worldwide name and domain ID of partner switch. *Peer* is displayed only if the switch has a configured partner.

State Quick loop state.

Master Master switch in dual switch quickLoop.

Non-master
Non-master in dual switch quickLoop.

Local Lip
Looplet on local switch lipped.

Remote Lip
Looplet on partner switch lipped.

Online
Switch comes online.

Offline
Switch goes offline.

Scope Dual or single (switch quick loop).

AL_PA bitmap:
AL_PA bitmaps of devices on the quick loop.

Remote AL_PAs
AL_PA of devices on the partner switch.
AL_PAs are listed per port base.

Local AL_PAs
AL_PA of devices on lthe ocal switch
AL_PAs are listed per port base

Local looplet state
Indicates the state of the local looplet

Member
Current quick loop member ports

Online
Current online ports in the quick loop. Looplet can be in one of the following states:

Online Completed loop initialization.

Lipped NL_port lipped.

Lipping FL_port lipped.

Initializing
Loop initialization in progress.

Bypassed
Looplet being bypassed.

Error Error found in this looplet.

Offline Looplet offline.

Operands

None

Example

The following example shows displaying quick loop information:

```
sw5:admin> qlShow
```

See also

qlEnable

quietMode

The **quietMode** command sets or clears the shell quiet mode.

Syntax

```
quietMode [newMode]
```

Availability

All users (display)

Administrator (set or clear)

Description

Use this command to change the output that is displayed on the switch console (serial port or Telnet session).

By default, quiet mode is off and all switch tasks can send output to the console, including output caused by asynchronous events such as reconfiguring the fabric, or logging in devices.

When quiet mode is on, only output that is produced by shell commands is shown; asynchronous output that is produced by other tasks is suppressed.

Turn quiet mode on when driving a Telnet session by using a script that does not expect asynchronous output.

Operands

This command has the following operand:

newMode

Specify to set or clear quiet mode. Valid values are:
`0` to clear quiet mode (all tasks can print to the console) or
`1` to set quiet mode (only shell commands can print).

Example

The followng example shows displaying the current mode, and then resetting quiet mode on:

```
sw5:admin> quietMode
Quiet Mode is OFF
sw5:admin> quietMode 1
Committing configuration...done.
Quiet Mode is now ON
```

ramTest

The **ramTest** command tests the bit write/read of the SDRAMs in the switch.

Syntax

```
ramTest [patternSize]
```

Availability

Administrator

Description

Use this command to verify the address and data bus of the SDRAMs that serve as the 16 MB CPU memory in the switch. The test consists of two subtests:

1. The **address subtest** verifies that SDRAM locations can be uniquely accessed.

   The method used is to write a unique pattern to each location in the SDRAMs. When all are written, the data is read back from each location and compared against the data previously written. A failure in the test implies that the address path between the CPU and the SDRAMs are faulty resulting in failures to program unique values. Following is the ramp pattern used in the test:

```
0x57626f42, 0x57626f43, 0x57626f44, 0x57626f45, ...
```

2. The data subtest verifies that each cell in the SDRAMs can be independently written and read, and that there is no short, stuck-at-1, or stuck-at-0 faults between data cells.

   The method used is to write pattern D to location N, write the complementary pattern D to location N+1, and then read and compare location N to location N+1. Bump the location to test:

N=N+1. Repeat the double write and read until all locations are tested with the following 9 patterns:

- 0x55555555
- 0x69696969
- 0x3c3c3c3c
- 0x1e1e1e1e
- 0x87878787
- 0x14284281
- 0x137ffec8
- 0x0f0f0f0f
- 0x00000000

Because the test requires the operating system to operate which is loaded in the same memory, it does not and cannot test all 16 MB of the memory. Instead, it tests the largest portion as given by the OS, which is typically about 13 MB. Following are the possible error messages, if failures are detected:

DIAG-MEMORY DIAG-MEMSZ DIAG-MEMNULL

Operands

This command has the following operand:

patternSize

If 0 (default), **ramTest** runs all 9 patterns in the data subtest. If N, **ramTest** runs N patterns in the data subtest. If N is greater than 9, it is truncated to 9. Only the data subtest is configurable. The address subtest is always run. This operand is optional.

Example

```
sw7:admin> ramTest
Running System DRAM Test ...... passed.
```

See also

camTest

centralMemoryTest

cmemRetentionTest

cmiTest

crossPortTest

portLoopbackTest

portRegTest

spinSilk

sramRetentionTest

reboot

The **reboot** command restarts the switch.

Syntax

```
reboot
```

Availability

Administrator

Description

Use this command to restart the switch. The restart takes effect immediately as the switch resets, then runs the normal power-on sequence.

While the switch is restarting, the Telnet session is closed and all fibre-channel ports are inactive. If the switch was part of a fabric, the remaining switches are reconfigured.

Operands

None

Example

The following example shows restarting the switch:

```
sw5:admin> reboot
Rebooting...
```

See also

fastboot

routeHelp

The **routeHelp** command displays the routing help commands.

Syntax

```
routeHelp
```

Availability

Administrator

Description

Use this command to display the routing help commands.

Operands

None

Example

```
switch:              admin> routeHelp
bcastShow            Print broadcast tree information
dlsReset             Turn off Dynamic Load Sharing
dlsSet               Turn on Dynamic Load Sharing
dlsShow              Print state of Dynamic Load Sharing
fspfShow             Print FSPF global information
interfaceShow        Print FSPF interface information
iodReset             Turn off In-Order Delivery
iodSet               Turn on In-Order Delivery
iodShow              Print state of In-Order Delivery
linkCost             Set or print the FSPF cost of a link
LSDbShow             Print Link State Database entry
mcastShow            Print multicast tree information
nbrStateShow         Print neighbor’s summary information
nbrStatsClear        Reset FSPF neighbor’s counters
topologyShow         Print paths to domain(s)
uRouteConfig         Configure static unicast route
uRouteRemove         Remove static unicast route
uRouteShow           Print port’s unicast routing info
```

setGbicMode

The **setGbicMode** command enables or disables the GBIC mode.

Syntax

```
setGbicMode [mode]
```

Availability

Administrator

Description

Use this command to enable or disable the GBIC mode. If the mode operand is 1, GBIC mode is enabled; if the mode operand is 0, GBIC mode is disabled. The mode is saved in flash memory and stays in the GBIC remains in that mode until the next running of **setGbicMode**.

The mode becomes active as soon as this command is run. It does not require a restart to take effect.

The GBIC mode, when enabled, forces the **crossPortTest** and the **spinSilk** commands to limit testing to ports with GBICs present. Consequently, testing is limited to those ports with a suspected problem.

Operands

This command has the following operand:

mode Specify whether to enable or disable GBIC mode. Specify 1 to enable GBIC mode or 0 to disable GBIC mode. The default value (if no operand specified) is 0.

Example

```
sw7:admin> setGbicMode 1
Committing configuration...done.
GBIC mode is now ON.
sw7:admin> setGbicMode
Committing configuration...done.
GBIC mode is now OFF.
```

See also

crossPortTest

spinSilk

setSplbMode

The **setSplbMode** command enables or disables two port loopback.

Syntax

```
setSplbMode [mode]
```

Availability

Administrator

Description

Use this command to enable set port loopback (SPLB) mode if the operand is 1 and disable the SPLB mode if the operand is 0. The mode is saved in flash memory and stays in that mode until another **setSplbMode** command is issued.

The mode becomes active as soon as this command is issued. It does not require a restart to take effect.

The SPLB mode, when enabled, forces **spinSilk** to disable two port loopback for M-to-M connected ports. This can be useful for isolating internal switch problems from GBIC problems because the internal paths are used much less with SPLB mode enabled.

The SPLB mode, when disabled, forces **spinSilk** to circulate frames between pairs of M-to-M connected ports as follows:

```
P1 TX >>> P1 RX -> P2 TX >>> P2 RX -> P1 TX
>>> cable or internal loop-back
-> routing table entry
```

The connections between pairs of M-to-M ports are chosen to exercise the connections between as many chips (or bloom quadrants) as possible, subject to the setting of allow_intra_chip and the availability of pairs of M-to-M ports. Any ports that are cross-cabled are routed to each other in the normal manner regardless of the SPLB mode setting:

```
P1 TX >>> P2 RX -> P1 TX
P2 TX >>> P1 RX -> P2 TX
```

Operands

This command has the following operand:

mode Specify whether to enable or disable SPLB mode. Specify `1` to enable SPLB mode or `0` to disable SPLB mode. The default value (if no operand is specified) is `0`.

Example

```
Sr99:admin> setSplbMode 1
Committing configuration...done.
SPLB mode is now ON.
Sr99:admin> setSplbMode 0
Committing configuration...done.
SPLB mode is now OFF.
```

See also

setGbicMode
spinSilk

spinSilk

The **spinSilk** command is a functional test of port M-to-N path at maximum switch speed.

Syntax

```
spinSilk [nMillionFrames]
```

Availability

Administrator

Description

Use this command to verify the functional operation of the switch at the maximum speed of 1 Gbps.

To run **spinSilk**, set up the routing hardware so that frames received by port M are retransmitted through port N and frames received by port N are retransmitted through port M. Each port M sends 4 frames to its partner port N using an external fiber cable; this exercises all switch components from the main board, to the GBIC, to the fiber cable, to the GBIC, and back to the main board.

The cables can be connected to any port combination as long as the cables and GBICs connected are of the same technology: a short wavelength GBIC port is connected to another short wavelength GBIC port using a short wavelength cable, and a long wavelength port is connected to a long wavelength port, and a copper port is connected to a copper port.

For best coverage, connect ports from different ASICs. Ports 0 - 3 belong to ASIC 0, ports 4 - 7 belong to ASIC 1, and so on. A connection from port 0 to port 15 exercises the transmit path between ASICs. A connection from port 0 to port 3 tests only the internal transmit path in ASIC 0.

The frames are continuously transmitted and received in all ports in parallel. The port LEDs flicker green rapidly while the test is running.

The following is the test method:

1. Determine port connections.
2. Enable ports for cabled loopback mode.
3. Configure the routing table to route frames received by port M to the partner port N and vice versa.

4. Transmit 4 frames of different lengths using port M. Following are the 4 frames:

```
2112 bytes of BYTE_LFSR
1000 bytes of CSPAT
128 bytes of RANDOM
512 bytes of RDRAM_PAT
```

The partner port N eventually sends 4 similar frames as follows:

```
2112 bytes of BYTE_LFSR
928 bytes of CSPAT
200 bytes of RANDOM
480 bytes of RDRAM_PAT
```

5. Periodically check each port for the following:

   - Each port has not died
   - Frames transmitted counter is incrementing
   - Statistic error counters are nonzero

```
ENC_in, CRC_err, TruncFrm, FrmTooLong, BadEOF, Enc_out,
BadOrdSet, DiscC3
```

   until one of the following is met:

   - The number of million frames requested per port are met.
   - All ports are marked bad.
   - The user sends a keyboard (or push button) interrupt to abort.

In this test, data is not read and checked, and the only CPU intervention is the periodic check of hardware counters.

Below is an example of the data used:

```
CSPAT: 0x7e, 0x7e, 0x7e, 0x7e, ...
BYTE_LFSR: 0x69, 0x01, 0x02, 0x05, ...
RANDOM: 0x25, 0x7f, 0x6e, 0x9a, ...
RDRAM_PAT: 0xff, 0x00, 0xff, 0x00, ...
```

GBIC Mode

If the **spinSilk** command is run with GBIC mode activated, only ports containing GBICs are tested. To activate GBIC mode, run the following command before running **spinSilk**.

```
sw:admin> setGbicMode 1
```

The state of the GBIC mode is saved in flash and it remains active (even after restarts or power cycles) until it is disabled as follows:

```
sw:admin> setGbicMode 0
```

For example, disable the switch, set the GBIC mode to 1, and run the **spinSilk** command to limit testing to:

```
only ports containing GBICs
that _all_ GBIC ports that are cable loopbacked
```

Because this test includes the GBIC and the fiber cable in its test path, use the results from this test in conjunction with the results from **crossPortTest** and **portLoopbackTest** to determine those switch components that are not functioning properly.

Below are the possible error messages if failures are detected:

```
DIAG-INIT
DIAG-PORTDIED
DIAG-XMIT
DIAG-PORTSTOPPED
DIAG-ERRSTAT
DIAG-ERRSTATS
```

Operands

This command has the following operand:

nMillionFrames

Specify the number of million frames per port to run this test. If omitted, the default passCountvalue is 0xfffffffe. This operand is optional.

Example

.

```
sw7:admin> spinSilk 2
Running Spin Silk ............
One moment please ...
switchName:    sw7
switchType:    2.2
switchState:   Testing
switchRole:    Disabled
switchDomain:  1 (unconfirmed)
switchId:      fffc01
switchWwn:     10:00:00:60:69:00:73:71
port 0:   cu Testing Loopback->15
port 1:   sw Testing Loopback->11
port 2:   sw Testing Loopback->6
port 3:   lw Testing Loopback->4
port 4:   lw Testing Loopback->3
port 5:   sw Testing Loopback->8
port 6:   sw Testing Loopback->2
port 7:   sw Testing Loopback->12
port 8:   sw Testing Loopback->5
port 9:   sw Testing Loopback->14
port 10:  sw Testing Loopback->13
port 11:  sw Testing Loopback->1
port 12:  sw Testing Loopback->7
port 13:  sw Testing Loopback->10
port 14:  sw Testing Loopback->9
port 15:  cu Testing Loopback->0
```

```
Transmitting ... done.
Spinning ...
port 0   Rx/Tx 1 of 1 million frames.
port 1   Rx/Tx 1 of 1 million frames.
port 2   Rx/Tx 1 of 1 million frames.
port 3   Rx/Tx 1 of 1 million frames.
port 4   Rx/Tx 1 of 1 million frames.
port 5   Rx/Tx 1 of 1 million frames.
port 6   Rx/Tx 1 of 1 million frames.
port 7   Rx/Tx 1 of 1 million frames.
port 8   Rx/Tx 1 of 1 million frames.
port 9   Rx/Tx 1 of 1 million frames.
port 10  Rx/Tx 1 of 1 million frames.
port 11  Rx/Tx 1 of 1 million frames.
port 12  Rx/Tx 1 of 1 million frames.
port 13  Rx/Tx 1 of 1 million frames.
port 14  Rx/Tx 1 of 1 million frames.
port 15  Rx/Tx 1 of 1 million frames.
```

```
Diagnostics Status: Tue Apr 6 04:10:12 1999
port#: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
diags: OK OK OK OK OK OK OK OK OK OK OK OK OK OK OK OK
state: UP UP UP UP UP UP UP UP UP UP UP UP UP UP UP UP
lm0:   2059619 frTx 2052666 frRx 0 LLI_errs. <looped-15>
lm1:   2054565 frTx 2052620 frRx 0 LLI_errs. <looped-11>
lm2:   2050424 frTx 2048321 frRx 0 LLI_errs. <looped-6>
lm3:   2053094 frTx 2042762 frRx 0 LLI_errs. <looped-4>
lm4:   2042957 frTx 2053290 frRx 0 LLI_errs. <looped-3>
lm5:   2056586 frTx 2053910 frRx 0 LLI_errs. <looped-8>
lm6:   2048992 frTx 2048569 frRx 0 LLI_errs. <looped-12>
lm9:   2039595 frTx 2051975 frRx 0 LLI_errs. <looped-14>
lm10:  2050130 frTx 2052565 frRx 0 LLI_errs. <looped-13>
lm11:  2054678 frTx 2056622 frRx 0 LLI_errs. <looped-1>
lm12:  2049707 frTx 2050131 frRx 0 LLI_errs. <looped-7>
lm13:  2053410 frTx 2050976 frRx 0 LLI_errs. <looped-10>
lm14:  2053358 frTx 2040971 frRx 0 LLI_errs. <looped-9>
lm15:  2056132 frTx 2063094 frRx 0 LLI_errs. <looped-0>
Central Memory OK
Total Diag Frames Tx: 31712
Total Diag Frames Rx: 32816
value = 0
```

sramRetentionTest

The **sramRetentionTest** command tests the data retention of the miscellaneous SRAMs in ASIC.

Syntax

```
sramRetentionTest [passcount]
```

Availability

Administrator

Description

Use this command to verify that data written into the miscellaneous SRAMs in the ASIC are retained after a 10-second wait.

The method used is to write a fill pattern to all SRAMs, wait 10 seconds, and then read all SRAMs checking that data read matches data previously written. Repeat using the complementary version of the pattern.

The following patterns are used:

```
0xffffffff (and 0x00000000)
0x55555555 (and 0xaaaaaaaa)
0x33333333 (and 0xcccccccc)
0x0f0f0f0f (and 0xf0f0f0f0)
QUAD_RAMP with a random seed value (and its invert)
```

Below are the possible error messages if failures are detected:

DIAG-REGERR

DIAG-REGERR_UNRST

DIAG-BUS_TIMEOUT

Operands

This command has the following operand:

passCount

Specify the number of times to run the test. The default value is 1. This command is optional.

Example

The following example shows turning off the dynamic load sharing option.

```
sw7:admin> sramRetentionTest
Running SRAM Retention Test ... passed.
```

See also

camTest

centralMemoryTest

cmemRetentionTest

cmiTest

crossPortTest

portLoopbackTest

ramTest

spinSilk

supportShow

The **supportShow** command prints switch information for debugging.

Syntax

```
supportShow [firstPort, lastPort, nLog]
```

Availability

All users

Description

Use this command to print the switch information for debugging purposes. This command runs the listed commands in the following order:

1. **version**
2. **tempShow**
3. **psShow**
4. **licenseShow**
5. **diagShow**
6. **errDump**
7. **switchShow**
8. **portFlagsShow**
9. **portErrShow**
10. **mqShow**
11. **portSemShow**
12. **portShow**
13. **portRegShow**
14. **portRouteShow**
15. **fabricShow**
16. **topologyShow**
17. **qlShow**
18. **nsShow**
19. **nsAllShow**
20. **cfgShow**
21. **configShow**

22. **faultShow**
23. **traceShow**
24. **portLogDump**

Operands

This command has the following operands:

firstPort Specify the first port, of a range of ports, to dump information. The default (if no operand specified) is to print state of port `0`. If only `firstPort` is specified, only information for `firstPort` is printed.

lastPort Specify the last port, of range of ports, to dump information. If `firstPort` is specified but `lastPort` is not specified, only `firstPort` information is printed for the port based commands (`portShow`, `portRegShow`, `portRouteShow`). If no operand is supplied, `firstPort` is set to `0` and `lastPort` is set to the maximum port of the switch.

nLog Specify the number of lines of **portLogDump** to print:

`0` = dump all lines (default)

`N` = dump the last N lines

`<0` = skip `portLogDump`

Example

```
sw7:admin> supportShow
Kernel: 5.3.1
Fabric OS: v2.1
Made on: Tue Apr 6 16:57:22 PDT 1999
Flash: Thu Apr 1 10:23:43 PST 1999
BootProm: Thu Oct 1 13:34:29 PDT 1998
37 34 37 45 49 Centigrade
98 93 98 113 120 Fahrenheit
Power Supply #1 is absent
Power Supply #2 is absent
byRdzdSRxyczSe0D:
Web license
Diagnostics Status: Tue Apr 6 16:22:34 1999
```

switchBeacon

The **switchBeacon** command sets the switch beaconing mode on or off.

Syntax

```
switchBeacon mode
```

Availability

Administrator

Description

Use this command to set the switch beaconing mode on (if the operand is 1) or off (if the operand is 0).

When beaconing mode is turned on, the port LEDs flash amber in a running pattern from port 0 to port 7, and then back again. You see a running pattern in amber LEDs, from left to right and right to left. The pattern continues until the switch is turned off.

Beaconing mode affects only the port LEDs. Other commands are still functional. The normal flashing LED pattern (associated with an active, faulty, or disabled port) is suppressed and the beaconing pattern is shown. However, if diagnostic frame-based tests **portLoopbackTest**, **crossPortTest**, and **spinSilk** are run, two patterns are interleaved. The diagnostic test flickers the LEDs green and the beaconing mode simultaneously runs the LEDs amber.

Use the **switchShow** command to display the status of beaconing.

Operands

This command has the following operand:

mode Specify `1` to enable beacon mode or `0` to disable beacon mode. This operand is required.

Example

The following example shows turning beaconing mode on:

```
sw5:admin> switchBeacon 1
```

The following example shows turning beaconing mode off:

```
sw5:admin> switchBeacon 0
```

See also

switchShow

switchDisable

The **switchDisable** command disables the switch.

Syntax

```
switchDisable
```

Availability

Administrator

Description

Use this command to disable the switch. All fibre-channel ports are taken offline; if the switch was part of a fabric, the remaining switches reconfigure.

The switch must be disabled before making configuration changes (using **configure** or **configDefault**) or before running many of the diagnostic tests. All commands that require the switch to be disabled send an error if invoked while the switch is enabled.

The switch does not need to be disabled before restarting or powering off.

As each port is disabled, the front panel LED changes to a slow flashing yellow.

Operands

None

Example

The following example shows disabling the switch:

```
sw5:admin> switchDisable
```

See also

switchEnable
switchShow

switchEnable

The **switchEnable** command enables the switch.

Syntax

```
switchEnable
```

Availability

Administrator

Description

Use this command to enable the switch. All fibre-channel ports that have passed POST are enabled. They can come online if connected to a device, or remain offline if disconnected. A switch might need to be enabled if it was previously disabled to make configuration changes or to run diagnostics.

If the switch is connected to a fabric, it rejoins the fabric. When this command is issued, the 10-second fabric stability countdown is displayed. If this switch remains the principal switch at the end of the count down, it assigns itself a domain ID. If another switch assumes the principal role, this switch becomes a subordinate switch and accepts a domain ID from the principal. See “switchDisable” on page 155 and “switchEnable” on page 155 for more information about this process.

As each port is enabled, the front panel LED changes to green for online ports, black for disconnected ports, or yellow for uninitialized ports.

Operands

None

Example

The following example shows enabling the switch:

```
sw5:admin> switchEnable
10 9 8 7 6 5 4 3 2 1
fabric: Principal switch
fabric: Domain 1
```

See also

switchDisable
switchShow

switchName

The **switchName** command displays or sets the switch name.

Syntax

```
switchName [“newName”]
```

Availability

All users (display)

Administrator (set)

Description

Use this command without an operand to display the current switch name. This name is also shown in the Telnet prompt, under each switch icon on the 2109 Web Tools fabric view, and in the output of many Telnet commands.

Use this command with the newName operand to assign a new switch name. Switch names can be up to 19 characters long, must begin with an alpha character, and can consist of a combination of alpha, numeric, and underscore characters.

Changing the switch name causes a domain address format RSCN to be issued.

Operands

This command has the following operand:

"newName"
Specify a new name for the switch, in quotation marks. This operand is optional.

Example

The following example shows changing a switch name to sw10:

```
sw5:admin> switchName “sw10”
Updating flash ...
sw10:admin>
```

See also

switchShow
fabricShow

switchShow

The **switchShow** command displays the switch and port status.

Syntax

```
switchShow
```

Availability

All users

Description

Use this command to display switch and port status information. Information can vary by switch model. Following is a description of the information provided. The first section provides switch summary information; it is followed by a section covering summary information by port.

Switch summary information:

switchName
Switch symbolic name.

switchType
Switch model and revision numbers.

switchState
Switch state: online, offline, testing, faulty.

switchRole
Switch role: principal, subordinate, disabled.

switchDomain
Switch domain ID: 0 -3 1 or 1 -2 39.

switchId
Switch embedded port D_ID.

switchWwn
Switch world-wide name.

switchBeacon
The beaconing state of the switch (either on or off).

The switch summary is followed by one line per port:

port number
Port number: 0 - 7.

module type
Port module type (GBIC or other).

Blank No module present.

sw Shortwave laser.

lw Longwave laser.

cu Copper.

id Serial ID.

port state

Port state.

No_Card No interface card present.

No_Module No module (GBIC or other) present.

No_Light Module is not receiving light.

No_Sync Module is receiving light but is out of sync.

In_Sync Module is receiving light and is in sync.

Laser_Flt Module is signaling a laser fault.

Port_Flt Port marked faulty.

Diag_Flt Port failed diagnostics.

Lock_Ref Locking to the reference signal.

Testing Running diagnostics.

Online Port is up and running.

comment

The comment field can be blank, or it can display:

Disabled Port is disabled.

Bypassed Port is bypassed (loop only).

Loopback Port is in loopback mode.

E-port Fabric port, shows WWN of attached switch.

F-port Point-to-point port, shows WWN of attached port.

G-port Point-to-point but not yet E-port or F-port.

L-port Loop port, shows number of NL_ports.

Operands

None

Example

The following example shows an 8-port hub:

```
Sr99:admin> switchshow
switchName: Sr99
switchType: 4.1
switchState: Online
switchRole: Principal
switchDomain:1
switchId: fffc01
switchWwn: 10:00:00:60:69:00:73:71
switchBeacon: OFF
port 0: sw No_Light
port 1: sw No_Light
port 2: lw No_Light
port 3: sw No_Light
port 4: sw No_Light
port 5: sw No_Light
port 6: sw No_Light
port 7: sw No_Light
Sr99:admin>
```

See also

switchDisable
switchEnable
switchName

switchStatusPolicySet

The **switchStatusPolicySet** command sets the policy parameters that determine the overall switch status.

Syntax

```
switchStatusPolicySet
```

Availability

Administrator

Description

This command enables you to set the policy parameters for calculating the overall status of the switch (enclosure). The policy parameter values determine how many failed or faulty units of each contributor are allowed before triggering a status change in the switch from healthy to marginal or down.

The command prints the current parameters in a three-column table format. The first column contains the contributor; the second column specifies the minimum number that contributes to the down or failed status; the third specifies the minimum number that contributes to the marginal or warning status. The command then prompts you to change the values for each policy parameter. The default values for the policy parameters are as follows:

Contributor	Default value for down	Default value for marginal
FaultyPorts	2	1
MissingGBICs	0	0
PowerSupplies	1	0
Temperatures	2	1
Fans	2	1
PortStatus	0	0

Any single contributor can force the overall status of the switch to marginal or down.

This command enables you to set a threshold for each contributor, so that a certain number of failures are allowed before changing the status of the switch.

Note: If the value of a policy parameter is 0, it means that this factor is not used to determine the status of the switch. For example, if FaultyPorts marginal parameter is set to 0, then any number of ports going down does not trigger a marginal status for the switch.

If the range of values for a particular contributor are set to 0 for both marginal and down, that contributor is not used in the calculation of the overall switch status.

Operands

None

Example

Notice that in the following example, the only parameters that are modified are the number of FaultyPorts allowed before the status of the switch changes to marginal and down.

```
ssw5:admin> switchStatusPolicySet
     To change the overall switch status policy parameters
     The current overall switch status policy parameters:
                         Down      Marginal
  -------------------------------------------------
     FaultyPorts         1         0
     MissingGBICs        0         1
     PowerSupplies       2         1
     Temperatures        2         1
     Fans                2         1
     PortStatus          0         0
The value 0 for a parameter means that it is not used in the calculation.

In addition, if the range of settable values in the prompt is (0..0) the policy
parameter is not applicable to the switch.

Simply hit the Return key.

The minimum number of:
FaultyPorts contributing to DOWN status: (0..8) [1] 2
FaultyPorts contributing to MARGINAL status: (0..8) [0] 1
MissingGBICs contributing to DOWN status: (0..8) [0]
MissingGBICs contributing to MARGINAL status: (0..8) [1]
bad PowerSupplies contributing to DOWN status: (0..2) [2]
bad PowerSupplies contributing to MARGINAL status: (0..2) [1]
bad Temperatures contributing to DOWN status: (0..5) [2]
bad Temperatures contributing to MARGINAL status: (0..5) [1]
bad Fans contributing to DOWN status: (0..6) [2]
bad Fans contributing to MARGINAL status: (0..6) [1]
PortStatus gone DOWN contributing to DOWN status: (0..8) [0]
PortStatus gone DOWN contributing to MARGINAL status:(0..8) [0]
Policy parameter set has been changed
... Committing configuration...done.
```

See also

switchStatusPolicyShow
switchStatusShow

switchStatusPolicyShow

The **switchStatusPolicyShow** command displays the policy parameters that determine the overall switch status.

Syntax

```
switchStatusPolicyShow
```

Availability

All users

Description

This command enables you to view the current policy parameters that are set for the switch. These policy parameters determine the number of failed or nonoperational units allowed for each contributor before triggering a status change in the switch.

The command prints the current parameters in a three-column table format. The first column contains of the contributor; the second column specifies the minimum number that contributes to the down or failed status; the third specifies the minimum number that contributes to the marginal or warning status. The default values for the policy parameters are as follows:

Contributor	**Default value for down**	**Default value for marginal**
FaultyPorts	2	1
MissingGBICs	0	0
PowerSupplies	1	0
Temperatures	2	1
Fans	2	1
PortStatus	0	0

The policy parameters determine the number of failed or nonoperational units for each contributor that trigger a status change in the switch. For example, if the FaultyPorts down parameter is set to 3, and three ports fail in the switch, the status of the switch changes to down.

Operands

None

Example

```
sw5:admin> switchStatusPolicyShow
The current overall switch status policy parameters:
                 Down    Marginal
----------------------------------------
FaultyPorts        1       0
MissingGBICs       0       1
PowerSupplies      1       0
Temperatures       3       1
Fans               3       1
PortStatus         0       0
```

See also

switchStatusShow
switchStatusPolicySet

switchStatusShow

The **switchStatusShow** command displays the overall status of the switch.

Syntax

```
switchStatusShow
```

Availability

All users

Description

This command displays the overall status of the switch. The overall status is calculated based on the most severe status of all contributors:

- Internal switch status
- Faulty ports
- Missing GBICs
- Power supplies
- Fans
- Temperatures
- Port status

The overall status can be one of the following:

- Healthy/OK: every contributor is healthy
- Marginal/Warning: one or more components are causing a warning status
- Down/Failed one or more contributors have failed

If the overall status is not healthy/OK, the contributing factors are listed.

Operands

None

Example

Two examples of the **switchStatusShow** command follow. The first example shows a switch with a status of marginal, the second example shows the same switch after all the errors have been corrected.

```
sw44:admin> switchStatusShow
The overall switch status is Marginal/Warning
Contributing factors:
* 1 missing power supply triggered the Marginal/Warning status
* 2 bad fans, 4 good fans triggered the Marginal/Warning status
* 1 missing GBIC triggered the Marginal/Warning status
...
```

```
sw44:admin> switchStatusShow
The overall switch status is HEALTHY/
OK
```

See also

switchStatusPolicyShow
switchStatusPolicySet

syslogdIpAdd

The **syslogdIpAdd** command adds the IP address of a syslog daemon.

Syntax

```
syslogdIpAdd IP_address
```

Availability

Administrator

Description

Use this command to add the IP address of a syslog daemon, that is the IP address of the server, which is running the syslogd process. Syslog daemon (syslogd) is a process available on most UNIX systems that reads and forwards system messages to the appropriate log files or users, depending on the system configuration.

When one or more IP addresses are configured, the switch forwards all error log entries to the syslogd on the specified servers. Up to six servers are supported.

Operands

This command has the following operand:

IP_address
Specify the IP address of the server running syslogd. This operand is required.

Example

The following example shows adding the address 192.168.1.60 to the list of machines to which system messages are sent:

```
sw5:admin> syslogdIpAdd “192.168.1.60”
Committing configuration...done.
```

See also

errShow
syslogdIpRemove
syslogdIpShow

syslogdIpRemove

The **syslogdIpRemove** command removes the IP address of a syslog daemon.

Syntax

```
syslogdIpRemove IP_address
```

Availability

Administrator

Description

Use this command to remove the IP address of a syslog daemon, that is the IP address of the server that is running the syslogd process.

Operands

This command has the following operand:

IP_address
Specify the IP address of the server running syslogd. This operand is required.

Example

The following example shows removing the address 192.168.1.60 from the list of machines to which system messages are sent:

```
sw5:admin> syslogdIpRemove “192.168.1.60”
Committing configuration...done.
```

See also

errShow
syslogdIpAdd
syslogdIpShow

syslogdIpShow

The **syslogdIpShow** command displays all syslog daemon IP addresses.

Syntax

```
syslogdIpShow
```

Availability

All users

Description

Use this command to display all syslog daemon IP addresses in the configuration database.

Operands

None

Example

```
sw5:admin> syslogdIpShow
syslog.IP.address.1: 192.168.1.60
syslog.IP.address.2: 192.168.1.88
syslog.IP.address.3: 192.168.2.77
```

See also

errShow
syslogdIpAdd
syslogdIpRemove

tempShow

The **tempShow** command displays the temperature readings.

Syntax

```
tempShow
```

Availability

All users

Description

Use this command to display the current temperature readings from each of five temperature sensors located on the main printed circuit board of the switch. One sensor is located in each corner and one is located at the center of the printed circuit board.

Operands

None

Example

```
sw5:admin> tempShow
43   40   44   48   5    Centigrade
109  104  111  118  113  Fahrenheit
```

See also

fanShow
psShow

topologyShow

This **topologyShow** command displays the unicast fabric topology.

Syntax

```
topologyShow [domain_number]
```

Availability

All users

Description

Use this command to display the fabric topology, as it is displayed to the local switch.

This includes:

- A list of all domains that are part of the fabric, and to each of those domains, all possible paths from the local switch.
- For each path, the cost, the number of hops from the local switch to the destination switch, the name of the destination switch, and a summary of all ports that are routed through that path.

In order for a frame to reach the correct domain, the output port describes the path to be taken through the routing hardware of the switches.

With the domain number specified, this command displays the topology information for the specified destination domain.

The display contains the following fields:

Local Domain ID
The domain number of the local switch.

Domain The domain number of the destination switch.

Metric The cost of reaching the destination domain.

Hops The number of hops to reach the destination domain.

Out Port The port that the incoming frame is forwarded to, in order to reach the destination domain.

In Ports (see note)
The bit map of the input ports uses the corresponding bit map of the out port to reach the destination domain. A bit set to 1

indicates that the port is being routed through the corresponding out port. The least significant bit represents port 0.

Note: This is the same information provided in a different format by the **portRouteShow** command and the **uRouteShow** command.

Flags Always “D”, indicating a dynamic path. A dynamic path is discovered automatically by the FSPF path selection protocol.

Name The name of the destination switch.

Operands

This command has the following operand:

domain_number
Specify the destination domain for which topology information is to be displayed. This operand is optional.

Example

```
switch:admin> topologyShow
Local Domain ID: 1
Domain   Metric  Hops  Out Port    In Ports    Flags   Name
----------------------------------------------------------------------
0        1000    1      2          0x00002000  D       “sw25”
                 1      6          0x00000000  D
                 1      7          0x00000000  D

Type <CR> to continue, Q<CR> to stop:
3        1000    1     13          0x000000c4  D       “sw4”
Type <CR> to continue, Q<CR> to stop:
4        2000    2      2          0x00002000  D       “sw10”
                 2      6          0x00000000  D
                 2      7          0x00000000  D

Type <CR> to continue, Q<CR> to stop:

8        2000    0      2          0x00002000  D       “sw16”
                 0      6          0x00000000  D
                 0      7          0x00000000  D
switch:admin> topologyShow 4
Local Domain ID: 1
Domain   Metric  Hops  Out Port    In Ports    Flags   Name
---------------------------------------------------------------
4        2000    2      2          0x00002000  D       “sw10”
                 2      6          0x00000000  D
                 2      7          0x00000000  D
```

See also

portRouteShow
uRouteShow

trackChangesSet

The **trackChangesSet** command allows configuring of the track-changes feature.

Syntax

```
trackChangesSet [mode], [snmptrapmode]
```

Availability

Administrator

Description

Use this command to enable and disable the track-changes feature. Also use it to enable or disable an SNMP trap. Trackable changes are:

- Successful login
- Unsuccessful login
- Logout
- Config file change from task
- Track-changes on
- Track-changes off

Operands

This command has the following operands:

Mode 1 = enable track-changes feature

0 = disable track-changes feature (default)

snmptrapmode
1 = send SNMP trap in addition to errlog

0 = do not send SNMP trap (default)

Example

```
sw:admin> trackChangesSet 1, 0
0x10f9bcd0 (tShell): Feb 10 15:04:38
     Error TRACK-TRACK_ON, 4, Track-changes on
Committing configuration...done.
0x10f9bcd0 (tShell): Feb 10 15:04:42
     Error TRACK-CONFIG_CHANGE, 4, Config file change from
task:tShell
sw:admin> trackChangesSet 0, 0
0x10f9bcd0 (tShell): Feb 10 15:04:50
     Error TRACK-TRACK_OFF, 4, Track-changes off
Committing configuration...done.
```

uptime

The **uptime** command displays the length of time the system has been operational.

Syntax

```
uptime
```

Availability

All users

Description

Use this command to display the length of time that the system has been in operation (also known as “up time”), the total cumulative amount of “up time” since the system was first started up, the date and time of the last restart, and the reason for the last restart.

For up and startup times less than 60 seconds, the time is displayed in seconds. For times greater than or equal to 60 seconds, the time is displayed in minutes. The output format adjusts accordingly.

The reason for the last switch restart is also recorded in the error log. The reasons for the last restart of the switch are listed in the following table. Not all reasons are applicable to all switch models:

Table 20. Descriptions of the reasons for the last start of the switch

Field	Description
Bus time-out (see note)	The port ASIC was accessed and no response was received.
Bus error (see note)	A nonexistent system address was accessed.
Panic (see note)	The firmware detected a critical hardware error or an internal inconsistency.
Fault (see note)	A CPU signaled a fault condition (critical firmware error).
Power-on	The last restart was caused by a power-on.
Watchdog (see note)	The watchdog timer caused a reset.
PushButtons	Pushbuttons 1 and 3 were pressed for two seconds, causing a system reset.
Restart	The last restart was caused by a user (from any management interface).
Powerfail NMI (see note)	The power supply caused a nonmaskable interrupt.
Watchdog NMI (see note)	The watchdog timer caused a nonmaskable interrupt.

Field	Description
PushButton NMI (see note)	Push buttons 2 and 4 were pressed for two seconds, causing a nonmaskable interrupt.
Software NMI (see note)	The firmware caused a nonmaskable interrupt.
Note: Caused by hardware or firmware failures. Information about the failure is stored in the switch. Follow the procedures in the switch manual.	

Operands

None

Example

```
sw5:admin> uptime
Up for: 3 days, 18:35
Powered for: 30 days, 16:05
Last up at: Mon Mar 22 12:00:00 1999
Reason: Power-on
```

See also

date
errShow
fastboot
reboot

uRouteConfig

The **uRouteConfig** command configures a static route.

Syntax

```
uRouteConfig [port_number, domain_number,
output_port_number]
```

Availability

Administrator

Description

Use this command to configure static routes. A static route is assigned a specific path; the path does not change with a topology change unless the path becomes unavailable.

After this command is issued, and if output_port_number is a usable port, all frames coming in from the port port_number that are addressed to domain_number are forwarded through the port output_port_number.

If output_port_number is not usable, the routing assignment is not affected. When output_port_number becomes usable the static route that is assignment for port_number is enforced.

output_port_number is usable if the associated neighbor is in B_ST_FULL state. See **interfaceShow** on page 223 for more information.

Operands

This command has the following operands:

port_number
Specify the port to be statically routed; can be either an F_port or an E_port.

domain_number
Specify the destination domain.

output_port_number
Specify the output port where traffic is to be forwarded.

Notes

Using static routes can affect load sharing. If a large number of routes are statically configured to the same output port, the ability of the switch to achieve optimum load sharing can be impaired.

To prevent routing loops, static route configuration using a nonminimum cost path is not allowed. If you attempt to configure such a route, you are asked if the entry should be saved in the database.

Example

The following example shows configuring a static route for all traffic coming in from port 1 and addressed to domain 2, to go through port 5:

```
switch:admin> uRouteConfig 1,2,5
The configuration will now contain the static route:
switch:admin> configShow “route”
route.ucastRoute.1.2: 5
route.ucastRouteCount: 1
```

See also

configShow
interfaceShow
uRouteRemove
uRouteShow

uRouteRemove

The **uRouteRemove** command removes a static route.

Syntax

```
uRouteRemove port_number, domain_number
```

Availability

Administrator

Description

Use this command to remove a statically configured route.

When this command is issued, the route to domain_number for port_number does not change. It does not change if the previous static route was along a minimum cost path. After this command is issued, the load sharing to the domain domain_number is re-evaluated.

Operands

This command has the following operands:

port_number
Specify the port to be statically routed; can be either an F_port or an E_port.

domain_number
Specify the destination domain.

Example

The following example shows removing a static route for all traffic coming in from port 1 and addressed to domain 2:

```
switch:admin> uRouteRemove 1, 2
```

See also

configShow
uRouteConfig
uRouteShow

uRouteShow

The **uRouteShow** command displays unicast routing information.

Syntax

```
uRouteShow [port_number] [domain_number]
```

Availability

All users

Description

Use this command to display the unicast routing information for a port, as it is known by the FSPF path selection and routing task. The routing information describes how a frame, that is received from a port on the local switch, is to be routed to reach a destination switch.

The following fields are displayed:

Local Domain ID
The domain number of the local switch.

In Port The port from which a frame is received.

Domain The destination domain of the incoming frame

Out Port The port to which the incoming frame is to be forwarded.

Metric The cost of reaching the destination domain.

Hops The number of hops that are required to reach the destination domain.

Flags Indicates if the route is dynamic (D) or static (S). A dynamic route is discovered automatically by the FSPF path selection protocol. A static route is assigned using the **uRouteConfig** command.

Next (Dom, Port)
The domain and port number of the next hop. These are the domain number and the port number of the switch to which Out Port is connected.

This command provides the same information as the **portRouteShow** command and the **topologyShow** command.

Operands

This command has the following operands:

No operand

Displays routing information for all active ports on the local switch, to all the domains in the fabric.

port_number

Displays routing information for the port port_number to all the domains in the fabric.

port_number, domain_number

Displays routing information for the port port_number to the domain domain_number.

Example1

```
switch:admin> uRouteShow

Local Domain ID: 1

In port   Domain    Out      Metric    Hops       Flags     Next
                    port                                    (Dom,por
                                                            t)

2         3         13       1000      1          D         3,7

Type <CR> to continue, Q<CR> to stop:

6         3         13       1000      1          D         3,7

Type <CR> to continue, Q<CR> to stop:

13        0         7        1000      1          D         0,8

          4         2        2000      2          D         0,13

switch:admin> uRouteShow 13

Local Domain ID: 1

In port   Domain    Out      Metric    Hops       Flags     Next
                    port                                    (Dom,por
                                                            t)

13        0         7        1000      1          D         0,8

          4         2        2000      2          D         0,13
```

See also

portRouteShow
topologyShow
uRouteConfig

version

The **version** command displays the firmware version information.

Syntax

```
version
```

Availability

All users

Description

Use this command to display firmware version information and build dates. The following fields are displayed:

Kernel The version of the switch kernel operating system.

Fabric OS
The version of the switch Fabric OS.

Made on The build date of the firmware running in switch.

Flash The build date of the firmware stored in flash proms.

BootProm
The build date of the firmware stored in boot prom.

Usually the Made On and Flash dates are the same, because the switch starts running flash firmware at startup time. However, in the time period between the firmware download and the next restart, the dates can differ.

Operands

None

Example

The following example shows displaying firmware version information:

```
sw5:admin> version
Kernel: 5.3.1
Fabric OS: v2.1
Made on: Fri Jan 22 15:21:20 PST 1999
Flash: Fri Jan 22 15:21:20 PST 1999
BootProm: Tue Dec 29 17:32:00 PST 1998
```

See also

firmwareDownload
restart

zoneAdd

The **zoneAdd** command adds a member to a zone.

Syntax

```
zoneAdd zoneName, zoneMemberList
```

Availability

Administrator

Description

Use this command to add one or more members to an existing zone.

Operands

The following operands are required:

zoneName
Name of the zone in quotes.

zoneMemberList
List of members to be added to zone, in quotes, separated by semicolons.

Can be one or more of the following:

- Physical fabric port number
- World-wide name
- QuickLoop AL_PA
- Zone alias name

Example

The following example shows adding alias for 3 disk arrays to “Blue_zone”:

```
sw:admin> zoneAdd “Blue_zone”, “array3; array4; array5”
```

Note: Use this command only if the devices that are connected to the fabric cannot handle occasional routing changes.

See also

zoneCreate

zoneDelete

zoneRemove

zoneShow

zoneCreate

The **zoneCreate** command creates a zone alias.

Syntax

```
zoneCreate zoneName, zoneMemberList
```

Availability

Administrator

Description

Use this command to create a zone.

A zone name is a C-style name beginning with a letter and followed by any number of letters, digits and underscore characters. Names are case sensitive, for example “Zone_1” indicates a different zone than “zone_1”. Blank spaces are ignored.

The zone member list must have at least one member (empty lists are not allowed). The members are described by a list of member definitions separated by semicolons.

Specify a physical fabric port number as a pair of decimal numbers “s.p.” where “s” is the switch number (domain ID) and “p” is the port number on that switch. For example, “2.12” specifies port 12 on switch number 2. When a zone member is specified by physical fabric port number, then all devices connected to that port are in the zone. If this port is an arbitrated loop, then all devices on the loop are in the zone.

Specify a world-wide name as 8 hex numbers separated by colons, for example“10:00:00:60:69:00:00:8a”. Zoning has no knowledge of the fields within a world-wide name; the eight bytes are simply compared with the node and port names presented by a device in a login frame (FLOGI or PLOGI). When a zone member is specified by node name, then all ports on that device are in the zone. When a zone member is specified by port name, then only that single device port is in the zone.

Specify a QuickLoop AL_PA as a QuickLoop name followed by a list of AL_PAs, for example “qloop1[01,02]”. QuickLoop names have the same format as zone names, and are created with the **qloopCreate** command to define a switch or pair of switches that form the QuickLoop.

Specify a zone alias name using the same format as a zone name; it is created with the **aliCreate** command. The alias must resolve to a list of one or more of the following:

- Physical fabric port numbers
- World-wide names

- QuickLoop AL_PAs

The types of zone members used to define a zone can be mixed. For example, a zone defined with the following members: “2,12; 2,14; 10:00:00:60:69:00:00:8a” would contain all devices connected to switch 2, port 12 and 14, and to the device with the world-wide name “10:00:00:60:69:00:00:8a” (either node name or port name), at the port in the fabric to which it is connected.

Operands

The following operands are required:

zoneName
Name for a zone to be created, in quotes. This name cannot be used for another zone object.

zoneMemberList
List of members to be included in zone, in quotes, separated by semicolons. Can be one or more of the following:

- Physical fabric port numbers
- World-wide names
- QuickLoop AL_PAs
- Zone alias names

Example

The following example shows creating 3 zones using a combination of port numbers and zone aliases:

```
sw:admin> zoneCreate “Red_zone”, “1,0; loop1”
sw:admin> zoneCreate “Blue_zone”, “1,1; array1; 1,2; array”
sw:admin> zoneCreate “Green_zone”, “1,0; loop1; 1,2; array”
```

See also

zoneAdd

zoneDelete

zoneRemove

zoneShow

zoneDelete

The **zoneDelete** command deletes a zone.

Syntax

```
zoneDelete zoneName
```

Availability

Administrator

Description

Use this command to delete a zone.

Operands

The following operand is required:

zoneName
Name of zone to be deleted, in quotes.

Example

The following example shows deleting zone “Blue_zone”:

```
sw:admin> zoneDelete “Blue_zone”
```

See also

zoneAdd

zoneCreate

zoneRemove

zoneShow

zoneRemove

The **zoneRemove** command removes a member from a zone.

Syntax

```
zoneRemove zoneName, zoneMemberList
```

Availability

Administrator

Description

Use this command to remove one or more members from an existing zone.

The member list is located by an exact string match; therefore, it is important to maintain the order when removing multiple members. For example, if a zone contains “array2; array3; array4” then removing “array3; array4” succeeds, but removing “array4; array3” fails.

If all members are removed, the zone is deleted.

Operands

The following operands are required:

zoneName
Name of zone, in quotes.

zoneMemberList
List of members to be removed from zone, in quotes, separated by semicolons. Can be one or more of the following:

- Physical fabric port numbers
- World-wide names
- QuickLoop AL_PAs
- Zone alias names

Example

The following example shows removing “array3”from the “Blue_zone”:.

```
sw:admin> zoneRemove “Blue_zone”, “array2”
```

See also

zoneAdd

zoneCreate

zoneDelete

zoneShow

zoneShow

The **zoneShow** command displays zone information.

Syntax

```
zoneShow [pattern]
```

Availability

All users

Description

Use this command to display zone configuration information.

If no parameters are specified, all zone configuration information (both defined and enabled) is displayed. See “cfgShow” on page 157 for a description of this display.

If a parameter is specified, it is used as a pattern to match zone configuration names; those that match in the defined configuration are displayed.

Operands

The following operand is optional:

pattern A POSIX-style regular expression used to match zone configuration names.

Patterns can contain:

- Question mark “?” that matches any single character
- Asterisk “*” that matches any string of characters
- Ranges “[0–9a-f]” that match any character within the range

Example

The following example shows all zones beginning with the letters “A” - “C”:

```
sw:admin> zoneShow “[A-C]*”
zone: Blue_zone 1,1; array1; 1,2; array2
```

See also

zoneAdd

zoneCreate

zoneDelete

zoneRemove

Appendix C. Veritas DMP settings in the fabric environment

Introduction

An issue has been observed in meshed fabric configurations of switches that affect disk I/O delay when operating in a Veritas dual-path SUN Solaris environment. There are three configuration settings that you must be aware of in order to plan for any path failures. These involve the Solaris sd driver, the host bus adapter driver settings, and the Veritas DMP parameter settings.

Analysis

The issue just described has been observed in a multi-switch fabric (including the Silkworm SW6400) with JNI FCE-6410 and Emulex LP8000 HBA devices. This issue has replicated in our test labs. Disk-attached devices have included the HDS 9960 Lightning RAID Storage array, though the problem is considered generic to any disk devices in use. The failure of an internal (active) inter-switch link replicates the issue observed where the disk I/O being interrupted does not immediately failover to another available alternate path within the fabric and subsequently causes up to a 60-second delay before resuming. The three configuration parameter settings to be aware of are:

- Veritas Dynamic MultiPathing (DMP)
- Host bus adapter settings
- Solaris sd driver parameter settings

Resolution and workaround

Veritas Dynamic MultiPathing (DMP)

Veritas Volume Manager incorporates a feature that enables multiport disk arrays to be connected to host systems through multiple paths. In the event of a loss of one connection to the array, DMP automatically routes the I/Os over the other available connections to the array. When using certain active/active Disk arrays (such as the HDS 9960) this feature provides greater I/O throughput by balancing the load uniformly across multiple I/O paths to the disk devices. The daemon within the Volume Manager that monitors the condition of available paths is called the *restore* daemon. The restore daemon re-examines the condition at a specified interval using a specified policy. The following command starts the restore daemon with a polling interval of 10 seconds using the check_all policy, which analyses all paths in the system and revives the paths that are back online, as well as disabling the paths that are inaccessible:

```
# vxdmpadm start restore interval=10 policy=check_all
```

Host bus adapter settings

Most host bus adapter vendors incorporate a parameter in their driver that defines the delay before failing all I/O for an offline target. This failure must occur before the DMP feature of Veritas can take over and continue I/Os to the other available path. In the case of the JNI FCE-6410 adapter, the user must edit the /kernel/drv/jnic.conf file to set the FailoverDelay parameter as follows:

```
# Configuration parameter: FailoverDelay
# Type: integer
# Default: 0 (sec)
#
# Delay (seconds) before failing all I/O for an offline target. If the delay
# timer expires, all I/O for the failed target is returned to the application.
# A zero value disables failover.
#
FailoverDelay = 2;
```

For testing purposes, this value was set to 2 seconds in order to introduce almost no delay in the I/O, but you must decide what value applies to your particular application. For the Emulex LP8000, this parameter is called *linkdown-tmo* and resides in the /kernel/drv/lpfc.conf file.

Solaris sd driver parameter settings

In addition to the previously mentioned delays, the Solaris sd driver adds a third source of delay that you must consider. For Solaris V2.8, the sd driver timeout value defaults to 60 seconds (or 0x3C). This value may be changed by editing the /etc/system file and adding the following line:

```
set sd:sd_io_time = 0xa è
```

This example is for a value of 10 seconds. This value must be expressed in hex format.

The grand total of time delay possible would be the sum of the three delays shown in the following example:

```
DMP delay + HBA driver delay + Solaris delay = Total I/O delay before failover to
alternate path
```

Pro-active fabric changes (changes done by a SAN administrator in managing the fabric) should not be done during any active data I/O process. It is recognized that this may be a significant limitation within an operation. It is recommended that the following guidelines be followed for minimizing I/O disruption:

- Do not add or delete an inter-switch link during active I/O periods.
- Do not add or remove a switch from the fabric during I/O periods.
- Do not modify zones and configure new zones during I/O periods.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

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

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

The following paragraph does not apply to the United Kingdom or another country where such provisions are inconsistent with local law:

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

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

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

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

IBM
StorWatch

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft Windows and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

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

Electronic emission notices

This section gives the electronic emission notices or statements for the United States and other countries.

Federal Communications Commission (FCC) statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors, or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation

Industry Canada compliance statement

This Class A digital apparatus complies with Canadian ICES-003.

Avis de conformite a la reglementation d’Industrie Canada: Cet appareil numerique de la classe A est conform a la norme NMB-003 du Canada.

European community compliance statement

This product is in conformity with the protection requirements of EC Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a nonrecommended modification of the product, including the fitting of non-IBM option cards.

This product is in conformity with the EU council directive 73/23/EEC on the approximation of the laws of the Member States relating to electrical equipment designed for use within certain voltage limits. This conformity is based on compliance with the following harmonized standard: EN60950.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to European Standard EN 55022. The limits for Class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

Attention: This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

Where shielded or special cables (for example, cables fitted with ferrites) are used in the test to make the product comply with the limits:

Properly shielded and grounded cables and connectors must be used in order to reduce the potential for causing interference to radio and TV communications and to other electrical or electronic equipment. Such cables and connectors are available from IBM authorized dealers. IBM cannot accept responsibility for any interference caused by using other than recommended cables and connectors.

Germany compliance statement

Zulassungsbescheinigung laut Gesetz ueber die elektromagnetische Vertraeglichkeit von Geraeten (EMVG) vom 30. August 1995.

Dieses Geraet ist berechtigt, in Uebereinstimmung mit dem deutschen EMVG das EG-Konformitaetszeichen - CE - zu fuehren.

Der Aussteller der Konformitaetserklaeung ist die IBM Deutschland.

Informationen in Hinsicht EMVG Paragraph 3 Abs. (2) 2:

Das Geraet erfuellt die Schutzanforderungen nach EN 50082-1 und EN 55022 Klasse A.

EN 55022 Klasse A Geraete beduerfen folgender Hinweise:

Nach dem EMVG:

"Geraete duerfen an Orten, fuer die sie nicht ausreichend entstoert sind, nur mit besonderer Genehmigung des Bundesministeriums fuer Post und Telekommunikation oder des Bundesamtes fuer Post und Telekommunikation betrieben werden. Die Genehmigung wird erteilt, wenn keine elektromagnetischen Stoerungen zu erwarten sind." (Auszug aus dem EMVG, Paragraph 3, Abs.4)

Dieses Genehmigungsverfahren ist nach Paragraph 9 EMVG in Verbindung mit der entsprechendenKostenverordnung (Amtsblatt 14/93) kostenpflichtig.

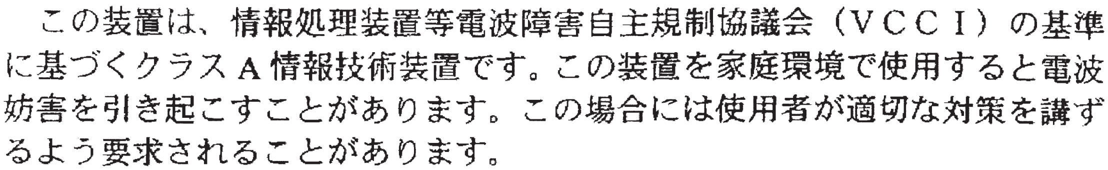
Nach der EN 55022:

"Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstoerungen verursachen. In diesem Fall kann vom Betreiber verlangt werden, angemessene Massnahmen durchzufuehren und dafuer aufzukommen."

Anmerkung:

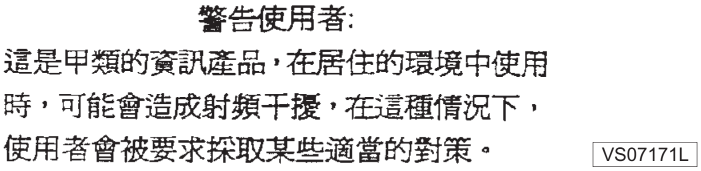
Um die Einhaltung des EMVG sicherzustellen, sind die Geraete wie in den Handbuechern angegeben zu installieren und zu betreiben.

Japanese Voluntary Control Council for Interference (VCCI) class 1 statement



この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Taiwan Class A compliance statement



警告使用者:
這是甲類的資訊產品，在居住的環境中使用
時，可能會造成射頻干擾，在這種情況下，
使用者會被要求採取某些適當的對策。

VS07171L

IBM license agreement for machine code

Regardless of how you acquire (electronically, preloaded, on media or otherwise) BIOS, Utilities, Diagnostics, Device Drivers or Microcode (collectively called “Machine Code”), you accept the terms of this Agreement by your initial use of a Machine or Machine Code. The term “Machine” means an IBM machine, its features, conversions, upgrades, elements or accessories, or any combination of them. Acceptance of these license terms authorizes you to use Machine Code with the specific product for which it is provided.

International Business Machines Corporation or one of its subsidiaries (“IBM”), or an IBM supplier, owns copyrights in Machine Code.

IBM grants you a nonexclusive license to use Machine Code only in conjunction with a Machine. As the rightful possessor of a Machine, you may make a reasonable number of copies of Machine Code as necessary for backup, configuration, and restoration of the Machine. You must reproduce the copyright notice and any other legend of ownership on each copy of Machine Code you make.

You may transfer possession of Machine Code and its media to another party only with the transfer of the Machine on which the Machine Code is used. If you do so, you must give the other party a copy of these terms and provide all user documentation to that party. When you do so, you must destroy all your copies of Machine Code.

Your license for Machine Code terminates when you no longer rightfully possess the Machine.

No other rights under this license are granted.

You may not, for example, do any of the following:

1. Otherwise copy, display, transfer, adapt, modify, or distribute in any form, Machine Code, except as IBM may authorize in a Machine’s user documentation.
2. Reverse assemble, reverse compile, or otherwise translate the Machine Code, unless expressly permitted by applicable law without the possibility of contractual waiver;
3. Sublicense or assign the license for the Machine Code; or
4. Lease the Machine Code or any copy of it.

The terms of IBM’s Machine warranty, which is incorporated into this Agreement by reference, apply to Machine Code. Please refer to that warranty for any questions or claims regarding performance or liability for Machine Code.

Statement of limited warranty

International Business Machines Corporation
Armonk, New York, 10504

The warranties provided by IBM in this Statement of Limited Warranty (Form Z125-4753) apply only to Machines you originally purchase for your use, and not for resale, from IBM or your reseller. The term “Machine” means an IBM machine, its features, conversions, upgrades, elements, or accessories, or any combination of them.

Unless IBM specifies otherwise, the following warranties apply only in the country where you acquire the Machine. If you have any questions, contact IBM or your reseller.

> **Machine:** IBM 3534 SAN Fibre Channel Managed Hub
> **Warranty Period:** One Year.*
> *Contact your place of purchase for warranty service information.

Production status

Each Machine is manufactured from new parts, or new and used parts. In some cases, the Machine may not be new and may have been previously installed. Regardless of the Machine's production status, IBM's warranty terms apply.

IBM warranty for machines

IBM warrants that each Machine 1) is free from defects in materials and workmanship and 2) conforms to IBM's Official Published Specifications. The warranty period for a Machine is a specified, fixed period commencing on its Date of Installation. The date on your receipt is the Date of Installation, unless IBM or your reseller informs you otherwise.

During the warranty period IBM or your reseller, if authorized by IBM, will provide warranty service under the type of service designated for the Machine and will manage and install engineering changes that apply to the Machine.

For IBM or your reseller to provide warranty service for a feature, conversion, or upgrade, IBM or your reseller may require that the Machine on which it is installed be 1) for certain Machines, the designated, serial-numbered Machine and 2) at an engineering-change level compatible with the feature, conversion, or upgrade. Many of these transactions involve the removal of parts and their return to IBM. You represent that all removed parts are genuine and unaltered. A part that replaces a removed part will assume the warranty service status of the replaced part.

If a Machine does not function as warranted during the warranty period, IBM or your reseller will repair it or replace it with one that is at least functionally equivalent, without charge. The replacement may not be new, but will be in good working order. If IBM or your reseller is unable to repair or replace the Machine, you may return it to your place of purchase and your money will be refunded.

If you transfer a Machine to another user, warranty service is available to that user for the remainder of the warranty period. You should give your proof of purchase and this Statement to that user. However, for Machines which have a life-time warranty, this warranty is not transferable.

Warranty service

To obtain warranty service for the Machine, you should contact your reseller or call IBM. In the United States, call IBM at 1-800-IBM-SERV (426-7378). In Canada, call IBM at 1-800-465-6666. You may be required to present proof of purchase.

IBM or your reseller will provide certain types of repair and exchange service, either at your location or at IBM’s or your reseller’s service center, to restore a Machine to good working order.

When a type of service involves the exchange of a Machine or part, the item IBM or your reseller replaces becomes its property and the replacement becomes yours. You represent that all removed items are genuine and unaltered. The replacement may not be new, but will be in good working order and at least functionally equivalent to the item replaced. The replacement assumes the warranty service status of the replaced item. Before IBM or your reseller exchanges a Machine or part, you agree to remove all features, parts, options, alterations, and attachments not under warranty service. You also agree to ensure that the Machine is free of any legal obligations or restrictions that prevent its exchange.

You agree to:

1. Obtain authorization from the owner to have IBM or your reseller service a Machine that you do not own; and
2. Where applicable, before service is provided:
   a. Follow the problem determination, problem analysis, and service request procedures that IBM or your reseller provide,
   b. Secure all programs, data, and funds contained in a Machine, and
   c. Inform IBM or your reseller of changes in a Machine's location.

IBM is responsible for loss of, or damage to, your Machine while it is 1) in IBM's possession or 2) in transit in those cases where IBM is responsible for the transportation charges.

Extent of warranty

IBM does not warrant uninterrupted or error-free operation of a Machine.

The warranties may be voided by misuse, accident, modification, unsuitable physical or operating environment, improper maintenance by you, removal or alteration of Machine or parts identification labels, or failure caused by a product for which IBM is not responsible

THESE WARRANTIES REPLACE ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THESE WARRANTIES GIVE YOU SPECIFIC LEGAL RIGHTS AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM URISDICTION TO JURISDICTION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF EXPRESS OR IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION OR LIMITATION MAY NOT APPLY TO YOU. IN THAT EVENT SUCH WARRANTIES ARE LIMITED IN DURATION TO THE WARRANTY PERIOD. NO WARRANTIES APPLY AFTER THAT PERIOD.

Limitation of liability

Circumstances may arise where, because of a default on IBM's part or other liability you are entitled to recover damages from IBM. In each such instance, regardless of the basis on which you are entitled to claim damages from IBM (including fundamental breach, negligence, misrepresentation, or other contract or tort claim), IBM is liable only for:

1. Damages for bodily injury (including death) and damage to real property and tangible personal property; and
2. The amount of any other actual direct damages or loss, up to the greater of U.S. $100, 000 or the charges (if recurring, 12 months' charges apply) for the Machine that is the subject of the claim.

UNDER NO CIRCUMSTANCES IS IBM LIABLE FOR ANY OF THE FOLLOWING: 1) THIRD-PARTY CLAIMS AGAINST YOU FOR LOSSES OR DAMAGES (OTHER THAN THOSE UNDER THE FIRST ITEM LISTED ABOVE); 2) LOSS OF, OR DAMAGE TO, YOUR RECORDS OR DATA; OR 3) SPECIAL, INCIDENTAL, OR INDIRECT DAMAGES OR FOR ANY ECONOMIC CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), EVEN IF IBM OR YOUR RESELLER IS INFORMED OF THEIR POSSIBILITY. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE EXCLUSION OR LIMITATION MAY NOT APPLY TO YOU.

Glossary

The glossary includes terms for the IBM 3534 Fibre Channel Managed Hub.

ACL. Access control list.

agent. The interface to a managed device.

alias server. A fabric software facility that supports multicast group management.

AL_PA. Arbitrated loop physical address.

ANSI. American National Standards Institute.

arbitrated loop. The FC arbitrated loop (FC-AL) is a standard defined on top of the FC-PH standard. It defines the arbitration on a loop where several FC nodes share a common medium.

ASIC. Application specific integrated circuit.

asynchronous transfer mode (ATM). A broadband technology for transmitting data over LANs or WANs based on relaying cells of a fixed size. It provides any-to-any connectivity and nodes can transmit simultaneously.

ATM. See *asynchronous transfer mode*.

BB. Buffer-to-buffer credit.

BIOS. Basic input and output system.

BISR. Built-in self-repair.

BTU. British thermal unit.

CAM. Content addressable memory.

cascading switches. Switches that are interconnected to build large fabrics.

class 2. A class of service where the fabric and destination N_port provide connectionless service with notification of delivery or nondelivery between the two N_ports.

class 3. A class of service that provides a connectionless service without notification of delivery between N_ports. The transmission and routing of class 3 frames is the same as for class 2 frames.

class F. A class of service used for interswitch control traffic. It provides connectionless service with notification of delivery or nondelivery between two E_ports.

CMI. Control messaging interface.

community (SNMP). A relationship between an SNMP agent and a set of SNMP managers that defines authentication, access control, and proxy characteristics.

COS. Class of service

CPU. Central processing unit.

credit. As applied to a switch, a numeric value that represents the maximum number of receive buffers provided by an F_port or FL_port to its attached N_port or NL_port respectively such that the N_port or NL_port can transmit frames without overrunning the F_port or NL_port.

daemon. In the AIX operating system, a program that runs unattended to perform a standard service. Some daemons are triggered automatically to perform their task; others operate periodically. Synonymous with demon. See also *qdaemon*.

defined configuration. The complete set of all zone objects that are defined in the fabric. The defined configuration can include multiple zone configurations.

domain_ID. The domain number that uniquely identifies the switch in a fabric. This switch domain ID is normally automatically assigned by the switch and can be any value between 0 - 31. This number can also be assigned manually.

DNS. Domain name server.

DOS. Disk operating system.

DRAM. Dynamic random access memory.

E_D_TOV. See *error detect time-out value.*

effective configuration. The particular zone configuration that is currently in effect. Only one configuration can be in effect at once. The effective configuration is built each time a zone configuration is enabled.

EIA. Electronic Industries Association.

ELP. Extended link parameters.

error detect time-out value (E_D_TOV). Defines the time the switch waits for an expected response before declaring an error condition. The error detect time-out value is adjustable in 1ms increments from 2 seconds up to 10 seconds.

E_port. A port that is used as an interswitch expansion port to connect to the E_port of another switch to build a larger switch fabric.

ESD. Electrostatic discharge.

fabric. The name applied to a network resulting from the interconnection of switches and devices comprised of high-speed fibre connections. A fabric is an active, intelligent, nonshared interconnect scheme for nodes.

FAN. Fabric address notification

FC. Fibre-channel.

FCA. See *fibre-channel arbitrated loop.*

FCC. Federal Communications Commission.

FCP. Fibre-channel protocol.

fibre-channel arbitrated loop (FCA). A standard defined on top of the FC-PH standard. It defines he arbitration on a loop where several FC nodes share a common medium.

FLOGI. Fabric login

FL_port. The fabric access port used to connect NL_ports to the switch in a loop configuration.

F_port. The fabric access port used to connect an N_port to a switch.

FRU. Field replaceable unit.

FSPF. Fibre-channel shortest path first.

gateway. Hardware that connects incompatible networks by providing the necessary translation, both for hardware and software.

GBIC. Gigabit interface converter.

Gbps. Gigabits per second.

GBps. Gigabytes per second.

G_port. A port that has not assumed a specific function. A G_port is a generic switch port that can operate either as an E_port or an F_port. A port is defined as a G_port, for example, when it is not connected or has not yet assumed a specific function in the fabric.

hardware translative mode. Method for achieving address translation. The following two hardware translative modes are available to a QuickLoop-enabled switch:

- Standard translative mode: Allows public devices to communicate with private devices across the fabric.
- QuickLoop mode: Allows private devices to communicate with other private devices across the fabric.

HBA. Host bus adapter.

hot swappable. Pluggable units that can be installed or removed while power is on.

ID. Identification.

IDB. interface descriptor block

in-band. A fabric that is zone managed using Telnet or StorWatch Specialist directly from a switch, not indirectly from one of the remote switches in the fabric. See *out-of-band*.

iinterswitch link (ISL). A fibre link between two switches

IP. Internet protocol.

ISL. See *interswitch link*.

isolated E_port. ISL is online but not operational between switches because of overlapping domain ID or nonidentical parameters such as E_O_TOVs.

IT. Information technology .

JBOD. Just a bunch of drives.

kBps. Kilobytes per second

LAN. See *local area network.*

LED. See *light-emitting diode*.

light-emitting diode (LED). A semiconductor chip that gives off visible or infrared light when activated.

LIP. QuickLoop initialization procedure.

LLI. Low level interface.

local area network (LAN). A computer network located on a user’s premises within a limited geographic area.

loop. A configuration of devices (for example, JBODs) connected to the fabric by an FL_port interface card.

loopback test. A test in which signals are looped from a test center through a data set or loopback switch and back to the test center for measurement.

L_port. A U_port (universal port) assigned as a loop port.

LWL. Long wavelength.

MIB. (1) Management information base. (2) The information that is on an agent. It is an abstraction of configuration and status information.

ms. Milliseconds

multicast. The transmission of the same data to a selected group of destinations.

NIS. Network information service

NL_port. The designation of an equipment port connected to the fabric in a loop configuration using an FL_port.

N_port. The designation of an equipment port connected to the fabric.

OFC. Open fibre control.

OS. Operating system.

out-of-band. A fabric that is remotely managed using Telnet or StorWatch Specialist indirectly from one of the devices in the fabric, not directly from the switch. See *in-band*.

PID. Port identification (address).

PLDA. Private loop direct attach.

PLOGI. Port login.

POST. See *power-on self-test*.

power-on self-test (POST). A series of self-tests that run each time the unit is started or reset.

qdaemon. In the AIX operating system, the daemon process that maintains a list of outstanding jobs and sends them to the specified device at the appropriate time.

R_A_TOV. See *resource allocation timeout value*.

RAM. Random access memory.

resource allocation time-out value (R_A_TOV). R_A_TOV is used to time out operations that depend on the maximum possible time that a frame could be delayed in a fabric and still be delivered. The value of R_A_TOV is adjustable in 1-microsecond increments over a range from 10 - 120 seconds.

RPC. Remote procedure calls.

RSCN. Remote state change notification.

RSH. Remote shell.

SAN. Storage area network.

SC. Session control.

SID. Source identification.

simple network management protocol (SNMP). A TCP/IP protocol that generally uses the user datagram protocol (UDP) to exchange messages between a management information base and a management client residing on a network. Because SNMP does not rely on the underlying communication protocols, it can be made available over other protocols, such as UDP/IP. There are many versions of the simple network management protocol. See *SNMPv1*.

SL. See *interswitch link*.

SNMP. See *simple network management protocol*.

SNMPv1. The original standard for SNMP, now referred to as SNMPv1.

SNMPv2C. Community-based SNMP.

SNMP-SET. A manager that can change information on the agent.

SNS. Simple name server.

SPLB. Set port loopback mode.

SRAM. Static RAM.

SWL. Short wavelength.

tachyon. A type of host bus adapter.

toggle. A switching device such as a toggle key on a keyboard. Pertains to any device that has two stable states.

token ring. A network with a ring topology that passes tokens from one attaching device to another; for example, the IBM Token-Ring Network.

trap (SNMP). A mechanism for SNMP agents to notify the SNMP management station of significant events.

TTL. Time-to-live.

tunneling. To treat a transport network as though it were a single communications link or LAN.

UDP. User datagram protocol.

unicast. Transmission of data to a single destination.

U_port. An unassigned port. A U_port can be assigned as a loop port (L_port), an expansion port (E_port), and so on.

VC. Virtual channel

WAN. Wide area network.

world-wide name (WWN). A unique identifier for a switch on local and global networks.

wrap connector. A connector that connects the output of a controller or cable to the input of the controller or cable. A wrap test then verifies that the connector or cable output and input circuits are working correctly.

wrap test. A test that verifies the connector or cable output and input circuits of a controller are working correctly.

WWN. See *world-wide name*.

zone alias. An alias for a set of port numbers or WWNs. Zone aliases can be used to simplify the entry of port numbers and WWNs. For example, &#147;host&#148; could be used as an alias for a WWN of 110:00:00:60:69:00:00:8a.

zone configuraton. A set of zones designated as belonging to the same zone configuration. When a zone configuration is in effect, all valid zones in that configuration are also in effect.

zoning. An interconnectivity method for allowing a set of devices to communicate within the set while not allowing communication with devices outside the set. There can be several sets and some sets can partially overlap.

Index

Numerics

10/100BaseT Ethernet LAN 7
3534 Managed Hub
  configurations 104
  front panel 41
  overview 1
  power on (ready) indicator 9
  with SNMP, managing 119

A

about this guide xix
ac power removal xv
access
  privilege 48
  to the IBM StorWatch Managed Hub Specialist 28
accessing
  administrative interface 48
  firmware upgrade 52
  IBM StorWatch Managed Hub Specialist 28
  license administration 56
  name server table view 33
  performance view 47
  reboot switch 53
  SNMP administration 54
  switch administration 48
  Telnet interface 58
  the Port statistics view 44
  user administration 51
  zone configuration settings 39
  zoning functions 35
accounting group 122
active paths 33
add license 56
Add Member 36
Add Other 37
adding
  multiple items to a zone 92
  new fabric 94
  new switch 94
address, IBM ii
admin privilege 48
administering zoning 35
administration and configuration capability 27
administrative interface 29, 48
agent 119
agent configuration 123
agtcfgDefault command 132
agtcfgSet command 135
agtcfgShow command 138
AL_PA
  bitmap, qlShow command field description 108
  zoning 116
alarms
  configuring 71
  error log entry 71
  Fabric Watch 60
  locking of the port log 71
  SNMP trap 70
  types supported by Fabric Watch 70
aliAdd command 96
alias
  commands 93
  members 37
  name 36
  server, definition 393
  zone 89
aliasShow command 141
aliCreate commands 97
aliRemove command 97
aliShow command 97
application specific integrated circuit (ASIC), definition 393
Apply 37
arbitrated loop
  definition 393
  zoning 116
Arbitrated loop settings 164
ASIC (application specific integrated circuit), definition 393
asynchronous transfer mode (ATM), definition 393
ATM (asynchronous transfer mode), definition 393
authenticationFailure 122, 123
Auto Refresh
  field description 34
  Interval field description 34
available MIB and trap files 124

B

backspace command 143
basic input/output system (BIOS),

definition 393
battery notice caution xvi
BB
definition 393
benefits of zoning 86
BIOS (basic input/output system), definition 393
blue zone 90
broadcast zones 37
browsers, Web 28
buffer-to-buffer (BB), definition 393
bypassing POST 53

C

cable
connections 5
length 5
pinouts 7
specifications 5
type 5
CAM
definition 393
test 9, 10
camTest
offline test 10
camTest command 146
Cancel 37
capabilities, IBM StorWatch Specialist 27
capability group 122
caution notice xv
central
maintenance functions 27
memory test 9, 10
processing unit (CPU), definition 393
centralMemoryTest
offline test 10
centralMemoryTest command 147
cfgAdd command 98
cfgClear command 101
cfgCreate command 98
cfgDelete command 98
cfgDisable command 101
cfgEnable command 101
cfgRemove command 98
cfgSave command 101
cfgShow command 99, 102
change
monitor threshold 62
password 51
user name 51
checklist, pre-installation 13
class
class 2, definition 393
class 3, definition 393
class F, definition 393
classes of fabric and hub elements 65, 66
CMem data retention test (cmemRetentionTest) 10
cmemRetentionTest
offline test 11
cmemRetentionTest command 149
CMI Conn test 9, 10
cmiTest
offline test 10
cmiTest command 151
coldStart 122
commands
agtcfgDefault 132
agtcfgSet 135
agtcfgShow 138
aliAdd 95, 96
alias 93
aliasShow 141
aliCreate 95, 97
aliDelete 95
aliRemove 95, 97
aliShow 95, 97
backspace 143
camTest 146
centralMemoryTest 147
cfgAdd 96, 98
cfgClear 96, 101
cfgCreate 96, 98
cfgDelete 96, 98
cfgDisable 96, 101
cfgEnable 96, 101
cfgRemove 96, 98
cfgSave 96, 101
cfgShow 96, 99, 102
cmemRetentionTest 149
cmiTest 151
configDefault 153
configDownload 155
configShow 158
configUpload 160
configuration 93
configuration management 101
configure 163
crossPortTest 170
date 175

diagClearError 177
diagDisablePost 179
diagEnablePost 181
diagHelp 183
diagShow 184
dlsReset 186
dlsSet 187
dlsShow 189
errDump 190
errShow 191
Fabric Watch Telenet 72
fabricShow 196
fanShow 198
fastboot 199
firmwareDownload 200
fspfShow 202
fwClassInit 73, 204
fwConfigReload 73, 205
fwConfigure 74, 206
fwShow 77, 209
gbicShow 211
h 213
help 215
i 216
ifModeSet 218
ifModeShow 220
ifShow 221
interfaceShow 223
iodReset 228
iodSet 229
iodShow 230
ipAddrSet 231
ipAddrShow 233
licenseAdd 235
licenseHelp 236
licenseRemove 237
licenseShow 238
linkCost 239
login 241
logout 242
loopdiagClear 243
loopdiagDone 244
LSDbShow 245
mcastShow 248
msConfigure 250
msPlClearDB 256
msPlMgmtActivate 257
msPlMgmtDeactivate 259
msPlatShow 252
msPlCapabilityShow 254
nbrStateShow 264
nbrStatsClear 261
nsAllShow 266
nsShow 268
overview of Telnet 72
parityCheck 270
passwd 272
portCfgEport 274
portCfgGport 276
portCfgLongDistance 280
portCfgLport 278
portcfgMcastLoopback 282
portDisable 284
portEnable 285
portErrShow 286
portLogClear 288
portLogDump 290
portLogShow 292
portLoopbackTest 297
portPerfShow 300
portRegTest 301
portRouteShow 303
portShow 305
portStatsShow 308
psShow 311
qloopartner 312
qloopShow 314, 316
qlPartner 106
qlShow 107
quietMode 318
ramTest 319
reboot 322
routeHelp 323
setGbicMode 324
setSplbMode 325
spinSilk 327
sramRetentionTest 332
summary and description of zoning 95
supportShow 334
switchBeacon 336
switchDisable 338
switchEnable 339
switchName 15, 341
switchShow 343
switchStatusPolicySet 346
switchStatusPolicyShow 348
switchStatusShow 350
syslogdIpAdd 352
syslogdIpRemove 353
syslogdIpShow 354

Telnet 73
tempShow 355
topologyShow 356
trackChangesSet 359
uptime 361
uRouteConfig 363
uRouteRemove 365
uRouteShow 366
Version 368
zone 93, 99
zone alias summary and description 96
zone configuration 98
zoneAdd 96, 99, 370
ZoneCreate 372
zoneCreate 96, 99
zoneDelete 96, 100, 374
zoneRemove 96, 100, 375
zoneShow 96, 100, 377
zoning 95
commit
change 53
configuration changes - ID field description 50
SNMP changes - SNMP administraton field description 55
user name/password change 51
community
SNMP, definition 393
complete installation 13
compliance statements
European community 385
FCC 384
Germany 385
industry Canada 385
Japanese VCCI 386
Taiwan Class A 387
components
system 2
zoning 88
comprehensive asset management 27
concepts, zoning 88
configDefault command 153
configDownload command 155
configShow command 158
configUpload command 160
configuration
agent 123
capability 27
commands 93
defined 90
dual-switch 104
effective 90
file 65
group 121
management commands 101
mixed loop and SAN 104
samples 104
saved 90
single-switch 104
zone 89
configure and administer individual ports 27
configure command
arbitrated loop settings 164
description 163
switch fabric settings 164
system service settings 166
virtual channel settings 167
configuring
QuickLoop zones 113
thresholds and alarms 71
connection
Ethernet 7
fibre optic cable 5
serial port 6
connector, male 9-pin D-Subminiature 7
content addressable memory (CAM), definition 393
continuous events 70
converter, gigabyte interface 2
copyright statement, IBM ii
CPU (central processing unit), definition 393
Create Alias 36
creating zones 116
credit, applied to a switch, definition 393
crossPortTest
cross port test diagnostic 10
offline and online tests 10
crossPortTest command 170
customer, pre-installation checklist 13

D

danger notice xv
date command 175
default IP address 14
definition, zone 88
Delete Alias 36
device status 27
devices included in a fabric 29
diagClearError command 177
diagDisablePost command 179

diagEnablePost command 181
diagHelp command 183
diagnostics
  overview 9
  running 10
diagShow command 184
disable
  port error message 129
  POST 53
  the community string or trap recipient fields 55
distributed zoning control 27
dlsReset command 186
dlsSet command 187
dlsShow command 189
DNS (domain name server), definition 393
domain
  # field 34
  destination domain ID (1, 2, or 3) 33
  ID definition 393
  ID field 30
  ID field description 49
  name server (DNS), definition 393
download
  file from 52
  flash now 52
downloading firmware
  from the 3534 Managed Hub Web site 24
  from the Web site for a UNIX host 25
  from the Web site for a Windows host 26
dual
  hub loop 109
  SC fibre optic plug connector 5
  switch configuration 104
duplex SC plug connectors 5
dust protection 6

E

E_D_TOV (error detect time-out value)
  definition 393
E_Port 109
E_port, definition 394
E_port, description of 109
effective configuration 90
electronic emission notices 384
ELP (extended link parameters), definition 393
emissions requirements and serial cabling 7
Enable Authentication Traps - SNMP administraton field description 55
end Telnet session 58
Enet IP 30
enforcing a zone 92
enterprise specific traps 123
  swFault 123
  swFCPortScn 123
  swSensorScn 123
errDump command 190
error
  detect time out-value (E_D_TOV), definition 393
  log entry 71
  message format 125
  messages 129, 379
error messages
  fan 129
  format 129, 379
  port 129
  thermometer 130
errShow command 191
ESD protection 6
Ethernet
  connection 7
  IP 50
  setting the port IP address 22
  subnetmask - ID field description 50
European community compliance statement 385
event
  changing monitor threshold 62
  range threshold 61
  rising or falling threshold 62
Event Trap Level - SNMP administraton field description 55
events
  continuous 70
  general description 69
  triggered 69
example of a threshold name 69
expansion port 109
extended link parameters (ELP), definition 393
extensive administration 27
extent of warranty 390
external machine checks xv

F

F_port, definition 394
fabric
  adding a new 94

definition 394
element MIB support 121
group 122
included devices 29
merging 94
multiswitch 93
name server table 33
splitting 95
topology 30, 31
topology view 28
view 28, 29
Fabric Watch
alarms 60
changing monitor threshold 62
classes
E_port 67
environment 66
F/FL_port 67, 68
fabric 66
GBIC 68
port 66
classes and areas 66
code upgrade 60
example of a threshold name 69
installing
Fabric Watch license 63
through Telnet 63
using the IBM StorWatch Specialist 64
license key 60
methods
of access 60
of installing the license 63
monitored elements 60
optional software 77
range threshold 61
required 3534 hub version level 60, 63
rising and falling threshold 62
Telnet commands 72
threshold behavior models 61
upgrade 59
using 64
fabricShow command 196
faceplate of the 3534 Managed Hub 1
failure, port 42
FAN
definition 394
fan error message 129
fanShow command 198
fast restart 53
fastboot
command 199
switch 53
fault
isolation 109
port 129
faulty looplet 109
FAX number, IBM ii
FC4 types 34
FCnet IP 30
FCP (fibre-channel protocol), definition 394
feature
codes 59
features, QuickLoop 103
Federal Communications Commission (FCC) statement 384
fiber optic
GBIC module, shortwave length 2
plug connector 5
ports 4
fibre-channel
cable connections 5
IP 50
port group 122
protocol (FCB), definition 394
shortest path first (FSPF), definition 394
subnetmask - ID field description 50
firmware
downloading 24
downloading from a UNIX host 25
downloading from the SAN Fibre Channel 3534 Managed Hub Web site 25
upgrade 52
firmwareDownload command 200
FL_port, definition 394
front panel
3534 Managed Hub 41
indicators
LED port 8
LED status 8
of the 3534 Managed Hub 41
FSPF (fibre-channel shortest path first), definition 394
fspfShow command 202
function of IBM zoning 87
fwClassInit command 73, 204
fwConfigReload command 73, 205
fwConfigure command 74, 206
fwShow command 77, 209

G

G_port, definition 394
gateway
- definition 394
- IP 50
- IP address 30

GBIC
- how to determine type 42
- hub connector 4
- installing 4
- module 2, 3
- module optical wavelength 5
- overview 2
- port 4
- rubber plug 4
- SC connector end 4
- types
  - copper 42
  - long wave 42
  - serial ID 42
  - short wave 42

gbicShow command 211
general restrictions xvi
generic traps 122
- authenticationFailure 122
- coldStart 122
- linkDown 122
- linkUp 122

Germany compliance statement 385
getting help 72
gigabit interface converter 2
green zone 90

H

h command 213
HBA
- specification 13
- supported, Web site 13

help
- command 215
- getting technical support 72, 83

high-performance fibre-channel managed hub 1
host
- bus adapter, definition 394
- name or host IP 52

hub
- (also called switch in this guide) 27
- connector on GBIC 4
- level 109
- offline (switchDisable) 10
- online (switchEnable) 10
- view 82

HyperTerminal session 16, 20

I

i command 216
IBM
- 3534 SAN Fibre Channel Managed Hub
  - introduction 1
- copyright statement ii
- electronic address ii
- FAX number ii
- license agreement for machine code 387
- mailing address ii
- simplicity of zoning 87
- warranty for machines 388

IBM StorWatch
- Managed Hub Specialist 28
- Managed Hub Specialist views 28

IBM StorWatch Specialist
- capabilities 27
- central maintenance functions 27
- central status monitoring 27
- comprehensive asset management 27
- device status 27
- distributed zoning control 27
- extensive administration and configuration capability 27
- overview 27, 64
- port status 27
- Telnet interface for access to specialized functions 27

IDB, definition 394
ifModeSet command 218
ifModeShow command 220
ifShow command 221
incorrect network parameters 14
increased SAN control 86
indicator
- LED 8
- power on (ready) 9

Industry Canada compliance statement 385
information technology (IT)
- a benefit of zoning 86
- definition 394

installing
- complete installation 13
- Fabric Watch using the IBM StorWatch

Specialist 64
GBICS 4
GBICs 4
hub 13
requirements for Fabric Watch 63
verifying the 3534 Managed Hub 24
installing Fabric Watch through Telnet 63
interface
descriptor block, definition 394
group of objects supported by SNMP agent 121
user 103
interfaceShow command 223
Internet Explorer 4.0 28
internet protocol (IP), definition 394
interswitch link (ISL), definition 394
introduction to the IBM 3534 SAN Fibre Channel Managed Hub 1
iodReset command 228
iodSet command 229
iodShow command 230
IP
address
default 14
setting 14
address in the Location/Address field 28
Cnet 30
Enet 30
Ethernet - ID field description 50
fiber-channel - ID field description 50
gateway 30
gateway - ID field description 50
host 52
host name 52
internet protocol, definition 394
syslog daemon - ID field description 50
ipAddrSet command 231
ipAddrShow command 233
ISL (interswitch link), definition 394
isolated E_port, definition 394
isolation, fault 109
IT (information technology)
definition 394
optimization 86

J

Japanese Voluntary Control Council for Interference (VCCI) class 1 statement 386
Java Plug-In 1.2.2 28
Java-enabled Web browsers, using to launch 28
JBOD (just a bunch of drives)
definition 394
not accessed from any zone 90
just a bunch of drives (JBOD) 90

K

keys and enabled features 56

L

L_port, definition 394
L_port, description of 109
LAN (local area network), definition 394
laser safety xvi
launching the IBM StorWatch Managed Hub Specialist 28
LED
(light-emitting diode), definition 394
flash speed and color 8
green 8
port indicators 8
status indicators 42
yellow 8
level port 109
liability, limitation of 390
license
administration 56
agreement for machine code (IBM) 387
key 56
license key
Fabric Watch 60
licenseAdd command 235
licenseHelp command 236
licenseRemove command 237
licenseShow command 238
light-emitting diode (LED), definition 394
limitation of liability 390
linkCost command 239
linkDown 122
linkUp 122
LIP (QuickLoop initialization procedure), definition 394
lithium battery caution xvi
LLI (low level interface), definition 394
local
AL_PAs, qlShow command field description 108
area network (LAN), definition 394
local looplet states, qlShow command

field description 108
locking of the port log 71
login command 241
logout command 242
long wavelength fiber optic GBIC module 3
loop
definition 394
port 109
switch upgrade 59
loopback 130
loopdiagClear command 243
loopdiagDone command 244
low level interface (LLI), definition 394
LSDbShow command 245
LWL
fiber optic cable 5
fibre optic GBIC module 3

M

male 9-pin D-Subminiature connector 7
manageability 2
management
example of zone 91
information base (MIB) 119
information base (MIB), definition 395
zone 87, 91
managing and monitoring the switch using zoning 91
managing the 3534 Managed Hub
with SNMP 119
maximum cable length 5
mcastShow command 248
member
zone 88
Member Selection List 36
memory test (ramTest) 9, 10
merging two fabrics 94
message classification 126
methods to manage the QuickLoop 103
MIB
(management information base), definition 395
description 119
downloading definitions 124
objects 120
tree 120
MIB-II support 121
mixed loop and SAN configuration 104
msConfigure command 250
msPIClearDB command 256
msPIMgmtActivate command 257
msPIMgmtDeactivate command 259
msPlatShow command 252
msPlCapabilityShow command 254
multicast
when used, definition 395
multiswitch fabrics 93

N

N_port
definition 395
login data 93
name
accessing server table 33
Auto Refresh
Interval server table field 34
server table field 34
COS server table field 34
description 30
domain # server table field 34
Done server table field 34
FC4 Types server table field 34
Member of Zones server table field 34
Node WWN server table field 34
Port
# server table field 34
ID server table field 34
types server table field 34
WWN server table field 34
refresh server table field 34
server
entries 33
group 122
table 30, 33
table fields 34
table view 29
simple server data base 33
Symbolic Name server table field 34
nbrStateShow command 264
nbrStatsClear command 261
Netscape 4.51 28
network parameters, incorrect 14
new switch, adding 94
NL_port, definition 395
no light 129
node WWN 34
notices
caution xv
danger xv

for products and services offered in the U.S.A. 383
lithium battery caution xvi
safety and environmental xv
translated xv
nsAllShow command 266
nsShow command 268

O

objects specified in MIB-II 121
offline 129
test 10
offline tests
camTest 10
centralMemoryTest 10
cmemRetentionTest 11
cmiTest 10
crossPortTest (and online test) 10
portLoopbackTest 10
portRegTest 10
ramTest (and online test) 10
spinSilk 10
sramRetentionTest 10
online tests 10
crossPortTest (and offline test) 10
ramTest (and offline test) 10
operating system (OS), definition 395
operation group 121
OS (operating system), definition 395
overview
IBM StorWatch Specialist 27
zoning 85

P

parityCheck command 270
passwd command 272
Peer, qlShow command field description 107
performance
aggregate routing capacity 2
view 47
Performance view 29
PID, definition 395
pinouts, cabling 7
pins, supported 7
platforms, supported, Web site 13
PLDA
definition 395
legacy devices 103
plug, protective 5
port
disabled - ID field description 50
error messages 129
failure 42
ID 34
indicators 8
level 109
loopback test
(portLoopbackTest) 10
check that frames are transmitted, looped back, and received 9
number supported 1
QuickLoop zones 114
register test 9
register test (portRegTest) 10
statistics view 29, 44
status 8, 27
type 34
WWN 34
portCfgEport command 274
portCfgGport command 276
portCfgLongDistance command 280
portCfgLport command 278
portcfgMcastLoopback command 282
portDisable command 284
portEnable command 285
portErrShow
command 286
portLogClear command 288
portLogDump command 290
portLogShow command
description 292
portLoopbackTest
command 297
offline test 10
portPerfShow command 300
portRegTest
command description 301
offline test 10
portRouteShow command 303
portShow command 305
portStatsShow
command description 308
POST
automatic diagnostic tests 9
definition 395
how to bypass 53
verifying 9
preface xix
pre-installation checklist 13
private loop direct attach (PLDA)

definition 395
legacy devices) 103
product recycling xvi
production status 388
protection, dust and ESD 6
protective plug 5
psShow command 311

Q

qlHelp command 104
qloopartner command 312
qloopShow command 314, 316
qlPartner command 104, 106
qlShow command 104, 107
QuickLoop
administration 57
commands 106
configuring zones 113
creating 113
define zone configuration 114
defining the zone 113
enable zone configuration 114
features 103
initialization procedure (LIP), definition 394
methods to manage 103
zones using ports 114
zoning 111
zoning advantages 112
quietMode command 318

R

R_A_TOV
definition 395
RAM (random access memory), definition 395
ramTest
offline and online test 10
ramTest command 319
random access memory (RAM), definition 395
range threshold 61
rapid access to any switch or hub 27
read-only
community string - SNMP administraton field description 55
read-write
community string - SNMP administraton field description 55
reboot
command description 322
switch function 53
Reboot Switch field descriptions 53
red zone 90
refresh 34
related publications xx
remote
AL_PAs, qlShow command field description 108
procedure calls (RPC), definition 395
shell (RSH)
definition 395
state change notification (RSCN)
definition 395
user name 52
remove
ac power xv
license 56
member 36
Rename Alias 36
requirements, emission 7
reset
firmware upgrade 52
SNMP administration - SNMP administraton field description 55
switch administration - ID field description 50
resource allocation time-out value (R_A_TOV), definition 395
restrictions
general xvi
usage xvii
rising or falling threshold 62
routeHelp command 323
RPC
command function 25
definition 395
RSCN (remote state change notification), definition 395
RSH (remote shell) 24
rubber plug, GBIC 4
running diagnostics 10

S

safety
and environmental notices xv
inspection xv
laser xvi
lithium battery xvi
sample configurations 104
SAN
definition 395

storage area network of hubs and switches 27

saved configuration 90

SC

connector end of GBIC 4

plug connectors 5

Scope, qlShow command field description 108

segmented, port 130

Self, qlShow command field description 107

sending 130

serial cabling and emissions requirements 7

serial port

cabling 7

connection 6

cover 6

pinouts 7

setting the IP address 16

server 14

service, warranty 389

setGbicMode command 324

setSplbMode command 325

setting

serial port 6

the IP address

preferred method 14

using the Ethernet port 22

using the serial port 16

zone 34

zone alias 35

zones 92

short wavelength fiber optic GBIC module 2, 3

simple

name server (SNS), definition 395

name server database 33

Network Management Protocol (SNMP) 119

network management protocol (SNMP), definition 395

single-switch configuration 104

SNMP

(Simple Network Management Protocol) 119

administration 54

agent configuration 123

agent configuration group 122

Description, definition 395

enterprise specific traps 123

fabric element MIB support 121

generic traps 122

group of objects supported by SNMP agent 121

MIB-II support 121

set command 121

SNMP v1 transports 121

transports 121

trap 70

vendor unique MIB 122

SNMP-based enterprise managers 65

SNMPv1

communities agent parameter 123

description 395

SET command 123

SNS (simple name server), definition 395

software updates, getting 83

specification

cable 5

zone 87

spinSilk

command 327

offline test 10

test (spinSilk) 10

splitting a fabric 95

SRAM

data retention test (sramRetentionTest) 10

definition 395

sramRetentionTest

offline 10

sramRetentionTest command 332

start Telnet session 25

State, qlShow command field description 107

statement of limited warranty 388

static RAM (SRAM), definition 395

statistics by port 44

storage area network

definition 395

of hubs and switches 27

StorWatch

Specialist xix, 27

switch view 41

support, syslogd 125

supported

pins 7

platforms Web site 13

supportShow command 334

swEventTrap 123

swFault enterprise specific trap 123

swFCPortScn enterprise specific trap 123

switch

administration 48
configuration 127
disabled - ID field description 50
fabric settings 164
icon 30
name 49
power on (ready) indicator 9
reboot function 53
system group 122
view 29
switchBeacon command 336
switchDisable command 338
switched loop architecture 1
switchEnable command 339
switchName
command 341
switchShow
command 343
switchStatusPolicySet command 346
switchStatusPolicyShow command 348
switchStatusShow command 350
SWL fiber optic
cable 5
GBIC module 2
swSensorScn enterprise specific trap 123
symbolic name 34
sysContact
agent parameter 123
variable 121
sysDescr
variable 121
sysLocation
agent parameter 123
variable 121
syslog daemon function 124
Syslog daemon IP - Switch Admin field description 50
syslogd
configuration 128
messages 126
starting 127
support 125
syslogdIpAdd command 352
syslogdIpRemove command 353
syslogdIpShow command 354
sysName agent parameter 123
sysObjectID variable 121
system
board 1, 2
components 2
contact - SNMP administraton field description 54
description - SNMP administraton field description 54
group of objects supported by SNMP agent 121
location - SNMP administraton field description 55
service settings 166
sysUpTime variable 121

T

Taiwan Class A compliance statement 387
Telnet
commands 73
commands overview 72
connection 6
end session 58
interface 29, 58, 65
interface for access to specialized functions 27
shell 104
start session 25
Telnet tests
CAM test 10
central memory test 10
CMem data retention test 10
CMI conn test 10
cross port test 10
Hub offline 10
Hub online 10
memory test 10
port loopback test 10
port register test 10
Spin silk test 10
SRAM data retention test 10
temperature threshold 61
tempShow command 355
terminate the existing Telnet session 58
thermometer error message 130
threshold
behavior models 61
naming conventions 68
topologyShow command 356
trackChangesSet command 359
trademarks 384
translated safety notices xv
trap
(SNMP), definition 396
enterprise specific 123

generic 122
recipients - SNMP administraton field description 55
recipients agent parameter 123
triggered events 69
tunneling, definition 396

U

U_port, description of 109
UDP (user datagram protocol), definition 396
unicast, definition 396
universal port 109
UNIX 28
downloading firmware 25
upgrade
Fabric Watch 59
Loop switch 59
uptime command 361
uRouteConfig command 363
uRouteRemove command 365
uRouteShow command 366
usage restrictions xvii
user
administration 51
datagram protocol (UDP), definition 396
interfaces 103
uses for zoning 87
using
Fabric Watch 64
QuickLoop zones 112

V

VarBind 123
vendor unique MIB 122
verify Fabric Watch license key 60
verifying
3534 Managed Hub installation 24
password 51
power-on self-test (POST) 9
Version command 368
view fabric topology 31
Virtual
channel settings 167

W

WAN (wide area network), definition 396
warranty
extent of 390
for machines (IBM) 388
service 389
statement of limited 388
Web
browsers 28
site address 24
sites xx
tools 117
where to start xix
who should use this book xix
wide area network (WAN), definition 396
Windows
95/98 or Windows NT 28
downloading firmware 26
world-wide name (WWN), definition 396
WWN
(world-wide name), definition 396
fabric view field description 30

Z

zone
adding multiple items 92
administration 30
administration interface 29, 34
alias commands 96
alias settings 35
aliases 89
benefits 86
broadcast 37
commands 93, 99
components 88
concepts 88
config settings fields 40
configuration commands 98
configuration data 93
configurations 89
configured dynamically 86
configuring QuickLoop 113
creating 116
define QuickLoop configuration 114
define the QuickLoop zone 113
definition 88
enable QuickLoop configuration 114
example of management 91
management 91, 92
members 88
QuickLoop 112
QuickLoop using ports 114
red, green, blue 90
settings 37
temporary 87
uses 87

zone settings field descriptions
- Add member 39
- Add Other 39
- Apply 39
- Cancel 39
- Create Zone 38
- Delete Zone 38
- Member Selection List 39
- Remove Member 39
- Rename Zone 39
- Zone Members 39
- Zone Name 38

zoneAdd command 99, 370
zoneCreate command 99, 372
zoneDelete command 100, 374
zoneRemove command 100, 375
zoneShow command 100, 377
zoning
- benefits 86
- command summary and description 95
- commands 95
- components 92
- concepts 88
- functionality 87
- overview 85
- QuickLoop 111
- setup and administration 92
- uses for 87
- using 91

Readers' comments — we would like to hear from you.

IBM 3534 SAN Fibre Channel Managed Hub
User's Guide

Publication No. GC26-7391-02

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	□	□	□	□	□

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	□	□	□	□	□
Complete	□	□	□	□	□
Easy to find	□	□	□	□	□
Easy to understand	□	□	□	□	□
Well organized	□	□	□	□	□
Applicable to your tasks	□	□	□	□	□

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? □ Yes □ No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Name

Address

Company or Organization

Phone No.

Readers' Comments — We'd Like to Hear from You
GC26-7391-02

Cut or Fold
Along Line

Fold and Tape

Please do not staple

Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

International Business Machines Corporation
RCF Processing Department
Dept. G26/Bldg.050-2
5600 Cottle Road
San Jose, CA
U.S.A. 95193-0001

Fold and Tape

Please do not staple

Fold and Tape

Cut or Fold
Along Line

Part Number: 18P3448

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

(1P) P/N: 18P3448

GC26-7391-02

Spine information:

IBM 3534 SAN Fibre Channel
Managed Hub User's Guide