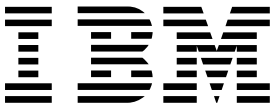


IBM 3534 SAN Fibre Channel Managed Hub Installation and Service Guide

SY27-7616-01

Note:

Before using this information and the product it supports, read the information in “Safety and environmental notices” on page xiii and *Notices* on page 151.

Second Edition (April 2001)

This edition replaces SY27-7616-00.

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 you comments to:

International Business Machines Corporation
RCF Processing Department
Dept. G26/Bldg. 050-3
5600 Cottle Road
San Jose, CA 95193-0001
U.S.A.
FAX: 1-800-426-6209

You can also send your comments 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

Tables

Safety and environmental notices

Safety notices are printed throughout this guide. *Danger* notices warn you of conditions or procedures that can result in death or severe personal injury. *Caution* notices warn you of conditions or procedures that can cause personal injury that is neither lethal nor extremely dangerous. *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 guide 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)

CAUTION:
A caution notice indicates the presence of a hazard that has the potential of causing moderate or minor personal injury.

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.

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. These materials should be recycled 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 is a class 1 laser product. 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 that guarantees that the system power source will cease to provide power if the maximum recommended operation limit or more is detected on the +3.3 V/+5 V 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 the laser safety.

Usage restrictions

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

About this guide

This guide describes how to install and maintain the IBM 3534 SAN Fibre Channel Managed Hub (hereafter referred to as the 3534 Managed Hub).

Who should use this guide

This guide is intended to be used by:

- A trained service support representative (SSR) to diagnose and solve hardware problems on the IBM 3534 SAN Fibre Channel Managed Hub.
- The customer during installation and setup of the 3534 Managed Hub. The 3534 Managed Hub is a customer setup unit (CSU). Before using the installation section of this guide, you should know how to service your own network and applicable software. You must also know how to safely work with electrical components.

Note: Throughout this guide, the term *switch* refers to switches and hubs unless otherwise noted.

Note: Throughout this guide, 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 "Chapter 6. Service procedures" on page 85. This ensures that you use the correct service, power on, and power 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 User's Guide*, GC26-7391
- *IBM External Devices Safety Informatio*n, SA26-7003
- *Electrical Safety for IBM Customer Engineers,* S229-8124

Another publication that can provide related information is the Fibre Channel Standards; see "Web sites" on page xviii.

Web sites

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

www.ibm.com/storage/fchub

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

www.fibrechannel.com

Chapter 1. Introduction

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 short wavelength optic ports, one pluggable gigabit interface converter (GBIC) port, and an operating system for building and managing a switched loop architecture.

Note: Throughout this guide, the term *switch* refers to switches and hubs unless otherwise noted.

Figure 1 shows the front panel of the 3534 Managed Hub. Ports are numbered sequentially starting with zero for the left-most port. The 3534 Managed Hub faceplate includes a silk-screen imprint of the port number.

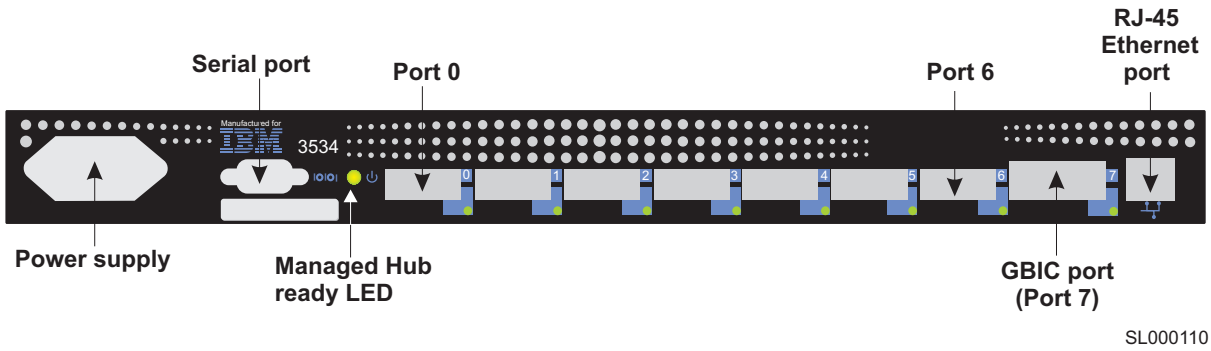


Figure 1. 3534 Managed Hub Front panel

IBM 3534 SAN Fibre Channel Managed Hub overview

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 3534 Managed Hub internet protocol (IP) address. The rest of the 3534 Managed Hub setup is automated.

Flexible A gigabit interface converter (GBIC) module and fixed optic ports support fiber transmission media.

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

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 worst-case 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 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 8 x 100 MBps (0.8 GBps) is provided.

A maximum switch latency of less than 2 µs is specified for class 2, class 3, and class F frames when the output port is free.

Manageability

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

System components

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

GBICs

Important: Do not look into the end of a fiber-optic cable or into a fiber-optic receptacle. This device 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 SC connector color-coded black, is based on short wavelength 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 should remain 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 module (part number and labeling vary)

The SWL 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 cable.

Cables up to 10 km (6.2 miles) in length with a maximum of five splices can be used. The GBIC module is shipped with a protective plug in place which should remain in place if no fiber-optic cable is connected to the port. Figure 3 shows an LWL GBIC module.

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

Fibre-channel 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 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 or fiber-optic ports, or both. 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 of the 3534 Managed Hub using standard dual SC plug connectors, as shown in Figure 4..

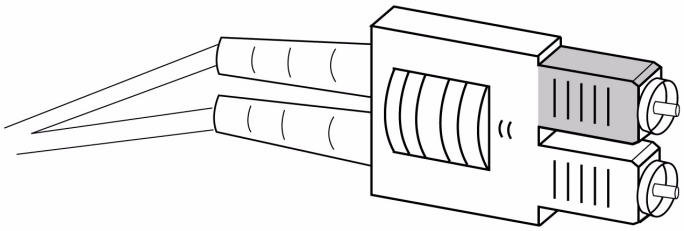


Figure 4. Dual SC fiber-optic plug connector

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

Serial port connection

The 3534 Managed Hub includes a serial port, which is used to set the IP address during setup, reinitialize a 3534 Managed Hub, or to run diagnostics. It is not used during normal operation. Figure 5 shows the location of the serial port connection.

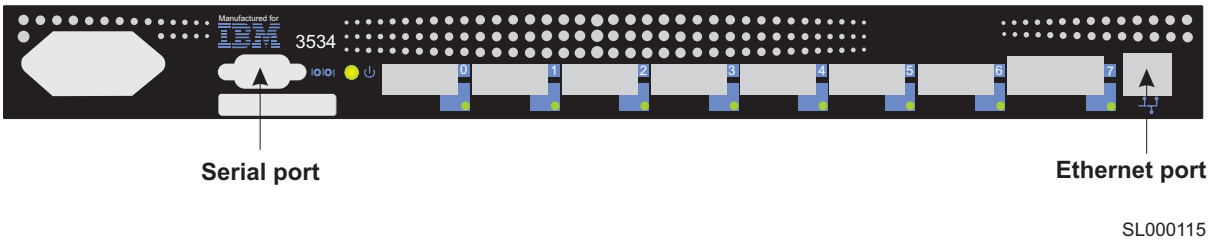


Figure 5. Serial port connection

The serial port settings are as follows:

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

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. Logging in again is required. A password is required to log in to the serial port session as password checking is skipped only when the 3534 Managed Hub is initially started.

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 supported. Table 2 shows the cabling pinouts.

Table 2. Cabling pinout.

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

Note: For dust and electrostatic discharge (ESD) protection, the 3534 Managed Hub includes a cover for the serial port. When not in use, the serial port should be covered.

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:

- Access to the SNMP agent of the 3534 Managed Hub
- Remote Telnet and Web access for remote monitoring and testing
- The setting or changing of the IP address

Note: The connection is only for Telnet, SNMP agent, and the Web-based server access. No fabric connection is used with this connection.

Front panel LED status indicators

Each 3534 Managed Hub port includes a light-emitting diode (LED) indicator. If a problem has been detected with the port, the LED indicators provide an indication of the type of problem. Faults and problems are displayed with a yellow port indicator. The color and blink speed of each port LED indicates the status of that port. Table 3 shows the LED indicators and the corresponding port status

Table 3. Front panel LED status indicators.

Indicators	Status
No light showing	No light or signal carrier (no module, no cable) for media interface LEDs.

Indicators	Status
Steady yellow	Receiving light or signal carrier, but attached device not yet online.
Slow[1] yellow	Disabled (result of diagnostics or the **portDisable** command). Blinks every 2 seconds.
Fast[2] yellow	Error, fault with the port. Blinks every 1/2 second.
Steady green	Online (connected with device over cable).
Slow[1] green	Online, but segmented (loopback cable or incompatible switch). Blinks every 2 seconds.
Fast[2] green	Internal loopback (diagnostic). Blinks every 1/2 second.
Flickering green	Online and frames are flowing through the port.
Green and yellow	The port is bypassed.
Notes: [1] Slow - blinks at 2 second intervals [2] Fast - blinks at 1/2 second intervals	

A properly functioning port with no GBIC installed has no light showing on the LED. When a GBIC is installed and a cable is connected to a properly functioning fibre-channel device, the LED indicator is steady green. A slow green blink indicates that the port detects light but cannot make a proper loop connection. This could indicate any of the following conditions:

- A loopback cable is installed.
- The fabric is segmented (an E-port connection to another hub or switch cannot be completed).
- The hub is connected to an incompatible switch.

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

After the POST diagnostics are run, the power on (ready) LED indicates that the system board diagnostics have completed successfully.

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 fibre-channel (FC) loop failures.

The 3534 Managed Hub supports POSTs and diagnostic tests. The diagnostic tests determine the status of the switch and isolate problems. The diagnostic tests are run using Telnet commands. For more information about diagnostic test commands and procedures, see “Appendix B. Diagnostics” on page 105.

Running power-on self-test (POST)

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

Table 4. Power-on self-test

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

After the 3534 Managed Hub completes the POST, the LED indicators change from the blinking state shown during the tests to a steady state.

If a yellow LED is displayed, it indicates that the port failed one of the POSTs.

If error conditions are found, they can be displayed through Telnet after the 3534 Managed Hub completes the POST.

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 "Appendix B. Diagnostics" on page 105

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

- 3534 Managed 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)**
- SpinSilk test **(spinSilk)**
- SRAM data retention test **(sramRetentionTest)**

- CMem data retention test **(cmemRetentionTest)**
- 3534 Managed Hub online **(switchEnable)**

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 shows the offline and online diagnostic tests.

Table 5. Offline and online diagnostic tests

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

Chapter 2. Customer planning

The following information is needed by the system administrator to properly configure the 3534 Managed Hub in an operational environment.

Table 6 shows an example of a filled-in worksheet for an installed switch. Following Table 6 is an explanation of each item in the table. Table 7 on page 13 is a blank worksheet for your use. Make as many copies as you need to plan the installation of each of your switches.

Table 6. 3534 Planning worksheet example

Item	Description
Firmware level	V 2.1.7
Firmware location: Server name Username Directory	 C02STOR01 sanman G:\sanman\2109\firmware\v2.1
Switch name	3534-1
Domain ID	1
FCnetID (Fibre-channel IP address)	
FC netmask	
WWN	To be supplied when box is turned on
Role	Edge hub
Syslog daemon IP address	192.20.236.4
Users defined - access level	admin - admin, petuser - none
SNMP information: System description System contacts System location Event trap level 0-5 Enable authentication traps RW community string RO community string Trap recipients IP Address	 TestSANlet1_3534-1 (Contact name) B/003-3 Col C-4 5 Refer to “Managing with SNMP” in the IBM SAN Fibre Channel Managed Hub User’s guide for additional information. No dingo pet 192.20.236.3
License keys	Required for optional features.

The following is a description of the items in Table 6 on page 11.

Firmware levels
The firmware levels for the 3534 Managed Hub and the required code that the service representative is to install on an NT StorWatch Specialist workstation.

Firmware location:
The directory location on the StorWatch Server that has the firmware for the 33534 Managed Hub. IBM recommends that a different directory be used for each level of firmware that is loaded.

Server name
The network name of the server where the StorWatch Specialist is run.

Username
The username on the StorWatch Specialist server that owns the firmware for the 3534 Managed Hub. IBM recommends that this not be a username with administrative or security privileges on the server.

Directory
The directory location where the firmware resides.

Switch name
The name of this particular fibre-channel switch.

Domain ID
The domain ID that identifies this switch in the SAN configuration.

FCnetID The fibre-channel IP address for this switch.

FC netmask
The netmask for the fibre-channel IP network.

WWN The World-wide name assigned by the manufacturer.

Role The role this switch will be assigned (principal switch, subordinate switch, or disabled switch).

Syslog daemon IP address
The IP address of the host that the syslog daemon messages will be forwarded to.

Users defined - access level
A list of users in SAN administration network and their roles.

License keys
The license keys required for the optional features.

Use Table 7 on page 13 to plan your switch installation. Make a copy for each switch you plan to install.

.

Table 7. 3534 Managed Hub customer planning worksheet

Item	**Description**
Firmware level	
Firmware location: Server name Username Directory	
Switch name	
Domain ID	
FCnetID (Fibre-channel IP address)	
FC netmask	
WWN	
Role	
Syslog daemon IP address	
Users defined - access level	
SNMP information:	
System description	
System contacts	
System location	
Event trap level 0-5	See *IBM 3534 SAN Fibre Channel Managed Hub User's Guide*
Enable authentication traps	
RW community string	
RO community string	
Trap recipients IP Address	
License keys	

Table 8. 3534 Managed Hub port configuration customer worksheet

Port number	Device name	**Device port**	**Cable length**	**Port type**	**Notes**	**Cable number**
0						
1						
2						
3						
4						
5						
6						
7						

Table 9 shows an example of a filled-in worksheet for an installed switch. Table 10 is a blank worksheet for your use in planning your switch installation. Make as many copies of Table 10 as you need to plan the installation of each of your switches.

Table 9. Zone definitions worksheet example

Zone member type (switch, port, WWN)	**Zone member**	**Zone configuration name**	**Comments**
Port (ID, P)	1, 15	Test_Zone_Config_1	K38 node 1
Port (ID, P)	1, 0	Same	3534-1 PMC1-1
Port (ID, P)	15, 3	Same	3534-2 PMC1-4
Port (ID, P)	15, 14	Same	K38 node 2
Port (ID, P)	1, 10	Same	EMC-1 dir 5 port 0
Port (ID, P)	15, 10	Same	EMC–1 dir 5 port 0

Table 10. Zone definitions customer worksheet

Zone member type (switch, port, WWN)	**Zone member**	**Zone configuration name**	**Comments**
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			

Table 11 shows an example of a filled-in worksheet for an installed switch. Table 12 on page 17 is a blank worksheet for your use in planning your switch installation. Make as many copies of Table 12 as you need to plan the installation of each of your switches.

Table 11. Zone configuration worksheet example

Zone member type (switch, port, WWN)	**Zone member**	**Zone configuration name**	**Connects to**
Port (ID, P)	1, 1	Test_Zone_Config_1	3534-1 PMC2–2
Port (ID, P)	1, 2	Same	3534-1 PMC3–3
Port (ID, P)	1, 3	Same	3534-1 PMC1–1
Port (ID, P)	1, 4	Same	3534-2 PMC2–2
Port (ID, P)	1, 5	Same	3534-2 PMC3–3
Port (ID, P)	1, 6	Same	s1411201e0 P2-I3
Port (ID, P)	1, 7	Same	s1411203e0 P2–I3
Port (ID, P)	1, 8	Same	s1411205e0 P2–I3
Port (ID, P)	1, 9	Same	3534-15 port 8
Port (ID, P)	1, 11	Same	EMC-1 dir 16 port 0
Port (ID, P)	1, 12	Same	2102-3 BDI
Port (ID, P)	1, 13	Same	2109-15 port 13
Port (ID, P)	15, 1	Same	3534-1 PMC2–5
Port (ID, P)	15, 2	Same	3534-1 PMC3–6
Port (ID, P)	15, 0	Same	3534-1 PMC1–4
Port (ID, P)	15, 4	Same	3534-2 PMC2–5
Port (ID, P)	15, 5	Same	3534-2 PMC3–6
Port (ID, P)	15, 6	Same	s1411201e0 P3–I3
Port (ID, P)	15, 7	Same	s1411203e0 P3–I3
Port (ID, P)	15, 8	Same	2109-1 port9
Port (ID, P)	15, 9	Same	s1411206e0 P2–I2
Port (ID, P)	15, 11	Same	EMC-1 dir 16 port 2
Port (ID, P)	15, 13	Same	2109-1 port 13

Table 12. Zone configuration customer worksheet

Zone member type (switch, port, WWN)	Zone member	Zone configuration name	Connects to
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			

Chapter 3. Installing the 3534 Managed Hub

This chapter describes how to install the 3534 Managed Hub.

Note: Throughout this guide, the term *switch* refers to switches and hubs unless otherwise noted.

Customer pre-installation checklist

It is important that you review the pre-installation checklist (Table 13) before you begin to install the 3534 Managed Hub. Some steps might vary because of the host platform that you attach to the 3534 Managed Hub. You should have the IP address for the 3534 Managed Hub and should have arranged for other installation activities.

Table 13. Customer pre-installation checklist

Step	Customer action or decision	Comments and references
1	Desktop or rack-mount installation Location	Determine whether the 3534 Managed Hub is to be installed on a desktop or mounted in a rack.
2	Ensure that the required host platform OS Service Pack is installed. For example: 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), BIOS, and device driver are available.	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 pre-installed and checked • Labeled with host system identifier and 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 13. Customer pre-installation checklist

Step	Customer action or decision	Comments and references
6	Make the following 3534 Managed Hub Ethernet port configuration decisions. 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 and/or route table entries.	**Attention:** The use of incorrect Ethernet parameters can cause problems on the Ethernet network. Obtain the 3534 Managed Hub Ethernet 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 should add 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 host's file. Failure to do this results in poor performance when using a Web browser to manage the 3534 Managed Hub.
8	Run the Ethernet cable from the server (see note) to the network hub.	None
9	Run the Ethernet cable from the network hub to where the 3534 Managed Hub will be installed.	None
10	Verify that the required firmware is available from the IBM Web site.	Firmware 2.2 is required and can be obtained from the Web site at: www.ibm.com/storage/fcswitch or contact IBM technical support.
Note: The term *server* used here refers to the computer you will use for the StorWatch SAN Fibre Channel Managed Hub Specialist.		

Installation instructions

The 3534 Managed Hub can be installed in either a desktop configuration or a rack-mount configuration. Before installing the 3534 Managed Hub and power cord, install either the desktop rubber mounting feet or install the 3534 Managed Hub in a rack.

Note: If you are missing parts, see the following Web site for the telephone number for parts replacement.

www.ibm.com/storage/fchub

Desktop installation

The 3534 Managed Hub is shipped as a desktop configuration. Adhesive rubber mounting feet are supplied. To apply the rubber feet, perform the following steps:

1. Turn the 3534 Managed Hub upside down and lay it on its top.
2. Clean the four depressions by wiping them free of dust.
3. Remove the rubber feet from the sheet provided with the shipping kit, and place one foot in each depression.
4. Firmly press the four rubber feet into place.
5. Return the 3534 Managed Hub to its normal upright position, and place it in its intended service location.

Rack-mount installation

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)

Read the following notices before starting the rack-mount installation:

Attention: Do not install in a rack where the internal rack ambient temperature will exceed 40°C (104°F) or where the airflow is compromised. The airflow is from the back of the unit to the front; do not block the front or the back of the rack.

Attention: Care should be taken that a hazardous condition is not created due to uneven mechanical loading when installing this unit in a rack. If the rack this equipment is being installed in has a stabilizer, it must be firmly attached before installing or removing this unit.

Attention: When rack mounting this unit, ensure that the fibre optic cables that are routed from this unit are not damaged or pinched by rack doors or hardware once installed.

Note: For racks with flush-mount doors, such as the 9306 Netfinity® racks, the following options exist:

- You can use this unit to replace a 3523 Netfinity Fibre Channel Hub by installing the rubber feet (see "Desktop installation" on page 21) and placing the 3534 Managed Hub on the rack tray that held the 3523.
- You can use the rack-mount slides, attaching the 3534 Managed Hub to the set of mounting holes, which are 3-inches offset into the rack, and eliminate the installation of the ears.

This unit requires 2 amps of power with an input of 110 - 127 V ac or 1 amp with an input of 200 - 240 V ac. Make sure that, when connecting the equipment to the supply circuit, overloading of circuits does not compromise the supply wiring or over current protection.

Tools required for the rack-mount installation include the following:

- Standard slotted screwdriver
- Nut driver (11/32 or wrench)

The 3534 Managed Hub is designed to be installed in an EIA standard 19-inch rack. The rack-mount slides and mounting bracket package are provided in the shipping container. Before starting the rack-mount installation, read the entire installation procedure.

To install the 3534 Managed Hub in the rack-mount configuration, perform the following steps:

1. Mount the moving slide and locking ears to the 3534 Managed Hub.
   a. Locate both slides and disassemble them. Fully extend the slide as shown in Figure 6, press the release, and pull the slide apart.

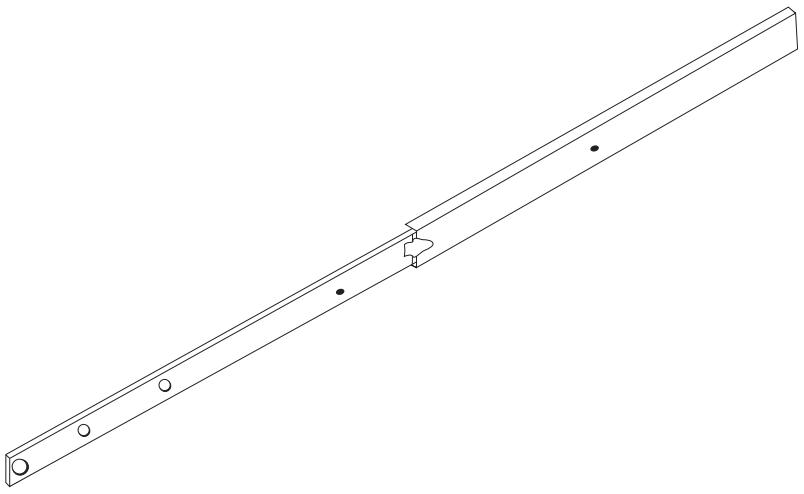


Figure 6. Moving slide

Note: For racks with flush-mount doors, such as the 9306 Netfinity racks, you can use the rack-mount slides, attaching the 3534 Managed Hub to the set of mounting holes, which are 3-inches offset into the rack, and eliminate the installation of the ears.

b. Mount the moving portion of the slide and the locking ears to the 3534 Managed Hub as shown in Figure 7 on page 23. Use the screws provided with the mounting ears in the small bag. Mount the moving portion of the slide first, and then the locking ears.

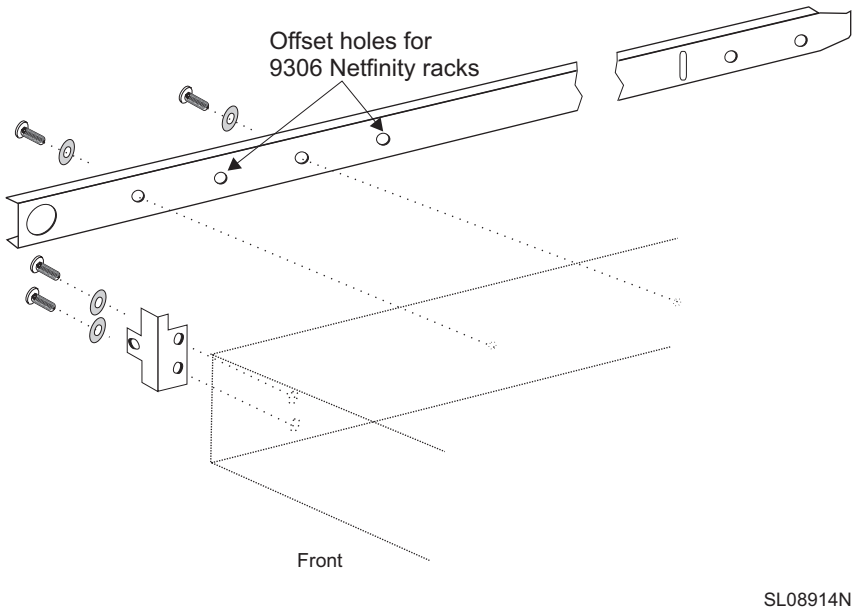


Figure 7. Mounting the moving portion of the slide and locking ears to the 3534 Managed Hub

2. Mount the fixed portion of the slide in the rack.

   a. Open the rack mounting brackets kit and mount the brackets to the wider, fixed portion of the slides (there are four of these). One bracket mounts to each end of the fixed portion of the slides.

   b. Leave the mounting screws on the rear bracket just finger tight. You will tighten the mounting screws after the 3534 Managed Hub is installed.

   c. The brackets on the front should be tightened, leaving approximately 15 mm (5/8-inches) of the bracket in front of the end of the outer fixed slide member. This allows space to install the locking ears.

      Attention: Ensure that you mount the brackets so that the 3534 Managed Hub sits level in the rack. You might need to adjust the alignment by loosening the four screws on the rack mounting brackets, checking the alignment, then retightening the screws as needed.

   d. Use the rack-mount clips and the longer screws provided to mount the fixed portion of the slides to the vertical mounting bars in the rack. See Figure 8 on page 24. Install three rack clips at the

front and at the back of the rack. The middle rack clip in the front is for the locking ears.

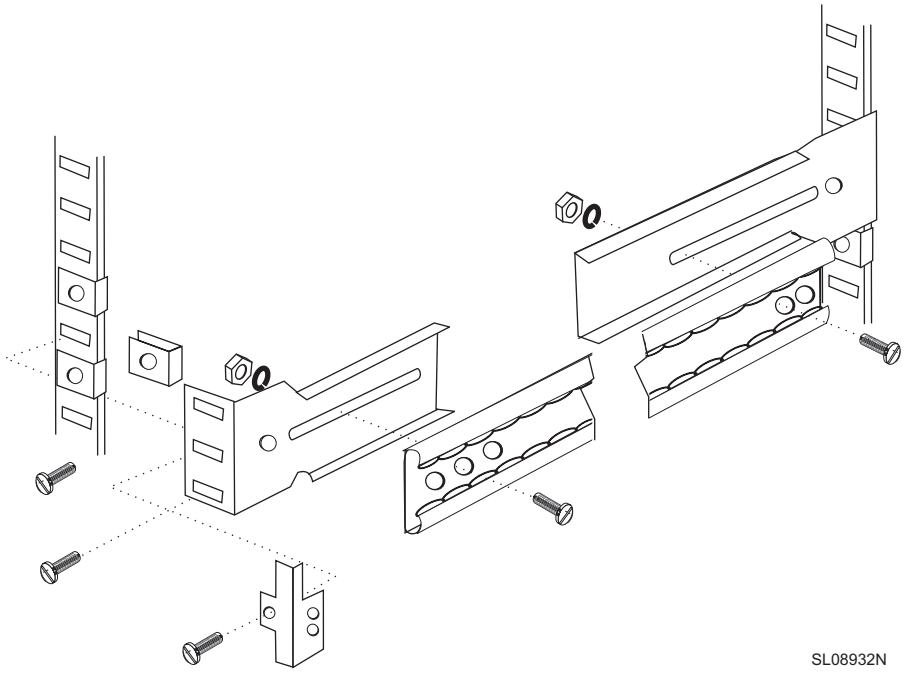


Figure 8. Mounting the fixed portion of the rail and securing the locking ears

3. Insert the 3534 Managed Hub and moving portion of the slides into the fixed portion of the slide on the rack.
   a. Lift the 3534 Managed Hub and match the portion of the rail that is mounted on the 3534 Managed Hub with the receiving rail members that are mounted in the rack as shown in Figure 9. Push the 3534 Managed Hub all the way into the rack.

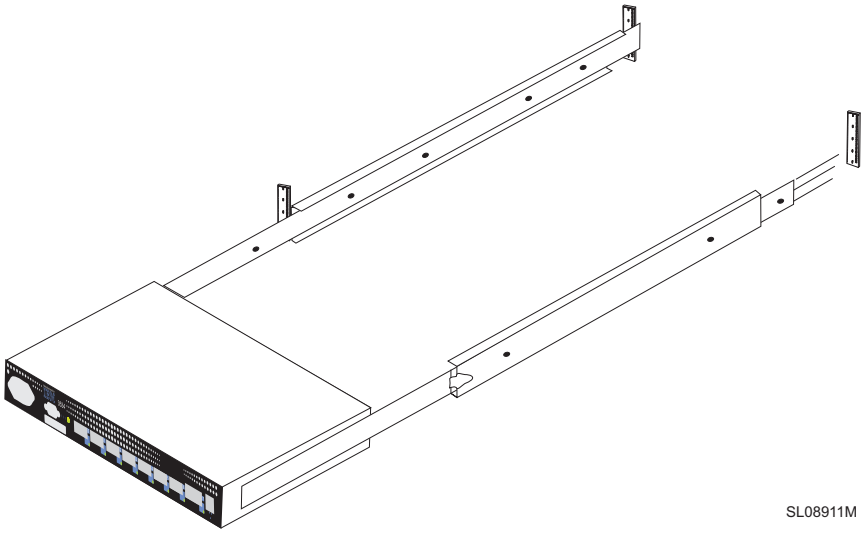


Figure 9. Inserting the slides into the rack rails

b. Slide the 3534 Managed Hub back and forth on the rail several times to make sure it moves easily. Move the 3534 Managed Hub partially forward and tighten the mounting screws on the rear brackets that were left finger-tight in step 2b.

4. Slide the 3534 Managed Hub fully back into the rack. Use the remaining screws provided with the locking ears to lock the 3534 Managed Hub in the rack. See Figure 8 on page 24.

This completes the rack-mount installation.

Installing the GBIC

The 3534 Managed Hub comes with seven fixed fiber-optic ports and one pluggable GBIC port as shown in Figure 10.

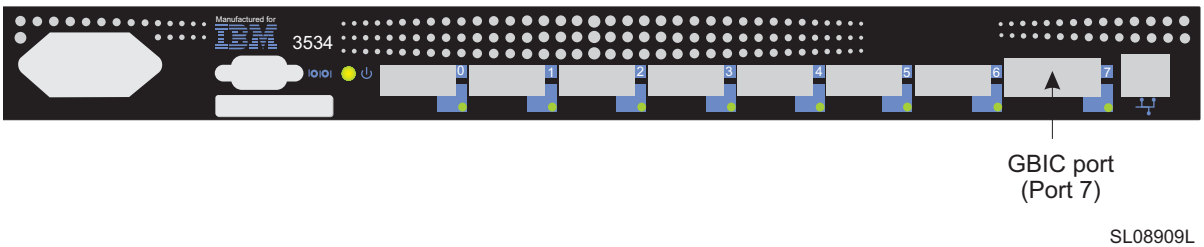


Figure 10. Location of the GBIC port

Leave the rubber dust protection plug inserted in the GBIC until a fibre-channel cable is inserted.

The GBICs are keyed and only seat if inserted correctly.

Figure 11 shows the front of the GBIC with the dust protection rubber plug removed. The plug should remain in place in the GBIC until a fibre-channel cable is inserted. The other end of the GBIC is inserted into the 3534 Managed Hub.

SL000143

Figure 11. Front end of the GBIC

Setting the IP address

The 3534 Managed Hub is shipped from the factory with a default IP address (10.77.77.77) pre-installed. 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.

If you can, use the default address to attach to your local area network (LAN) to establish a network connection to the 3534 Managed Hub. This is the easiest way to set the IP address. 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. Ask your system administrator if the default address can be used.

If you cannot use the default IP address, you can set the IP address with either the serial port or the Ethernet port. Setting the IP address through the serial port is the preferred method. To set the IP address, use the information provided by the system administrator on the pre-installation checklist. Figure 12 shows the location of the serial port and Ethernet port on the 3534 Managed Hub.

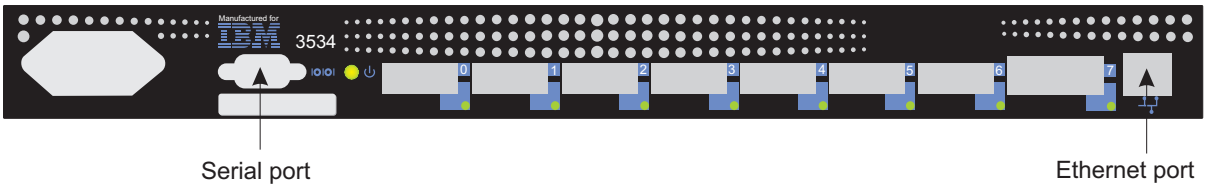


Figure 12. Serial port and Ethernet port on the 3534 Managed Hub

Setting the 3534 Managed Hub name

The **switchName** command sets the name of the 3534 Managed Hub.

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

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

The command syntax is:

```
switchName “new_name_of_hub”
```

```
switch : admin> switchName "sw3"
Updating flash...
```

The name can contain 19 characters, have alphanumeric characters, but the first character must be alphabetic.

Setting the IP address using the Ethernet port

Before attempting to set the IP address using the Ethernet port, the system administrator should provide a host on the same subnet as the 3534 Managed Hub. A secondary address should be set 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 30.

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

1. Attach the LAN 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 12 on page 27 for the 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)

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 from the label. If the IP address on the label was not used, you need to get the current IP address from the system administrator.

   The 3534 Managed Hub responds as shown below. For each prompt, type in the information as shown and press Enter.

   a. `Login: admin`

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

   b. `Password: password`

      This is the default password. You do not see the password as you type.

   c. `Ipaddress: admin> ipAddrSet`

      This is the command to set the IP address.

   d. `Ethernet IP address [current address is shown]: new IP address`

      This is the new address from the system administrator.

   e. `Ethernet Subnetmask [Current subnet mask is shown or None]: new Subnetmask or press Enter.`

      This is the new Subnet mask from the system administrator or, if none is required, press Enter.

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

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

   g. `Gateway address [Current Gateway address or None]:`

This is the Gateway address the system administrator provided or, if none is required, press Enter.

h. `Ipaddr:admin> logout`

This ends the Telnet session.

4. You have completed the installation of the 3534 Managed Hub. To check the 3534 Managed Hub fibre-channel ports, see "Verifying the 3534 Managed Hub installation" on page 36.

ipAddrSet example

ipAddrSet

Sets Ethernet and fibre-channel IP addresses.

Syntax

`ipAddrSet`

Availability

Administrator

Description

Use this command to set the Ethernet and fibre-channel IP addresses. You are prompted for:

```
Ethernet IP address:
        IP address of the Ethernet port.

Ethernet subnet mask:
        IP subnet mask of the Ethernet port.

Fibre-channel IP address:
        IP address of the fibre-channel ports.

Fibre-channel subnet mask:
        IP subnet mask of the fibre-channel
        ports.

Gateway address:
        IP address of the gateway.
```

After each prompt, the current value is shown. You can:

- Press Return to retain the current value.
- Enter an IP address in conventional dot (‘.’) notation.
- Type none.
- Press Ctrl+C to cancel changes.
- Press Ctrl+D to accept changes and end input.

The final prompt allows you to type y to set the new IP addresses immediately; or type n to delay the changes until the next switch reboot. (Entering y closes the Telnet session.)

A change to these values issues the domain address format required state change notification (RSCN).

Example

To enable 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
```

Setting the IP address using the serial port

Opening a HyperTerminal session varies depending on which version of Windows® you are using. The following procedure is based upon the use of a laptop computer running Windows 98. To start a Hyper-Terminal session, click **Start —> Programs —> Accessories**.

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:

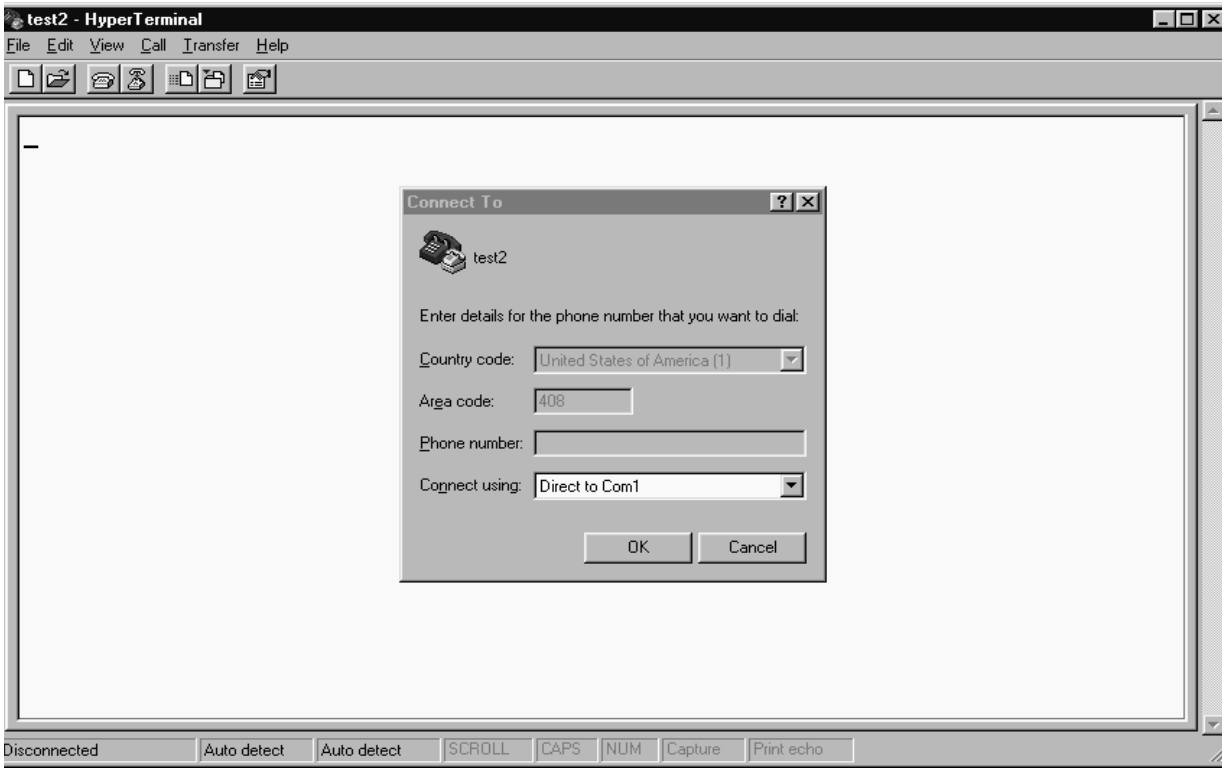
1. Using the serial cable that came with the 3534 Managed Hub, connect your service terminal (PC or laptop) to the serial port before plugging the 3534 Managed Hub into the electrical outlet. See Figure 12 on page 27 for the location of the serial port.
2. Start up a terminal emulation session.
   - Hyperterm
   - Flow control=no
   - Emulation=autodetect
3. Plug in the 3534 Managed Hub.
4. Open a HyperTerminal session and configure it as follows:
   a. In the Connection Description window (shown in Figure 13), type the name you want to use for your new session. Select any icon from the **Icon** menu, and click **OK**.

SL08939

Figure 13. Connection Description window

b. The Connect To window is displayed as shown in Figure 14.

   In the **Connect using** field, select **Direct to Com1** from the drop-down menu and click **OK**.



SL08940F

Figure 14. Connect To window

c. The COM1 Properties window is displayed, as shown in Figure 15.

   Set the following parameters in the **Port Settings** tab, then click **OK**.

   Bits per second: `9600`
   Data bits: `8`
   Parity: `None`
   Stop bits: `1`
   Flow control: `None`

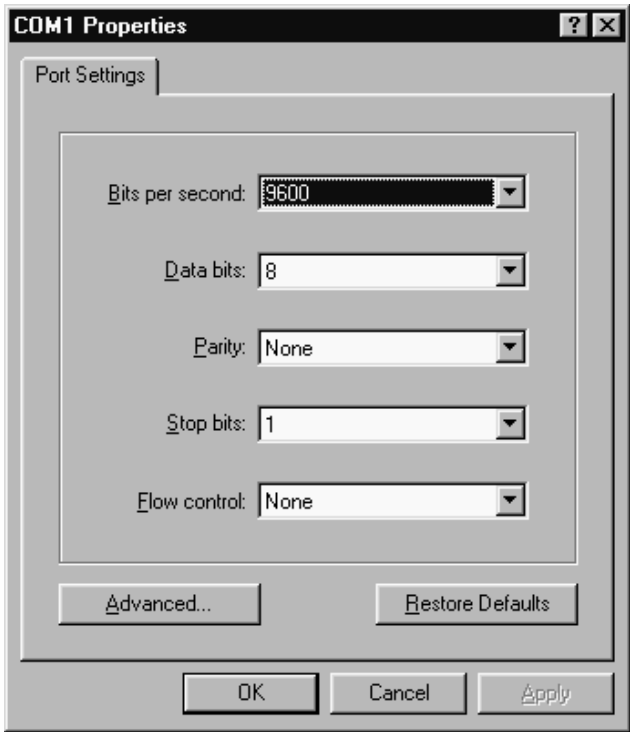


Figure 15. COM 1 Properties - Port Settings window

d. In the HyperTerminal window, click **File —> Properties**.

e. The Properties window is displayed as shown in Figure 16.

   Click the **Settings** tab, set the **Emulation** field to **autodetect,** then click **OK.**

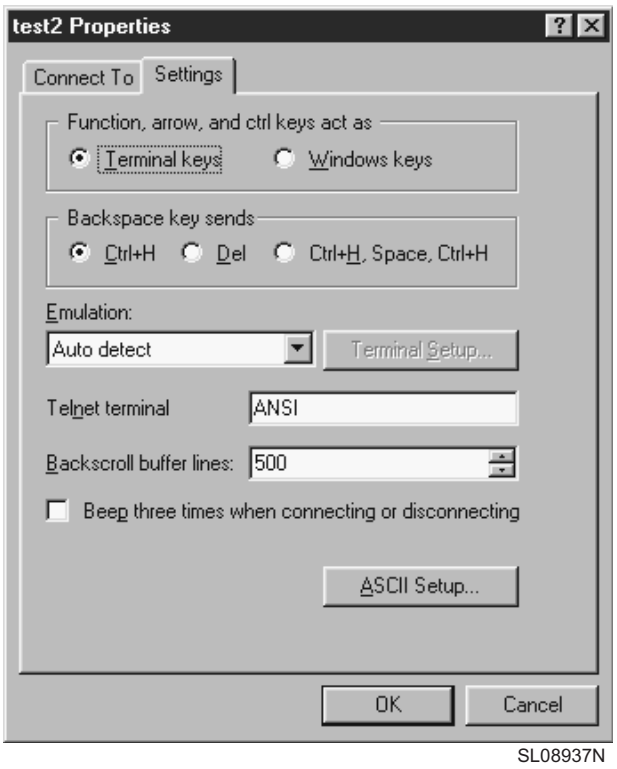


Figure 16. Settings - Emulation window

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)

5. Start up the 3534 Managed Hub by inserting the power cord into the electrical outlet and waiting for 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.

6. 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 17.

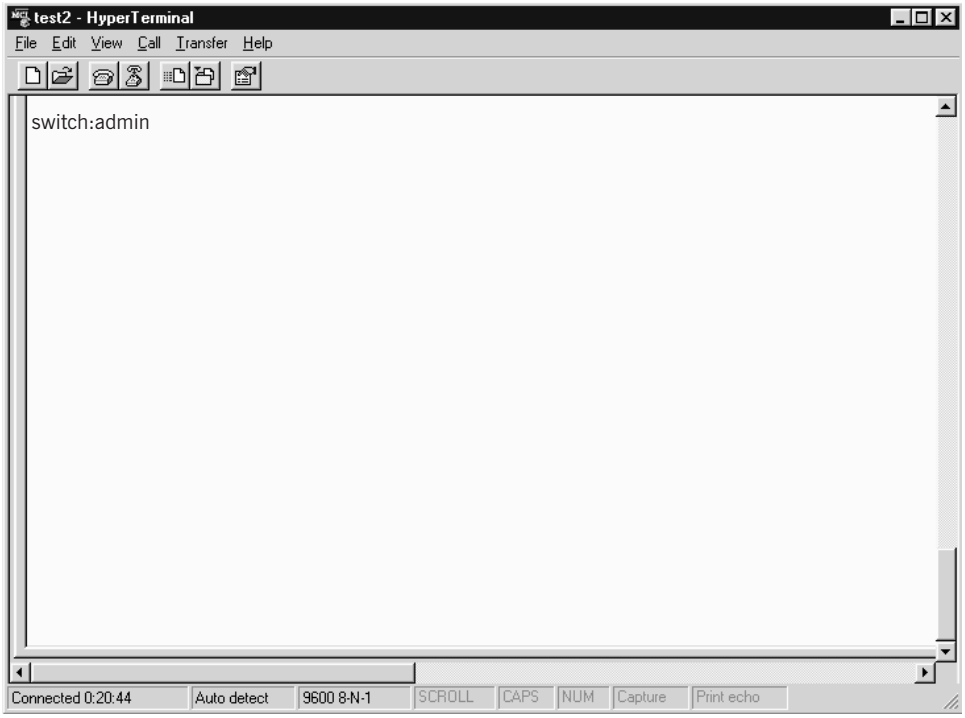


Figure 17. HyperTerminal session

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

a. `Admin> ipAddrSet`

   This command sets the IP address. See “ipAddrSet example” on page 29.

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

   This is the new address provided by the system administrator.

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

   This is the new Subnetmask provided by 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 provided by the system administrator.

g. `Admin> Logout`

This ends the Serial port session.

7. You have completed the installation of the 3534 Managed Hub. Remove the cable from the serial port connector. To check the 3534 Managed Hub fibre channel ports before turning the hub over to the system administrator, see “Verifying the 3534 Managed Hub installation” on page 36.

Verifying the 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 grey 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 any of these checks fail, refer to "Problem determination" on page 85. Otherwise, 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, new code is released that you can easily download 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 will need to 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

1. Download the firmware from the SAN Fibre Channel 3534 Managed Hub Web site at:

   www.ibm.com/storage/fchub

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

   ```
   Password: password
   ```

5. Type the following command:

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

   For example:

   ```
   firmwareDownload "192.111.2.1", "timm", "/tmp/os/
   v2.1.3"
   ```

   where:

   host name/IP address
   Either the name of the host or the IP address of the host

username
A valid host username

filename
The path to the new firmware file.

The RSH server validates the user name 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

1. Download the firmware from the SAN Fibre Channel 3534 Managed Hub Web site at:

   www.ibm.com/storage/fchub

   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 RSHD daemon. There is no need to run the cat.exe utility as this is done automatically.
4. Go to "Downloading firmware from a UNIX host" on page 37. Follow steps 2 through 6.

Note: When downloading firmware to a 3534 Managed Hub using the **firmwareDownload** command, use the UNIX directory (forward slash /) addressing, and not the PC directory (backward slash \) addressing 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 4. Feature code upgrades

This chapter contains the following optional features:

- Entry Fabric Switch feature code upgrade
- Fabric Watch feature code upgrade

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 3534 Entry Fabric Switch 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 3534 Entry Fabric Switch is ideally suited for low-end SAN environments with hosts and devices that support FC_AL. The 3534 Loop Switch feature supports the use of FL_ports only.

The IBM 3534 Entry Fabric Switch 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 loop switch supports F and FL ports and the name server (1E_port).

Switch usability information can be obtained from the *IBM SAN Fibre Channel Managed Hub User's Guide*. This book introduces the IBM 3534 Managed Hub 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 3534 Managed Hub remotely.

You can view this book at the following Web site:

www.ibm.com/storage/fcswitch/

With this upgrade applied, this unit performs as an eight-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 3534 Managed Hub, type `licenseShow` on the Telnet command line. For additional information, see "Installing Fabric Watch through Telnet" on page 42.

This section describes the Fabric Watch software and how to install it, plus detailed information for using thresholds to manage 3534 Managed Hub functions.

Fabric Watch allows the SAN manager to monitor key fabric and 3534 Managed 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 element exceeds 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 Hub with Fabric OS, version 2.2 or later. You can access Fabric Watch 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 3534 Managed 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** command. See “fwConfigure” on page 55 for more information.

Threshold behavior models

There are three thresholds 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 18.

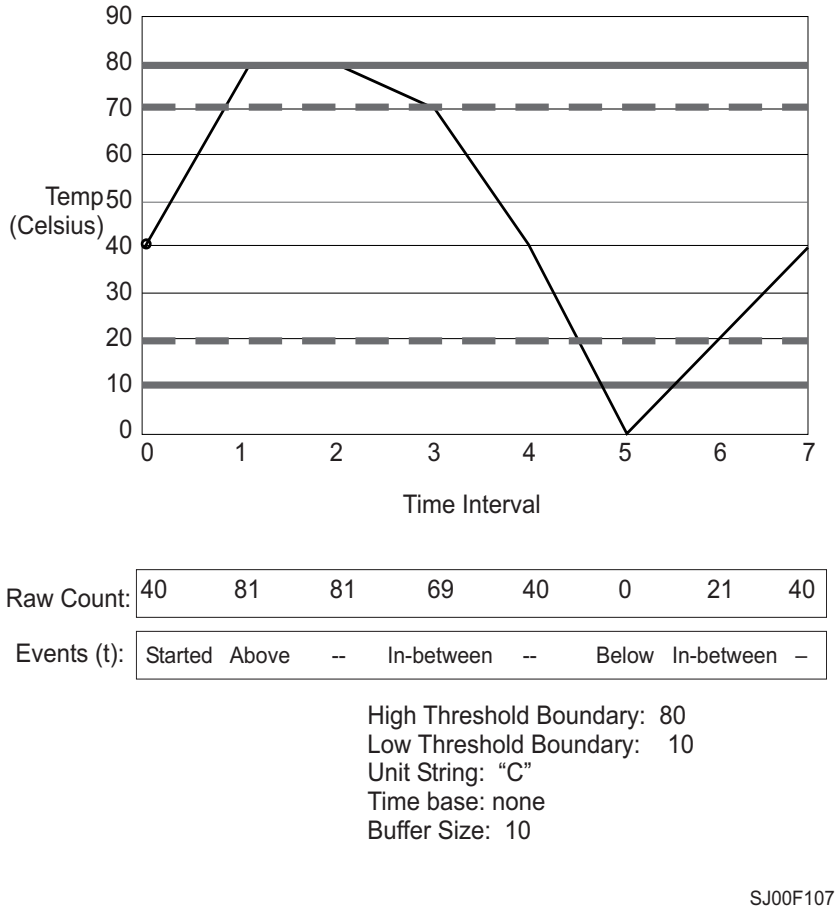


Figure 18. Example of range threshold: temperature (Celsius)

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 or falling threshold is error rate as shown in Figure 19.

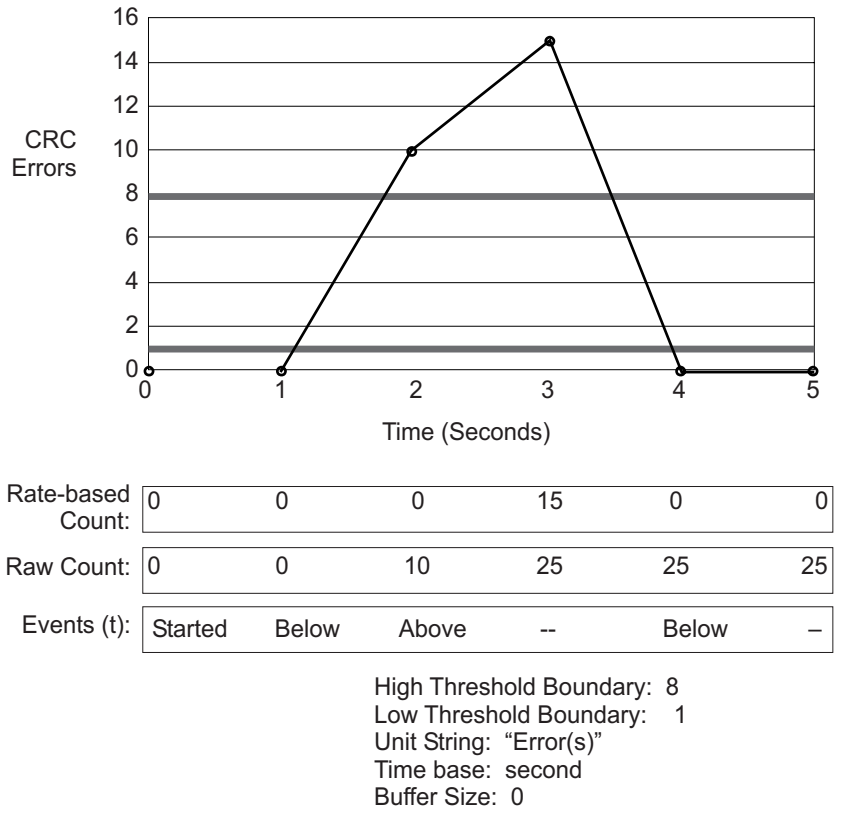


Figure 19. Example of rising and falling threshold: error rate

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

To use 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 in the 3534 Managed 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 with either the Telnet commands or the IBM StorWatch Specialist.

Installing Fabric Watch through Telnet

Perform the following steps to install Fabric Watch through Telnet.

1. Log onto the 3534 Managed Hub through 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 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
   QuickLoop license
   ```

   If the Fabric Watch license is not included in the list or is incorrect, continue to 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 to Step 5.
5. Load the Fabric Watch classes and areas by doing one of the following:
   - Typing the Telnet command: `fwClassInit`
   - Restarting the 3534 Managed Hub.

The Fabric Watch feature is available as soon as you complete Step 5.

Installing Fabric Watch using the IBM StorWatch Specialist

To install Fabric Watch with the IBM StorWatch Specialist, perform the following steps.

1. Launch the Web browser. Type the 3534 Managed Hub name or the IP address in the **Location/ Address** field (for example: `http://111.111.222.33`), and press Enter.

   The IBM StorWatch Specialist launches, displaying the Fabric View.

2. Click the **Admin** button on the relevant 3534 Managed 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 doing one of the following:

   - Typing the Telnet command: `fwClassInit`
   - Restarting the 3534 Managed Hub.

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

Using Fabric Watch

Fabric Watch provides the following 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 alarm event that was generated

User interfaces

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

With the IBM StorWatch Specialist, you can:

- View the fabric and 3534 Managed Hub events with the Fabric-wide Event view.
- View and modify the threshold and alarm configurations with the Fabric Watch View.
- Upload and download the configuration file with the **Config Admin** tab in the Hub Admin window.

Telnet interface

You can perform the following actions using a Telnet interface:

- Query fabric and 3534 Managed 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. You can use the Base (MIB) variables to perform the following actions:

- Query the MIB variable for individual fabric and 3534 Managed 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 3534 Managed Hub to the host, editing the file with a text editor, then downloading the modified file back to the 3534 Managed Hub. You can then ensure a uniform configuration throughout the fabric by distributing the configuration file to all the 3534 Managed Hubs in the fabric.

The configuration file can be uploaded and downloaded through either the IBM StorWatch Specialist (with the **Config Admin** tab in the Hub Admin window) or the **configUpload** and **configDownload** commands. After downloading the configuration file back to the 3534 Managed Hub, you must either restart the 3534 Managed Hub or use the **fwConfigReload** command to reload the configuration file.

Classes

Fabric and hub elements are organized into groupings of closely related elements, which are called classes.

There are seven major classes:

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

Environmental
Monitors the 3534 Managed Hub environmental 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_port error and performance counters.

F/FL_port (copper)
Monitors copper F/FL_port error and performance counters.

GBIC Monitors operational values for smart GBICs.

In addition, each class is subdivided into areas, as listed in Table 14.

Table 14. 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 14. 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.
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 lowercase characters). Table 15 lists the valid class name abbreviations.

  Table 15. Abbreviations for the class names

Class	Abbreviation
Fabric	fabric
Environment	env
Port	port
E_port	eport
F/FL_port (optical)	fopport
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 3534 Managed 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 3534 Managed 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 can flag an event (as shown in *Triggered events*). Then the threshold is hidden and disabled. When an item is added, the threshold is displayed and enabled, and Fabric Watch can 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. For example, if the 3534 Managed Hub temperature exceeds the upper boundary, a triggered event is generated at the point that the boundary is exceeded, 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 the buffer, or rises above the lower boundary plus the 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 generates 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, hub event 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 3534 Managed 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 3534 Managed 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.

Threshold area values

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.

Alarms

The following alarms can be added or deleted:

ERRLOG Logs errors to the 3534 Managed Hub. If configured correctly, 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

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 3534 Managed Hub. In this case, changes from one connection might not be updated to the other, and some may be lost. If "`Committing configuration...`" is displayed during a Telnet session, then the configuration might have recently been modified from another connection. Table 16 contains a summary of the Fabric Watch Telnet commands, including a reference to the detailed explanation of the command.

Table 16 contains a summary of the Fabric Watch Telnet commands, including a reference to the detailed explanation of the command.

Table 16. Fabric Watch Telnet commands

Command	Description	Page
fwClassInit	Initializes all classes under Fabric Watch.	53
fwConfigReload	Reloads the Fabric Watch configuration.	54
fwConfigure	Displays and allows modification of threshold information and the Fabric Watch configuration.	55
fwShow	Displays the thresholds that are monitored by Fabric Watch.	58

fwClassInit

The **fwClassInit** command initializes 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

The following is an example of 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 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

The following is an example of 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 the Fabric Watch configuration and status. It also allows modification of this information

Syntax

```
fwConfigure
```

Availability

Administrator

Description

Allows the admin account to display and modify threshold information and the Fabric Watch configuration. The 3534 Managed Hub elements 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 following table shows the Fabric Watch classes and areas.

Class	Area
Fabric	Loss of E_port Fabric reconfigure Segmentation changes Domain ID changes Zoning changes Fabric to QuickLoop changes Fabric logins GBIC state change
Environment	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 is an example for 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 that are monitored by Fabric Watch.

Syntax

```
fwShow
```

Availability

All users

Description

Use 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 3534 Managed 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.

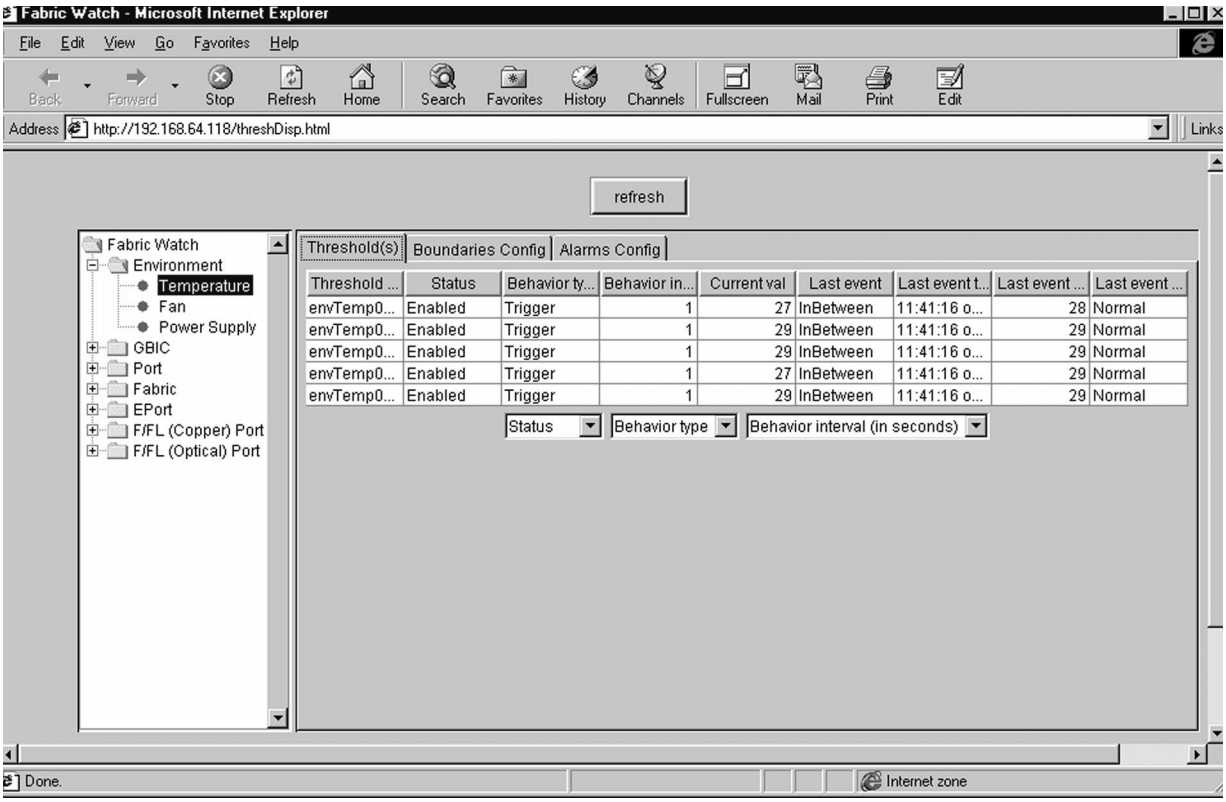
Fabric Watch view contains three tabs: **Threshold**, **Boundaries Config**, and **Alarm Config**. The following items are visible regardless of which tab is selected:

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

Use the **Threshold** tab to configure Fabric Watch thresholds. See Figure 20.



SJ00F13(

Figure 20. Threshold tab in 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 status of a threshold, select the threshold name, click the Status drop-down list, and select the new status.

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 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
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 (value that generated the last event).

Last event state
Displays the last state of the event.

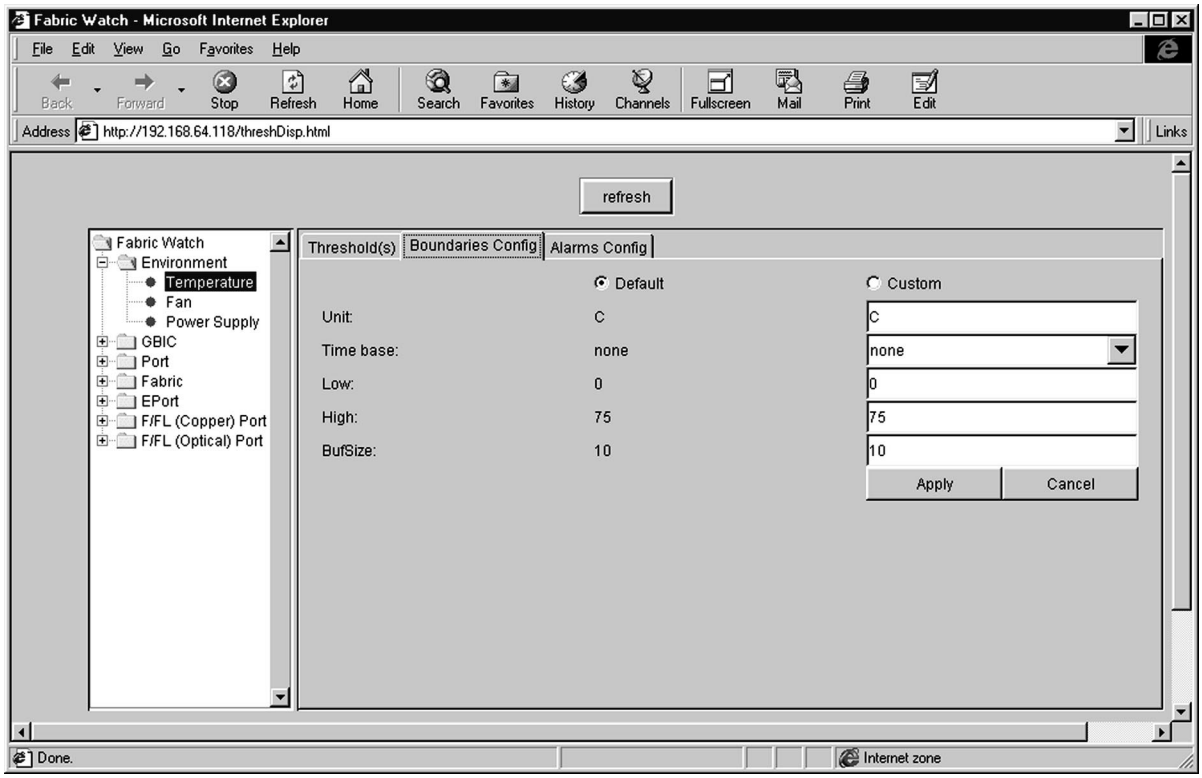
Status drop-down list
Click to select the status (enabled or disabled) of the selected threshold.

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

Use the **Boundaries Config** tab to configure Fabric Watch boundaries. See Figure 21.



SL000162

Figure 21. Boundaries Config tab in the Fabric Watch view

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

Default Displays the default values for the boundary configuration:

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 the boundary configuration:

Changed
Exceeded
Below
Above
InBetween

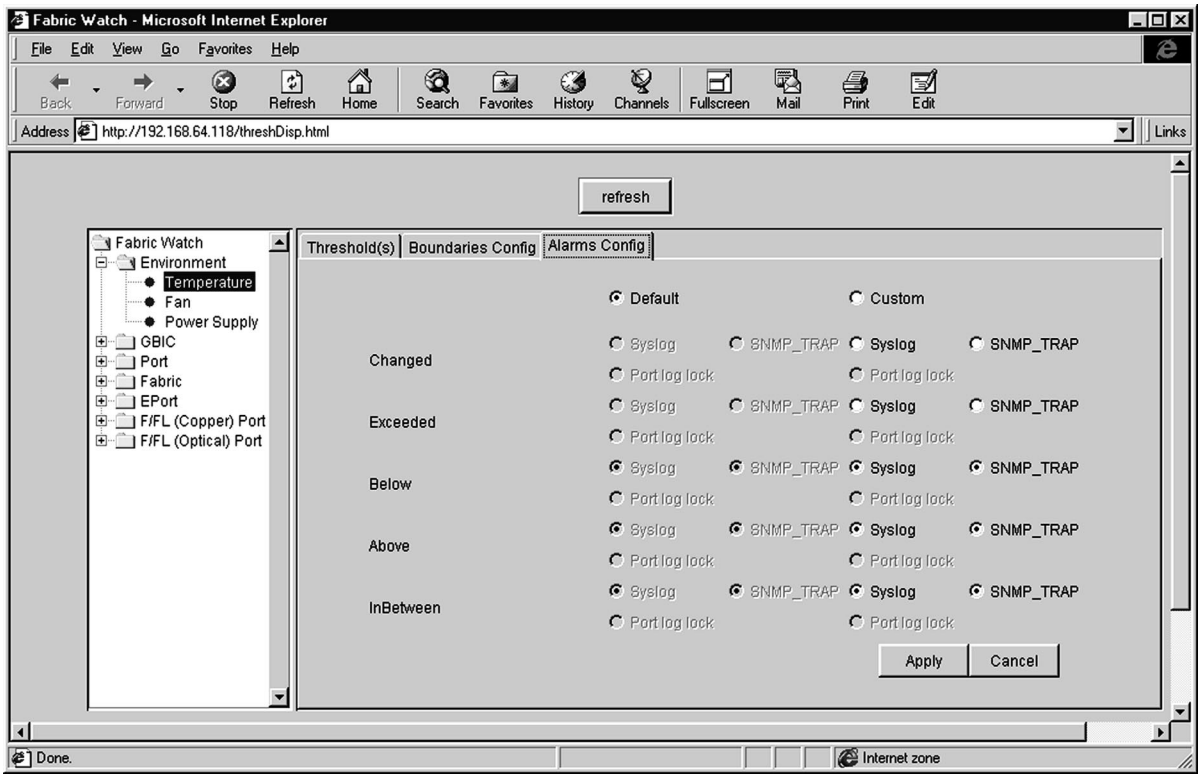
Select Syslog, SNMP_Trap, or Port log lock to indicate the type of alarm that you want to associate with each event.

Apply Click to apply specified values.

Cancel Click to cancel changes made to custom values.

Alarm config tag

Use the **Alarm Config** tab to configure Fabric Watch alarms. See Figure 22.



SL000161

Figure 22. 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.

The enterprise-specific trap is sent by Fabric Watch about an event 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 the 3534 Managed Hub status. If the 3534 Managed 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/`

   The 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 available in the Hub view.

   Fabric 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 3534 Managed Hub serial number

- The 3534 Managed Hub world-wide name
- 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 following Web site:

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. For information on Quickloop, see the *"IBM 3534 SAN Fibre Channel Managed Hub User's Guide."* The following topics are discussed:

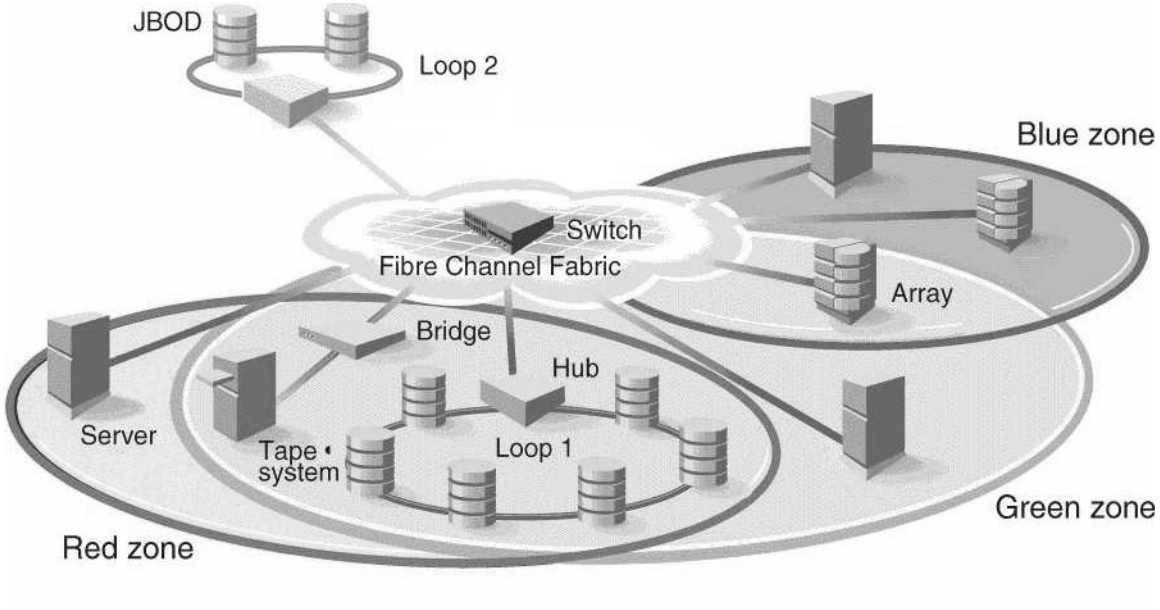
- Overview
- Zoning components
- Zone management
- Zone enforcement
- Multiswitch fabrics
- Zoning commands

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 23 on page 68 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.



SL000137

Figure 23. 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 (FLOGI or 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 Figure 24 on page 73.

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 an initiator sees 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 23 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 24 shows the configuration, with an additional disk drive loop to which none of the zones can communicate.

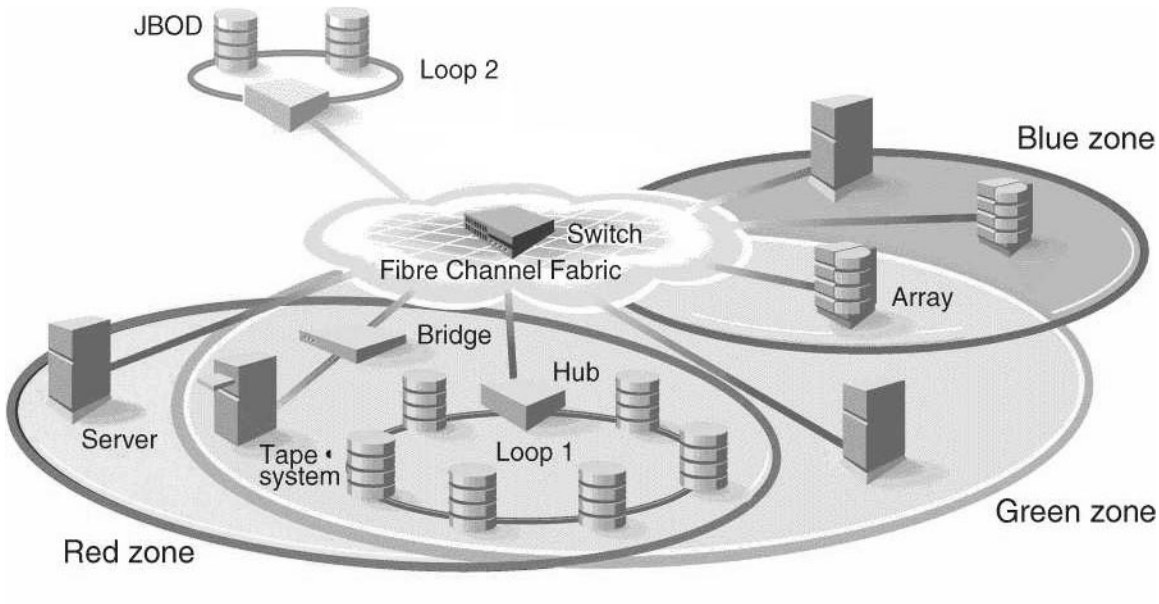


Figure 24. Zone management example

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 80 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 76. 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 17 summarizes the zoning commands.

Table 17. Zoning commands summary

Command	Description	See page
Zone alias commands		
aliAdd	Adds a member to a zone alias	78
aliCreate	Creates a zone alias	78
aliDelete	Deletes a zone alias	78
aliRemove	Removes a member from a zone alias	79
aliShow	Shows a zone alias definition	79
Zone configuration commands		
cfgAdd	Adds a zone to a configuration	79
cfgCreate	Creates a zone configuration	79
cfgDelete	Deletes a zone configuration	80
cfgRemove	Removes a zone from a configuration	80
cfgShow	Shows a zone configuration definition	80
Zone commands		
zoneAdd	Adds a member to a zone	80
zoneCreate	Creates a zone	81
zoneDelete	Deletes a zone	81
zoneRemove	Removes a member from a zone	81
zoneShow	Shows a zone definition	82

Command	Description	See page
Configuration management commands		
cfgClear	Clears all zone configurations	82
cfgDisable	Disables a zone configuration	82
cfgEnable	Enables a zone configuration	83
cfgSave	Saves zone configurations in flash memory	83
cfgShow	Shows a zone configuration definition	84

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. Service procedures

Note: Throughout this guide, the term *switch* refers to switches and hubs unless otherwise noted.

This chapter discusses the service procedures for the IBM 3534 SAN Fibre Managed Hub. Following these procedures resolves most 3534 Managed Hub and GBIC failures.

The 3534 Managed Hub provides extensive diagnostics that can be used in extended service environments that are not resolved in these service procedures. See “Appendix B. Diagnostics” on page 105 for information about these diagnostics. Before you begin, see Figure 25 to familiarize yourself with the location of the various 3534 Managed Hub components and indicators.

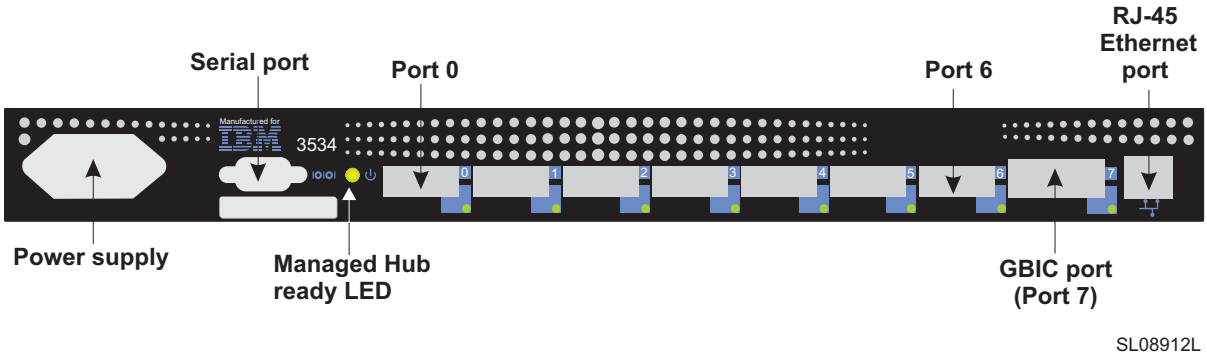


Figure 25. Front panel of the 3534 Managed Hub

Problem determination

Attention: If you are going to service a functional 3534 Managed Hub, never unplug cables or GBICs when there is activity on the associated ports. This causes immediate failure of the communications path. To determine if a port has active communications, see "Visually inspect LEDs" on page 86. If it becomes necessary to unplug active ports, the customer must stop communications on these ports.

Always begin problem determination here by checking the following areas. Before performing any repair action, gather as much information as possible.

For the latest information on the 3534 SAN Fibre Channel Managed Hub, see the following Web site at:

www.ibm.com/storage/fchub

System reported error or failure to access a device

Either the customer has reported a 3534 Managed Hub related system error message or the customer has reported a failure accessing storage or hosts attached to the 3534 Managed Hub. If the host reported error message from the 3534 Managed Hub is known, or a customer communications failure symptom is known, see the “Service reference table” on page 87. After identifying the error message or the symptom, perform the recommended service action.

Visually inspect LEDs

Observe the front panel LED status indicators, then check the information in “Service reference table” on page 87. If a faulty condition is observed, perform the recommended service action.

Determine if zoning is in effect

The 3534 Managed Hub implements *zoning*. Zoning is a feature that permits a system administrator to define port and AL_PA communication setup and permissions. It is possible that the customer has ports zoned in a way that prevents them from communicating. Ask the customer if zoning is in effect. If it is, the customer should check the zoning setup to make sure that zoning is not the source of the problem.

Zoning is explained in the *IBM 3534 SAN Fibre Channel Managed Hub User’s Guide*. To display and check zones, the customer must log on to the 3534 Managed Hub using Telnet in admin mode and issue the **zoneShow** command. Zone management can also be shown by using zone administration from the Storwatch Managed Hub Specialist Web interface. Any active or configured zones are displayed.

Check for problems on attached devices

To determine if the source of the problem is an attached device, check the following:

- LEDs
- Display panels
- Firmware levels
- Operating status

Check FC host versions

For an updated list of supported host platforms and fibre-channel host bus adapters, see the following Web site at:

www.ibm.com/storage/fchub

You need to determine the following:

- Operating system version
- Service pack version
- Hot fix version
- HBA hardware version
- HBA firmware version
- HBA device driver version

If an update is required, perform the update.

Service reference table

Table 18 lists the types of error messages or failure indications that might be encountered. For the recommended action, see the corresponding action code in Table 19, “Action codes and recommended actions,” on page 88.

Table 18. Service reference table

Description	Action Code
System reported error message	
The customer has reported that a fan failure was reported to the system.	1
Customer reports a failure to communicate with a host or device	
Communication failure on all ports.	2
Communication failure on some ports.	3
Visual LED observation.	
Slow yellow blink port LED (2 second blink).	3
Fast yellow blink port LED (1/2 second blink).	3
Steady yellow port LED.	3
Slow green blink port LED (2 second interval).	3
Fast green blink port LED (1/2 second interval)	3
Steady green port LED (port is online and the connected host/ device is not sending data).	0
Flickering green port LED (port is online and the connected host/ device is sending data.	0
Interleaving green and yellow port LED (port is bypassed).	5
Port LED is off on port 7 (and a GBIC and cable are installed).	3
Port LED is off on port 7 (no GBIC installed).	0
Port LED is off on port 7 (GBIC installed but no cable).	3
Ready LED is anything other than steady green.	3
Port LED is off on port 0, 1, 2, 3, 4, 5, or 6 (and a cable is installed).	3
Port LED is off on port 0, 1, 2, 3, 4, 5, or 6 (but no cable is installed).	3

Action codes and recommended actions table

Table 19 lists the action codes and the recommended actions.

Table 19. Action codes and recommended actions

Action code	Action
0	Normal, no action required.
1	See “Fan failure (action code 1)” on page 88.
2	See “All ports fail to communicate (action code 2)” on page 88.
3	See "Abnormal port LED function (action code 3)" on page 89.
4	See "Abnormal Ready LED (action code 4)" on page 91.
5	See "Port in bypass mode (action code 5)" on page 91.
6	See “Checking the customer configuration (action code 6)” on page 92.
7	See “Suspect fiber-channel cable (action code 7)” on page 92.

Fan failure (action code 1)

You are here because a 3534 Managed Hub message to the system indicates that a fan failure has occurred, or you suspect a fan failure for another reason.

Replace the 3534 Managed Hub. See "Replacing the 3534 Managed Hub" on page 96.

All ports fail to communicate (action code 2)

You are here because there is a complete failure (no data can be passed through the hub).

1. Observe the front of the 3534 Managed Hub. If the ready LED is on and steadily green, see “Abnormal port LED function (action code 3)” on page 89.

   If not, verify the following:

   a. The power cord is seated.

   b. There is power in the electrical outlet.

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. If the LED is now on, unplug the unit from the electrical outlet, wait 15 seconds, then plug the unit into the electrical outlet. If the ready LED

is on and steadily green, go to "Verifying a repair that required 3534 Managed Hub replacement" on page 98.

3. If the ready LED is not on and steadily green, replace the entire 3534 Managed Hub. See "Replacing the 3534 Managed Hub" on page 96.

Abnormal port LED function (action code 3)

You are here for one of the following reasons:

- You started from the action code for a total hub failure, and observed the ready LED was functioning normally.
- The customer reported that only some ports were failing while others were operating.
- You observed an abnormal LED status on one or more ports.

Be sure that all cables and GBICs are properly seated. Observe the LEDs for the failing ports. If you do not know which ports are failing, go to "Checking the 3534 Managed Hub" on page 90.

1. If the port LED blinks slow yellow (blinks every two seconds), the port is disabled. The customer needs to re-enable the port using the Storwatch Managed Hub Specialist Web interface or a Telnet session. See the *IBM 3534 SAN Fibre Channel Managed Hub User's Guide* for information about disabling and re-enabling ports. Have the customer re-enable the port.
2. If the port LED blinks fast yellow (blinks every 1/2 second):
   a. Remove the incoming cables from the failing ports. Mark them to ensure that you can return them to the same port.
   b. If the port is port 7, remove and reseat the GBIC.
   c. Insert one of the small single GBIC port wrap connectors (black for ports 0 - 6). For port 7, the connector is black if the GBIC is short wavelength or gray if it is long wavelength. Wait 10 seconds and observe the associated port LED. If it is blinking green, the GBIC and port are functional. Do this for all suspect ports. If all ports show a blinking green port LED, check the other customer configuration information or the associated fibre-channel cables. See "Checking the customer configuration (action code 6)" on page 92 and "Suspect fiber-channel cable (action code 7)" on page 92.
   d. If any of the LEDs for ports 0 - 6 do not blink green, replace the 3534 Managed Hub. See "Replacing the 3534 Managed Hub" on page 96. If the LED for port 7 does not blink green, replace the GBIC with a new (known good) GBIC.
   e. After replacing the GBIC in port 7, again insert the single port wrap connector. If the port LED still does not blink green, replace the 3534 Managed Hub. See "Replacing the 3534 Managed Hub" on page 96.
3. If the port LED is steady yellow, this indicates that the port is receiving a signal, but the attached device is not yet online and the device is probably not in the ready state. Have the customer make the device

ready. If the customer is unable to correct the problem, see "Abnormal port LED function (action code 3)" on page 89.

4. If the port LED blinks fast green (1/2-second blink, not a flickering light), replace the 3534 Managed Hub. See "Replacing the 3534 Managed Hub" on page 96.
5. If the port LED blinks slow green (every 2 seconds), it indicates that a bad cable or a wrap cable is installed.
   a. Verify if a wrap cable is installed or if a wrap connector is installed at the other end of the cable. If either of these situations is true, correct it.
   b. If a wrap cable or wrap connector is not installed, replace the cable or ask the customer to have his cabling supplier check the cable, whichever is appropriate.
   c. If you are replacing the cable, see “FRU list” on page 95. There are FRU part numbers for the 5 m (16.4 ft.) and the 25 m (82 ft.) short wavelength cables supplied with this product.
6. If the port 0 - 6 LEDs show no light with no cable installed, or if port 7 shows no light with a GBIC installed but no cable:
   a. This is normal. A cable from an appropriate device needs to be installed if the port is to be used.
   b. If the device cable is present, insert the cable into the GBIC or port.
7. If the port LED shows no light and a cable is installed, make sure that the attached device is turned on and ready.
8. If the attached device is turned on and ready, it is necessary to check other customer configuration information, or the associated fibre-channel cables. See "Checking the customer configuration (action code 6)" on page 92 and "Suspect fiber-channel cable (action code 7)" on page 92.

Checking the 3534 Managed Hub

Attention: Do not remove cables or GBIC from ports that are:

- Blinking green: This is a normally operating port with communications in progress.
- Steady green: The port is connected to a functional device, but there is no data traffic in progress. If this port is believed to be the problem, the failure is not with the 3534 Managed Hub. Instead, the attached device or host is not attempting to send data. See the appropriate host, device, or application documentation to resolve the problem.

Use the following procedure to ensure that the 3534 Managed Hub is operating correctly.

1. Remove the incoming cables from the suspect ports. Mark them to make sure that you can return them to the same port.
2. Remove and reseat the GBIC in port 7 if it is installed.
3. Insert one of the small single GBIC port wrap connectors (black for ports 0 - 6). For port 7, the connector is black if the GBIC is short wavelength or gray if it is long wavelength.

   Wait 10 seconds and observe the associated port LED. If it slowly blinks green (every 2 seconds), the GBIC and port are functional. Do this for all suspect ports.
4. If all ports slowly blink green (every 2 seconds), check the customer configuration information or the associated fibre-channel cables. See "Checking the customer configuration (action code 6)" on page 92 and "Suspect fiber-channel cable (action code 7)" on page 92.
5. If any of the LEDs for ports 0 - 6 do not blink green, replace the 3534 Managed Hub. See "Replacing the 3534 Managed Hub" on page 96. If the LED for port 7 does not blink green, replace the GBIC, then continue with step 6.
6. After replacing the GBIC in port 7, insert the single port-wrap connector. If the port LED still does not blink green, replace the 3534 Managed Hub. See "Replacing the 3534 Managed Hub" on page 96.

Abnormal Ready LED (action code 4)

You are here because you have seen an abnormal indication for the ready LED.

1. Verify the following:
   a. The power cord is seated.
   b. There is power in the electrical outlet.

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. If the LED is now on, unplug the unit from the electrical outlet; wait 15 seconds, then plug the unit back into the electrical outlet. If the ready LED is on and steadily green, go to "Verifying a repair that required 3534 Managed Hub replacement" on page 98.
3. If the ready LED is not on and steadily green, replace the entire 3534 Managed Hub. See "Replacing the 3534 Managed Hub" on page 96.

Port in bypass mode (action code 5)

The port is in bypass mode because it has been unable to initialize the link.

1. Remove the cable from the port. The LED should go off.
   - If the LED goes off, go to step 2.
   - If the LED stays interleaving green and yellow, go to step 3.
   - If the LED goes to some other state, note the new state and refer to “Appendix B. Diagnostics” on page 105 to determine the correct action.
2. The LED is off. This state is normal operation for the 3534 Managed Hub. When the cable was connected, the LED was interleaving green and yellow, indicating that the port was not receiving correct information over the fiber link to enable it to correctly initialize the link. See the appropriate manual for the device at the other end of the cable, and resolve why a valid link initialization frame is not being sent.
3. When the cable is removed, the LED should go off. However, if it interleaves green and yellow, there is a problem with the hub.
   - If the interleaving port is 0 - 6, you must replace the hub. See "Replacing the 3534 Managed Hub" on page 96.
   - If the interleaving port is port 7, replace the GBIC and see if this resolves the problem. See "Replacing a GBIC module" on page 96. If replacing the GBIC module does not solve the problem, you must replace the 3534 Managed Hub. See “Replacing the 3534 Managed Hub” on page 96.

Checking the customer configuration (action code 6)

1. Check the customer configuration to ensure that the customer has appropriately configured any systems, HBAs, storage devices, and code levels.

   To get the latest information on compatible devices and hosts, see the following Web site at:

   www.ibm.com/storage/fchub

2. The HBAs should be running in FCAL mode. You should run diagnostics as available on the systems HBAs.

   If the HBAs are correctly configured and pass diagnostics, and you have not found any fault with the 3534 Managed Hub after reviewing and following all other instructions in the service procedures, you might need to replace the fibre-channel cable. See "*Suspect fiber-channel cable (action code 7)* ."

Suspect fiber-channel cable (action code 7)

To check the fiber-channel cable, perform the following steps:

1. Verify that the ends of the suspect cable are fully seated.
2. Verify that the pair of fibre connectors are correctly oriented at both ends of the cable. You can check the cable by swapping the two fibres at one end to see if this corrects the problem. If this does not

correct the problem, restore the fibre cables to their original configuration.

3. If the HBA does not have wrap capability and you have access to both ends of the cable, check the cable by plugging it into two short wavelength ports on the same 3534 Managed Hub, if available. To do this test, make sure that the length of the of cable is less than 500 m for short wavelength. Many bad cables can be detected by simply plugging them into two ports and observing the port indicator LEDs. The LEDs should blink slow green (every 2 seconds). If they do not, the cable is bad.
4. If the host or device HBA has a diagnostic to wrap a cable, perform this diagnostic. If the diagnostic still reports failure, replace the cable or have the customer replace the cable.
    a. If this is an IBM-provided cable, replace the cable. There are two lengths of cable available for the 3534 Managed Hub: 5 m (16.4 ft.) and 25 m (82 ft.) short wavelength. If these are appropriate, replace the cable.
    b. If the cables were obtained from some other IBM product, you need to determine the appropriate FRU.
    c. If the customer obtained the cable from someone other than IBM, the customer needs to replace the cable.
5. If the LED blinks slow green, you can test it further by using the CrossPort diagnostic test. See “crossPortTest” on page 125.
6. If it is not possible or not appropriate to access the 3534 Managed Hub in this way, replace the short cable. If you are dealing with a long cable or one where both ends cannot be accessed at the 3534 Managed Hub, you need to have the cable installer test the cable.

Chapter 7. Field replaceable units

This chapter describes the field replaceable units (FRUs) available for the 3534 Managed Hub, the procedures to replace them, and the procedure to verify the repair.

Note: Throughout this guide, the term *switch* refers to switches and hubs unless otherwise noted.

FRU list

Table 20 lists the field replaceable units available for the 3534 Managed Hub.

Table 20. Field replaceable units

Description	Part number	Replacement procedures
3534 Managed Hub FRU	35L1801	See "Replacing the 3534 Managed Hub" on page 96.
Power cord	36L8886	None
GBIC module LW	03K9208	See "Replacing a GBIC module" on page 96.
GBIC module SW	03K9206	See "Replacing a GBIC module" on page 96.
5-meter fibre-channel cable	03K9202	None
25-meter fibre-channel cable	03K9204	None
Rack slides	34L2722	See "Installation instructions" on page 20.
Rack-mount brackets	34L2767	See "Installation instructions" on page 20.
Switch securing ears	34L2723	See "Installation instructions" on page 20.

Replacing 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)

To replace a 3534 Managed Hub, perform the following steps:

1. Check with the customer to verify that the unit to be replaced is not currently being used.
2. Unplug the 3534 Managed Hub from the electrical outlet.
3. Remove all cabling that is attached to the front panel. Label the fiber cables before removing them.
4. Remove the GBIC that is plugged into port 7, if applicable.
5. If the 3534 Managed Hub is installed in a rack, remove it from the rack. See "Rack-mount installation" on page 21.
6. Put the new 3534 Managed Hub into position. See "Desktop installation" on page 21 or "Rack-mount installation" on page 21.
7. Insert the GBIC into port 7. See "Installing the GBIC" on page 25.

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)

8. Attach the power cord and plug it into the electrical outlet.
9. Go to "Verifying a repair that required 3534 Managed Hub replacement" on page 98. Be sure to set the IP address *before* connecting the Ethernet cable as described in "Setting the IP address" on page 26.

Replacing a GBIC module

The GBIC module is installed and removed by sliding it into the system board from the front of the unit. SNMP traps are generated upon GBIC insertion and removal.

Removing a GBIC module

Figure 26 shows an IBM GBIC. Pull down the metal swing bar on the front of the GBIC and pull it out. Carefully move the GBIC from side to side to unseat it. (You may find that the removal of the GBIC module requires more force than on other units.)

Figure 26. IBM GBIC module

Installing a GBIC module

Attention: The GBIC module is keyed so that it can be inserted in only one way. Do not forcibly insert the module if it does not slide in easily.

1. Insert the GBIC module into the port until the connector is firmly seated into port 7. The latch prongs will lock and prevent accidental removal of the GBIC.
2. Go to “Verifying FRU repair” on page 97.

Verifying FRU repair

You can replace a GBIC without removing power from the 3534 Managed Hub or disrupting operations. Use the following procedures to verify that a FRU is functioning properly.

Verifying a repair that did not require 3534 Managed Hub shut down

Perform the following procedure for a FRU that did not require shut down:

1. Reinstall the functional GBIC that you removed.
2. Verify that the 3534 Managed Hub ready LED is on.
3. Plug the appropriate wrap connector (black for shortwave and grey for longwave) into the GBIC. Verify that the port 7 LED blinks a slow green (every 2 seconds).
4. Reconnect any other cables you might have removed.
5. If the 3534 Managed Hub passes all checks, return the 3534 Managed Hub to the customer. If any check fails, go to "Problem determination" on page 85.

Verifying a repair that required 3534 Managed Hub replacement

This procedure is performed after replacing the 3534 Managed Hub. However, you can use this verification procedure any time that a 3534 Managed Hub is shut down and the entire 3534 Managed Hub function needs to be checked.

Attention: Do not install the Ethernet cable until reviewing Step 11.

1. Disconnect any cables that you installed, except the power cord.
2. Connect the power cord to 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)

3. Plug the unit into the electrical outlet.
4. Verify that the associated ready LED is on.
5. Wait 2 minutes while POST diagnostics run.
6. Verify that the 3534 Managed Hub ready LED is on.
7. Install a GBIC in port 7, if applicable.
8. Plug the appropriate wrap connector (black for ports 0 - 6; black for port 7 shortwave and grey for port 7 longwave) into each port. Verify that each associated port LED blinks slow green (every 2 seconds).
9. If any of the checks fail, go to "Problem determination" on page 85.
10. Reinstall all cables except the Ethernet cable (the cable that attaches in the RJ-45 connector).
11. If you replaced the 3534 Managed Hub, you need to set the 3534 Managed Hub IP address. To do this, see "Setting the IP address" on page 26. The 3534 Managed Hubs are shipped with the IP address

set to 10.77.77.77. The address on the label in the upper left corner of the 3534 Managed Hub might or might not have been used by the customer. Determine from the customer LAN administrator what the IP address settings should be before setting the IP address. After setting the IP address, return the 3534 Managed Hub to the customer.

Note: If this unit was cascaded to an IBM 2109 Fibre Switch or to another IBM 3534 Managed Hub, the configuration information is automatically refreshed from the connected unit. Otherwise, inform the customer that any configuration information needs to be re-entered.

12. If you did not replace the 3534 Managed Hub, install the Ethernet cable and return the 3534 Managed Hub to the customer.

Appendix A. 3534 Managed Hub specifications

Appendix A provides the specification information for the 3534 Managed Hub.

Attention: Throughout this guide, the term *switch* refers to switches and hubs unless otherwise noted.

General Specifications

Table 21 shows the general specifications for the 3534 Managed Hub.

Table 21. General specifications

Specifications	Description
ANSI fibre-channel protocol	Fibre-channel ANSI standard (FC-PH)
Fabric initialization	Complies with FC-SW 3.2
IP over fibre channel (FC-IP)	Complies with 2.3 of the FCA profile
System architecture	Nonblocking shared-memory loop switch
System processor	Superscalar 33 MHz Intel® i960RP
Number of fibre-channel ports	Seven fixed SW FC ports and one GBIC port
Fibre-channel port speed	1.0625 Gbps full duplex
Modes of operation	Fibre-channel class 2 service and fibre-channel class 3 connectionless service
Aggregate switch I/O bandwidth	8 Gbps full duplex
Frame buffers	16 buffers per port at 2112 bytes per frame
Fabric latency	<2 microseconds with no contention
Data transmission range	Up to 500 m (1625 ft) for SWL optical link Up to 10 km (32 808 ft.) for LWL optical link
Chassis types	Back-to-front airflow

Table 22 shows fabric management standard features.

Table 22. Fabric management standard features

Standard features	Description
Fabric management	Simple name server, alias server, SNMP, Telnet, WWW
User interface	RJ-45 front panel connector for 10BASE-T or 100BASE-T Ethernet or in-band
Serial port	Local front panel RS-232 port for recovering factory settings

Optical port specifications

Fibre-channel interfaces of a 3534 Managed Hub system equipped with an optical port interface use a short wavelength (780 - 850 nm) or long wavelength (1270 - 1350 nm) laser transmitter. The laser complies with 21 CFR(J) class 1 laser safety requirements. It uses non-open fibre control (OFC) optical GBICs in the switch circuit. Safe class 1 operation is guaranteed by limiting the optical power emitted by the port, thereby eliminating the need for physical shutters. The optical GBIC uses the duplex-SC connector scheme.

Environmental specifications

The primary operating environments for the 3534 Managed Hub are server rooms, network equipment closets, and offices. The acceptable environmental ranges for a 3534 Managed Hub are shown in Table 23

Table 23. 3534 Managed Hub environmental specification

Specification	**Value**
Temperature (operating)	10°C - 40°C (40°F – 104°F)
Temperature (nonoperating)	35°C - 65°C (95°F – 149°F
Operating humidity	5% - 85% noncondensing at 40°C (104°F)
Nonoperating humidity	95% RH noncondensing at 40°C (104°F)
Operating altitude	0 - 3 km (0 - 9843 ft.) above sea level
Nonoperating altitude	0 - 12 km (0 - 393 ft.) above sea level
Operating shock	4 g, 11 Ms duration, half sine
Nonoperating shock	20 g, 11 MS duration, square wave
Operating vibration	5, 5-500-5 Hz at 1.0 octave per minute
Nonoperating vibration	10, 5-500-5 Hz at 1.0 octave per minute

Dimensions

This sections contains the physical dimensions for the 3534 Managed Hub.

The 3534 Managed can may be configured for either:

- Rack-mount with two rack-mount brackets
- Desktop with four rubber feet

Table 24. Rack-mount dimensions

Specification	Value
Height	43.4 mm (1.71 in.)
Width	428.6 mm (16.88 in.)
Depth	254.76 mm (10.03 in.) 1U, 19-inch rack mount (EIA compliant)
Weight	4.1 kg (9 lbs.)

Table 25. Desktop dimensions

Specification	Value
Height	43.4 mm (1.71 in.)
Width	428.6 mm (16.88 in.)
Depth	254.76 mm (10.03 in.)
Weight	4.1 kg (9 lbs.)

Power supply

The 3534 Managed Hub has a universal power supply that is capable of functioning world-wide without voltage jumpers or switches. The power supply is autoranging in terms of accommodating input voltages and line frequencies. The power supply is fully integrated into the unit.

Table 26. Power supply requirements

Specification	Value
Total power	75 watts
Input voltage	100 - 240 V ac
Input line frequency	47 - 63 Hz
Inrush current	10 amps peak, > 300 µs - hot or cold start
Harmonic distortion	Active power factor correction per IEC1000-3-2
Input line protection	Fused
BTU rating	110 W X 3.412 BTU/hr/W = 375 BTU/hr

Appendix B. Diagnostics

Appendix B provides diagnostic information for the 3534 Managed Hub.

Attention: Throughout this guide, the term *switch* refers to switches and hubs unless otherwise noted.

General information

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 aid in isolating any equipment or fabric failures.

The 3534 Managed Hub supports power-on self-tests (POSTs) and diagnostic tests. The diagnostic tests determine the status of the 3534 Managed Hub and isolate problems.

Telnet commands are used to determine the status of 3534 Managed Hub, error conditions, and 3534 Managed Hub operating statistics. A Telnet session can be established from the IBM StorWatch Specialist. The same Telnet commands can also be issued using the service terminal connected to the serial port.

Attention: Many of the diagnostic tests are disruptive to 3534 Managed Hub operation. Read the information on each diagnostic before beginning a test or procedure.

Isolating a system fault

Various loopback paths are built into the 3534 Managed Hub hardware for diagnostic purposes. A loopback path test within the 3534 Managed Hub verifies the proper internal fibre-channel port logic functions and the paths between the interfaces and central memory.

Diagnostics also support external loops that include the system board and the GBIC module in cross-port configurations. These port-to-port diagnostics allow you to check installed fiber cables and perform port fault isolation.

Removing power

After all data transferring processes that are external to the 3534 Managed Hub are completed, removing power from the 3534 Managed Hub does not disrupt the fabric.

Note: Error messages are stored in random access memory (RAM) and are lost when power is removed from the 3534 Managed Hub. Access the error message log and note any error messages before removing power from the 3534 Managed Hub.

Service actions for error messages

See Table 31, “Diagnostic error messages,” on page 146 and Table 32, “System error messages,” on page 149. Then refer to Table 30, “Action codes and the recommended action,” on page 145 for the appropriate service action for each message.

Running diagnostics on the 3534 Managed Hub

There are three methods to access the 3534 Managed Hub for running diagnostics. All methods use the Telnet commands and differ only in the initial login requirement and the access level given to the user.

Attaching to the serial port while the 3534 Managed Hub is off

If you can attach your service terminal to the 3534 Managed Hub before turning it on, you are automatically logged on as the admin ID and can issue all diagnostic commands. You can watch the progress of the POST diagnostics as they are posted to your service terminal.

1. Attach your service terminal to the serial port on the front of the 3534 Managed Hub and start a terminal emulation session on your service terminal.
2. Start the 3534 Managed Hub by plugging the power cord into an electrical outlet.
3. As the 3534 Managed Hub runs POST, you will see the results posted.
4. When the 3534 Managed Hub has completed POST, you are logged on as admin. The 3534 Managed Hub leaves the terminal session open. Press Enter. The 3534 Managed Hub responds with:

   ```
   Admin>
   ```

5. You can perform any of the diagnostics described in this section by typing the appropriate command. The 3534 Managed Hub shows the results as the diagnostic progresses.

Attaching to the serial port while the 3534 Managed Hub is on

If the 3534 Managed Hub is on, you can attach your service terminal, log in, and run most diagnostics.

1. Use an admin username and password that is recognized by the 3534 Managed Hub from the system administrator.
2. After you get an admin username, stop any Ethernet session that is active on the Ethernet port.
3. Attach your service terminal to the serial port on the 3534 Managed Hub. The Ethernet port and the serial port are mutually exclusive.
4. On your service port, type:

   ```
   Login username
   ```

5. Type in your password. The password does not display as you type it in.

   ```
   Password:
   ```

You can now type any diagnostic command and observe the results as they are posted to your service terminal.

Running diagnostics from a Telnet session on the Ethernet

The easiest way to run diagnostics is through a LAN-attached server that can access the 3534 Managed Hub Ethernet port.

You need to get an admin level username and password from the system administrator, as well as the 3534 Managed Hub IP address or name.

When you have the IP address, admin level username, and password, perform the following steps:

1. Go to the server that has LAN access and, in an open window, type:

   ```
   Telnet IPaddress or name
   ```

   where the Telnet IPaddress is the 3534 Managed Hub IP address or the name is the 3534 Managed Hub name.

2. The 3534 Managed Hub responds:

   ```
   Type the username you were given and press Enter.
   ```

3. The 3534 Managed Hub responds:

   ```
   IPaddress password
   ```

You can now run any of the diagnostics and observe the results as the 3534 Managed Hub displays them in your Telnet session.

Power-on self tests

Table 27 lists the diagnostic tests that are run automatically during POST.

Table 27. POST

Test	Description
Memory test	Checks CPU RAM memory.
Port register test	Checks the ASIC registers and SRAMs.
Central memory test	Checks the system board SRAMs.
CMI conn test	Checks the CMI bus between ASICs.
CAM test	Checks the CAM.
Port loopback test	Checks all of the 3534 Managed Hub hardware: frames are transmitted, looped back, and received.

POST runs differently depending on the startup method. A power cycle (disconnecting from power and reconnecting to power) is considered a cold start. All other starts from a powered-on state (such as restart or panic) are considered warm starts.

From a cold start condition, POST runs the long version of ramTest. From a warm start condition, POST runs a shorter version of the ramTest. The start time with POST varies depending on the startup method.

A 3534 Managed Hub that is restarted with POST disabled generates the `DIAG-POST_SKIPPED` error log message.

Diagnostic commands

All commands are case sensitive and must be entered exactly as shown.

These tests are available from the Telnet session or from the service terminal connected to the local serial port. The test name is followed by the command used to run the test.

- .3534 Managed 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)**

Simultaneously press Ctrl+C and Enter to end, continue, view stats, or log test results. When you press Ctrl+C and Enter, you receive the message:

```
Diags: (Q)uit, (C)ontinue, (S)tats, (L)og
```

- Enter `Q` to end the diagnostic test.
- Enter `C` to continue testing.
- Enter `S` to view statistics.
- Enter `L` to save results.

Attention: All offline diagnostic tests are disruptive to 3534 Managed Hub operations. Before attempting these diagnostic tests or procedures, make sure that the entire 3534 Managed Hub is available.

Note: See Table 31, “Diagnostic error messages,” on page 146 for the actual error message descriptions and the appropriate service actions.

Table 28 shows the available offline and online tests.

Table 28. Offline and online tests

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

ramTest

The **ramTest** command tests the bit write and read of the SRAMs in the switch.

Syntax

```
ramTest [patternSize]
```

Availability

Administrator

Description

Use this command to verify the address and data bus of the SRAMs that serve as the 16 MB CPU memory in the switch.

The test consists of two subtests:

1. The address subtest verifies that SRAM locations can be uniquely accessed.

   The method used is to write a unique pattern to each location in the SRAMs. 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 SRAMs are faulty, resulting in failures to program-unique values.

   Following is the ramp pattern used in the address subtest:

   0x57626f42, 0x57626f43, 0x57626f44, 0x57626f45, and so on.

2. The data subtest verifies that each cell in the SRAMs 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 running the test requires an operating system that 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.

Below 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), the **ramTest** command runs all nine 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 can be configured. 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

portRegTest

The **portRegTest** command performs the bit write and 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, that is, 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:

0x0001
0x0002
0x0004
0x0008
0x0010
0x0020
0x0040
0x0080
0x0100
0x0200
0x0400
0x0800
0x1000
0x2000
0x4000
10x8000

Repeat this procedure until all ASIC SRAMs and registers have been tested.

If failures are detected, the 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

centralMemoryTest

The **centralMemoryTest** command tests the bit write and 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 operands are omitted, the default values are used.

passCount
The number of times to run this test. The default is 1.

dataType
The data type to use when writing the central memory. The **dataTypeShow** command lists the data types allowed. The default value is QUAD_RAMP.

dataSeed
The initial seed value QUAD_RAMP pattern with a seed value of 0xdead is as follows: 0xdead, 0xdeae, 0xdeaf, 0xdeb0, and so on. The default is a random value run.

Example

```
sw7:admin> centralMemoryTest
Running Central Memory Test ... passed.
```

See also

camTest
cmemRetentionTest
cmiTest
crossPortTest
portLoopbackTest
portRegTest
ramTest
spinSilk
sramRetentionTest

cmiTest

The **cmiTest** command tests the connection of one ASIC to another 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 status bit in any ASIC.

The following is completed 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 CMI 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

camTest

The **camTest** command tests the function of the CAM memory.

Syntax

```
camTest [passCount]
```

Availability

Administrator

Description

Use this command to verify that the 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

portLoopbackTest

The **portLoopbackTest** command tests the function of the port N-to-N path.

Syntax

```
portLoopbackTest [passCount]
```

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.

Perform the following steps:

1. Set all ports for parallel loopback.
2. Create a frame F of the 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 eight 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 being 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

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 the data read matches the 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

```
sw7:admin> sramRetentionTest
Running SRAM Retention Test ... passed.
```

See also

camTest
centralMemoryTest
cmemRetentionTest
cmiTest
crossPortTest
portLoopbackTest
ramTest
spinSilk

cmemRetentionTest

The **cmemRetentionTest** command tests the data retention of the central memory SRAMs.

Syntax

```
cmemRetentionTest [passCount, dataType, dataSeed]]
```

Availability

Administrator

Description

Use this command to verify 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 operands. If all operands are omitted, the default values are used.

passCount
The number of times to run this test. The default is 1.

dataType
The data type to use when writing the central memory. The **dataTypeShow** command lists data types allowed. The default value is QUAD_RAMP.

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, ...The default is a random value.

Example

```
sw7:admin> centralMemoryTest
Running Central Memory Test ... passed.
```

See also

camTest
cmemRetentionTest
cmiTest
crossPortTest
portLoopbackTest
portRegTest
ramTest
spinSilk
sramRetentionTest

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 the transmitter of port M and looping the frames back through an external fiber cable into a 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 system 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 7 tests 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. Check if a port other than N receives the frame.

   ```
   ENC_in, CRC_err, TruncFrm, FrmTooLong, BadEOF,
   Enc_out, BadOrdSet, DiscC3
   ```

6. Check the transmit, receive, or class 3 receiver counters to see if they are stuck at some value.
7. Check that the number of frames received is equal to the number of frames transmitted.
8. Repeat steps 3 through 7 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 or switchDisable mode
- singlePortAlso mode
- GBIC mode

switchEnable or switchDisable mode

This mode can be run in one of two states, online or offline.

In the online state, the switch is enabled before running 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 mode is active) or two ports (if singlePortAlso mode is not active) must be cable loopbacked to each other. If this criteria is not met, one of the following messages is sent to the Telnet shell:

```
Need at least one port(s) connected to run this test.
(singlePortAlso active)
```

```
Need at least two port(s) cross-connected to run this test.
(singlePortAlso not active)
```

In the offline state, the switch is disabled before running 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 ends.

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.
```

singlePortAlso mode

Specify singlePortAlso mode by running 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 **setGbicMode** command before running the **crossPortTest** command.

```
sw:admin> setGbicMode 1
```

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 mode activated and limit the **crossPortTest** to only ports containing GBICs that are cable loopbacked to each other (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 execute this test. If omitted, the default value is 0xfffffffe.

singlePortAlso
Specify 1 to connect port N to itself (port N to port 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
```

See also

camTest
centralMemoryTest
cmemRetentionTest
cmiTest
portLoopbackTest
portRegTest
ramTest
spinSilk
sramRetentionTest

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 that are received by port M are retransmitted through port N, and frames that are received by port N are retransmitted through port M. Each port M sends four 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, 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. A connection from port 0 to port 7 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 the port connections.
2. Enable the 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 four frames of different lengths using port M. Below are the four 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 four 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 is active.
   - The frames transmitted counter is incrementing.
   - The following statistic error counters are nonzero.

     `ENC_in, CRC_err, TruncFrm, FrmTooLong, BadEOF, Enc_out, BadOrdSet, DiscC3`

     until one of the following condition 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 end the test.

In this test, data is not read and checked, and the only CPU intervention is the 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 an active GBIC mode, only ports that contain 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 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 **spinSilk** command to limit testing to those ports that contain GBICs 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

The **spinSilk** command has the optional operand nMillionFrames. Specify the number of million frames per port to run this test. If the operand is omitted, the default passCountvalue is 0xfffffffe.

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: w 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
```

```
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.
Diagnostics Status: Tue Apr 6 04:10:12 1999
port#: 0 1 2 3 4 5 6 7
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
```

See also

camTest
centralMemoryTest
cmemRetentionTest
cmiTest
crossPortTest
portLoopbackTest
portRegTest
ramTest
sramRetentionTest

diagClearError

The **diagClearError** command clears the diagnostic software flag to allow for retest.

Syntax

```
diagClearError [port]
```

Availability

Administrator

Description

Use this command to clear the diagnostic software flag that indicates whether a port is bad or OK. The current flag settings are displayed by using the **diagShow** 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 that has cleared. For example:

```
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 diagnostic 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 running POST at restart.

Syntax

```
diagDisablePost
```

Availability

Administrator

Description

Use this command to disable running power-on self-test (POST) when the switch is restarted. This mode is saved in flash memory and POST remains disabled until it is enabled using the **diagEnablePost** command.

A switch that is 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
```

The POST includes the following tests:

ramTest
: Bit write and read test of SRAMS in the switch.

portRegTest
: Bit write and read test of the ASIC SRAMs and registers.

centralMemoryTest
: Bit write and 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 the 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 version of **ramTest** while the warm restart (software reset) runs the short version of **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 running POST at the next restart.

Syntax

```
diagEnablePost
```

Availability

Administrator

Description

Use this command to enable running power-on self-test (POST) at the next switch restart. This mode is saved in flash memory and POST remains enabled until it is disabled using the **diagDisablePost** command.

The POST includes the following tests:

ramTest
Bit write and read test of SRAMS in the switch.

portRegTest
Bit write and read test of the ASIC SRAMs and registers.

centralMemoryTest
Bit write and 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 the 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 version of **ramTest** while the warm startup (software reset) runs the short version of **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

diagShow

The **diagShow** command prints the diagnostic results 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:

- The 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`.
- The current state of ports. Active ports are marked `UP` and inactive ports are marked `DN`.
- The 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 eight statistic error counters: `ENC_in, CRC_err, TruncFrm, FrmTooLong, BadEOF, Enc_out, BadOrdSet, DiscC3`
- The state of central memory based on the results of diagnostics that were run since the last restart. The state is marked `OK` if the previous **centralMemoryTest** passed; `FAULTY` if the switch failed the **centralMemoryTest**.
- The number of total diagnostic frames that were 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, the **diagShow** command indicates the total as 0.)

  The transmitted and received values might not always be the same; for example, they might not be the same if an error occurred in one of the ports during one of the above tests.

The **diagShow** command can also be run using the s (stats) option of the QCSL diag prompt, which is generated when a diagnostic test is keyboard-interrupted.

The command 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 the **diagShow** command every four seconds unless stopped by a keyboard interrupt.

You can also use this command to isolate a bad GBIC. A changing LLI_errs value prefixed by two asterisks in quotation marks, “**”, 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 **diagShow** commands. 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
diags: OK OK OK OK OK OK OK OK
state: 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
```

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 that mode until another **setGbicMode** command is issued.

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** command and the **spinSilk** command 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

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 following commands in the order shown:

version
tempShow
psShow
licenseShow
diagShow
errDump
switchShow
portFlagsShow
portErrShow
mqShow
portSemShow
portShow
portRegShow
portRouteShow
fabricShow
topologyShow
qlShow
nsShow
nsAllShow
cfgShow
configShow
faultShow
traceShow
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 the state of port 0. If only firstPort is specified, only information for firstPort is printed.

lastPort Specify the last port, of a 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 specified, 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
...
```

Diagnostic error messages

If any port fails during a diagnostic test, it is marked BAD in the status display.

To retest a port that has been marked BAD, use the **diagClearError** (port#) command to clear the port and set its status to OK. This command clears the port status only and does not clear the logs or change the condition of the port. The **diagClearError** (port#) command should only be used during diagnostic procedures to reset a bad port for retest.

Some error messages contain the following abbreviations:

sb = Should be

er = Bits in error

Note: If you run the **portStatsShow** command or the **diagShow** command before running a test, errors might be displayed as a result of the normal synchronization process. These errors should be addressed if the number of errors found increases when running the **portStatsShow** command again.

Table 29 lists the probable test failures and the corresponding action codes. For the recommended repair action that corresponds to the action code, see Table 30.

Table 29. Probable failure actions

Failed test	Action code
ramTest	1
portRegTest	1
centralMemoryTest	1
cmiTest	1
cmemRetentionTest	1
sramRetentionTest	1
camTest	1
portLoopbackTest	1
crossPortTest	2
spinSilk	2

Table 30 shows the action codes and the recommended repair action for each action code. For the failed test that corresponds to the action code, see Table 29.

Table 30. Action codes and the recommended action

Action code	Recommended action
1	Replace the 3534 Managed Hub.
2	Further diagnostic action is required. The failure can be a GBIC, imbedded optic, cable, or system board. This error is typically the result of running a wrap test. The tests should be run again after swapping cables and GBICs to determine the cause. To help determine if the failure is a GBIC, imbedded optic, or cable, see "Chapter 6. Service procedures" on page 85. It is unlikely that the system board is at fault, as most system board failures cause a POST failure.
3	Replace the 3534 Managed Hub.
4	Replace the 3534 Managed Hub.

Error message number

An error number (ERR#xxxx) is at the end of an error message. Table 31 matches each error number with the test that caused the error and the name of the error. The table also shows the error description, probable cause, and the action code. See Table 30 for the recommended action.

Error message tables

Table 31. Diagnostic error messages

Message	Description	Probable cause	Action Code
DIAG-BADINT Err#1030, 2030 [centralMemoryTest, cmiTest]	The port received an unexpected interrupt.	ASIC failure	1
DIAG-BUS_TIMEOUT Err#0BoF, 4040F [portRegTest, sramRetentionTest]	The ASIC register or the ASIC SRAM did not respond to an ASIC data access.	ASIC failure	1
DIAG-CAMSID Err#223C [camTest]	The ASIC failed the SID NO translation test.	ASIC failure	1
DIAG-CLEAR_ERR Err#0001	The port diagnostic error flag (OK or BAD) is cleared.	Informational only	None required
DIAG-CMBISRF Err#1021 [centralMemoryTest]	The ASIC's central memory SRAMs did not complete the BISR within the time-out period.	ASIC failure	1
DIAG-CMBISRTO Err#1020 [centralMemoryTest]	The ASIC's central memory SRAMs did not complete the BISR within the time-out period.	ASIC failure	1
DIAG-CMERRPTN Err#102B [centralMemoryTest]	An error was detected at the wrong port.	ASIC failure	1
DIAG-CMERRTYPE Err#102A [centralMemoryTest]	The port received the wrong CMEM error type.	ASIC failure	1
DIAG-CMICKSUM Err#2036 [cmiTest]	The CMI message that was received failed bad checksum test.	ASIC or system board failure	1
DIAG-CMIDATA Err#2035 [cmiTest]	The CMI data that was received did not match the data that was transmitted.	ASIC or system board failure	1
DIAG-CMIINVCAP Err#2034 [cmiTest]	An unintended ASIC erroneously received the CMI capture flag.	ASIC or system board failure	1
DIAG-CMINOCAP Err#2033 [cmiTest]	The CMI intended receiver ASIC failed to receive the CMI capture flag.	ASIC or system board failure	2

Table 31. Diagnostic error messages (continued)

Message	Description	Probable cause	Action Code
DIAG-CMISA1 Err#2032 [cmiTest]	An attempt to send a CMI message from ASIC to ASIC failed.	ASIC failure	1
DIAG-CMNOBUF Err#1029 [centralMemoryTest]	The port could not get any buffer.	ASIC failure	1
DIAG-DATA Err#266E, 306E [portLoopbackTest, crossPortTest]	The payload that was received by the port did not match the payload that was transmitted.	System board, GBIC module, imbedded optic or fiber cable failure	1
DIAG-ERRSTAT Err#2640-2647, 3040-3047, 3840-3847 [portLoopbackTest, crossPortTest, spinSilk]	The port error statistics counter is non-zero, meaning an error was detected when receiving frames. One of the following status errors occurred. • Enc_in – Encoding error, inside frame • CRC_err – Cyclic redundancy check on frame failed • TruncFrm – Truncated frame • FrmTooLong – Frame too long • BadEOF – Bad end of file • Enc_out – Encoding error, outside frame • BadOrdSet – Bad symbol on fiber-optic cable • DiscC3 – Discarded class 3 frames	ASIC, system board, GBIC module, imbedded optic or fiber cable failure	
DIAG-INIT Err#264F, 304F, 384F [portLoopbackTest, crossPortTest, spinSilk]	The port failed to go active in the loopback mode requested.	ASIC, system board, GBIC module, imbedded optic or fiber cable failure	1
DIAG-INTNIL Err#2031 [cmiTest]	ASIC failed to get a CMI error (interrupt).	ASIC failure	1
DIAG-INTNOTCLR Err#102C [centralMemoryTest]	The interrupt bit could not be cleared.	ASIC failure	1
DIAG-LCMEM Err#1027 [centralMemoryTest, cmemRetentionTest]	The data read from the central memory location did not match the data that was previously written into the same location.	ASIC failure	1

Table 31. Diagnostic error messages (continued)

Message	Description	Probable cause	Action Code
DIAG-LCMEMTX Err#1F27, 1028 [centralMemoryTest]	Central memory transmit path failure: ASIC 1 failed to read ASIC 2 using the transmit path.	System board failure	1
DIAG-LCMRS Err#1F25, 1025 [centralMemoryTest, cmemRetentionTest]	Central memory read short: *M* bytes requested but got less than *M* bytes.	ASIC failure	1
DIAG-LCMTO Err#1F26, 1026 [centralMemoryTest, cmemRetentionTest]	Central memory timeout: Data transfer initiated did not complete within the timeout period.	ASIC failure	1
DIAG-MEMNULL Err#0112 [ramTest]	Test failed to malloc.	System board failure	1
DIAG-MEMSZ Err#0111 [ramTest]	Memory size to be tested is less than or equal to zero.	System board failure	1
DIAG-MEMORY Err#0110 [ramTest]	Data read from RAM location did not match data that was previously written into the same location.	CPU RAM failure	1
DIAG-PORTABSENT Err#2670, 3070, 3870 [portLoopbackTest, crossPortTest, spinSilk]	The port is not present.	ASIC or system board failure	1
DIAG-PORTDIED Err#265F, 305F, 385F [portLoopbackTest, crossPortTest, spinSilk]	The port was in loopback mode and then went inactive.	ASIC, GBIC module, imbedded optic or fiber cable failure	2
DIAG-PORTSTOPPED Err#3874 [spinSilk]	The port is no longer transmitting, as indicated by the number of frames transmitted counter being stuck at *N* frames.	ASIC, GBIC module, imbedded optic or fiber cable failure	2
DIAG-PORTWRONG Err#3078 [crossPortTest]	Frame erroneously received by port *M* instead of the intended port *N*.	ASIC failure	1
DIAG-POST_SKIPPED Err# 0004 [managed hub initialization]	POST is skipped. The message recommended that POST be run.	Informational only	None required

Table 31. Diagnostic error messages (continued)

Message	Description	Probable cause	Action Code
DIAG-REGERR Err#0B15, 0415 [portRegTest, sramRetentionTest]	Data read from ASIC register or ASIC SRAM did not match data that was previously written into same location.	ASIC failure	1
DIAG-REGERR_UNRST Err#0B16, 0416 [portRegTest, sramRetentionTest]	The port failed to unreset.	ASIC failure	1
DIAG-STATS Err#2660 - 2662, 3060 - 3062 [portLoopback Test, crossPortTest]	The port counter value did not match the number of frames actually transmitted. Possible counters reporting: • FramesTx - number of frames transmitted • FramesRx - number of frames received • Cl3FrmRx - number of class 3 frames received	ASIC, GBIC module, imbedded optic or fiber cable failure	2
DIAG-TIMEOUT Err#266F, 306F, 386F [portLoopbackTest, crossPortTest, centralMemoryTest]	For portLoopbackTest and crossPortTest: The port failed to receive the frame within the time-out period For centralMemoryTest: The port failed to detect an interrupt within the time-out period.	ASIC, GBIC module, imbedded optic or fiber cable failure	2
DIAG-XMIT Err#2271, 2671, 3071, 3871 [portLoopbackTest, crossPortTest, spinSilk, camTest]	The port failed to transmit the frame.	ASIC failure	1

Table 32 shows the system error messages, their description, and probable cause.

Table 32. System error messages

Message	Description	Probable Cause	Action
TEMP, 4_FAILED, LOG_CRITICAL	Managed Hub overheated	Fan failure	3
TEMP, 5_FAILED, LOG_CRITICAL	Managed Hub overheated	Fan failure	3
FANS, 1_FAILED, LOG_WARNING	Managed Hub overheated	Fan failure	3
FANS, 2_FAILED, LOG_ERROR	Managed Hub overheated	Fan failure	3
FANS, 3_FAILED, LOG_CRITICAL	Managed Hub overheated	Fan failure	3
FANS, 4_FAILED, LOG_CRITICAL	Managed Hub overheated	Fan failure	3
FANS, 5_FAILED, LOG_CRITICAL	Managed Hub overheated	Fan failure	3

Table 32. System error messages (continued)

Message	Description	Probable Cause	Action
FANS, 6_FAILED, LOG_CRITICAL	Managed Hub overheated	Fan failure	3
POWER, 1_FAILED, LOG_CRITICAL	Managed Hub power failure	Power supply failure	4

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 on 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, N.Y. 10504–1785
U.S.A.

The following paragraph does not apply to the United Kingdom or any other 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 WARRANTIES 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.

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

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

- IBM
- IBM 3534 Managed Hub
- StorWatch
- Netfinity.

Intel is a registered trademark of the Intel corporation in the United States, other countries, or both.

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 companies, product, and 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 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。

Korean Government Ministry of Communication (MOC) statement

Please note that this device has been approved for business purposes with regard to electromagnetic interference. If you find this is not suitable for your use, you may exchange it for one with a non-business purpose.

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

This glossary provides definitions for terminology used in the IBM 3534 Fibre Channel Managed Hub.

AL_PA. Arbitrated loop physical address.

alias server. A fabric software facility that supports multicast group management.

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/output system.

BISR. Built-in self-repair

CAM. Content addressable memory.

class 2. The fabric and destination N_port provide connectionless service with notification of delivery or nondelivery between the two N_ports.

class 3. 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 messages interface.

community (SNMP). A relationship between an SNMP agent and a set of SNMP managers that defines authentication, access control, and proxy characteristics.

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 may transmit frames without over-running the F_port or NL_port.

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.

E_D_TOV. See *error detect time out value.*

E_port. A port is designated an E_port when it is used as an interswitch expansion port to connect to the E_port of another switch to build a larger switch fabric.

ELP. Extended link parameters.

ESD. Electrostatic discharge

error detect time-out value. Defines the time that 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.

F_port. The fabric access port used to connect an N_port.

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.

FCAL. Fiber-channel arbitrated loop.

FC. Fibre channel

FCP. Fibre channel protocol.

FL_port. The FL_port is the fabric access port used to connect NL_ports to the switch in a loop configuration.

FRU. Field replaceable units

FSPF. Fibre channel shortest path first.

G_port. 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.

gateway. Hardware that connects incompatible networks by providing the necessary translation, both for hardware and software.

GBIC. Gigabit interface converter

HBA. Host bus adapter.

interswitch link (ISL). A fiber 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.

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.

LWL. Long wavelength.

MIB. Management information base.

multicast. Multicast is used when multiple copies of data are to be sent to designated multiple destinations.

N_port. The designation of an equipment port connected to the fabric.

NL_port. The designation of an equipment port connected to the fabric in a loop configuration using an FL_port.

NIS. Network information service

OS. Operating system.

PLDA. Private loop direct attach.

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.

R_A_TOV. See *resource allocation time out 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.

SID. (1)Source identification. (2) Single image data.

SWL. Short wavelength

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. Since SNMP does not rely on the underlying communication protocols, it can be made available over other protocols, such as UDP/IP.

SNMP.*S*ee *simple network management protocol.*

SNMPv1. The original standard for SNMP is now referred to as SNMPv1.

SNS. Simple name server.

SRAM. Static RAM.

trap (SNMP). A mechanism for SNMP agents to notify the SNMP management station of significant events.

tunneling. (1) A technique for making two different networks interwork where the source and destination hosts are on the same type of network, but there is a different network in between. (2) To treat a transport network as though it were a single communication link or LAN.

UDP. User datagram protocol.

unicast. (1) Unicast routing provides one or more optimal paths between any two switches that make up the fabric. This is for a single copy of the data to be sent to designated destinations. (2) Transmission of data to a single destination.

WAN. Wide area network.

World-wide name (WWN). A unique name for a switch on local and global networks.

WWN. See *world-wide name*.

Index

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

W

Z

Readers' comments—we would like to hear from you

IBM 3534 SAN Fibre Channel Managed Hub
Installation and Service Guide

Publication No. SY27-7616-01

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
SY27-7616-01

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 95193-0001
U.S.A.

Fold and Tape **Please do not staple** Fold and Tape

SY27-7616-01

Cut or Fold
Along Line

Part Number: 19P3123

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

(1P) P/N: 19P3123

SY27-7616-01

Spine information:

IBM 3534 SAN Fibre Channel
Managed Hub

Installation and Service Guide