IBM TotalStorage™ SAN Fibre Channel Switch

3534 Model F08 User's Guide

Read Before Using

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

GC26-7454-00

IBM TotalStorage™ SAN Fibre Channel Switch

3534 Model F08 User's Guide

GC26-7454-00

Note:
Before using this information and the product it supports, read the general information under “Notices” on page 285.

First Edition (May 2002)

Contents

Figures

Tables

Safety and environmental notices

This section contains information about:

- Safety notices used in this book
- Safety inspection for this product
- Environmental guidelines for this product

Safety notices and their translations

Safety notices are printed in English throughout this book.

- A *Danger* notice warns you of conditions or procedures that can result in death or severe personal injury.
- A *Caution* notice warns you of conditions or procedures that can cause personal injury that is neither lethal nor extremely hazardous.
- An *Attention* notice warns you of conditions or procedures that can cause damage to machines, equipment, or programs.

For translations of danger and caution notices, see *IBM TotalStorage SAN Fibre Channel Switch 3534 Model F08 Translated Safety Notices*, GC26-7459-00. The notices are listed in numeric order based on their IDs, which are displayed in parentheses at the end of each notice. See the following examples for the location of the ID numbers.

DANGER

An electrical outlet that is not correctly wired could place a 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. (1)

CAUTION:
The 3534 Model F08 switch is designed to be installed by the customer, and is certified as ″customer setup″. Make sure that the system or rack into which the switch will be installed is also designed and certified for customer setup; if it is not, then the switch must be installed by a CE. (1)

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.

CAUTION:
The 3534 Model F08 switch is designed to be installed by the customer, and is certified as ″customer setup″. Make sure that the system or rack into which the switch will be installed is also designed and certified for customer setup; if it is not, then the switch must be installed by a CE. (1)

Checking the machine

Perform the following external machine checks:

1. Verify that all external covers are present and are not damaged.

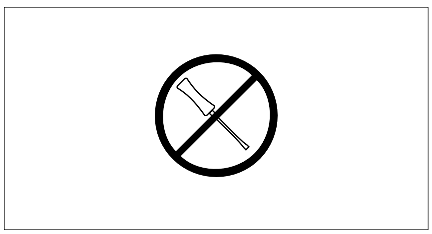
2. Ensure that all latches and hinges are in correct operating condition.
3. If the 3534 Model F08 is not installed in a rack cabinet, check for loose or broken feet.
4. Check the power cord for damage.
5. Check the external signal cable for damage.
6. Check the cover for sharp edges, damage, or alterations that expose the internal parts of the device.
7. Correct any problems that you find.

Checking the safety labels

Perform the following safety label checks:

1. Verify that the power supply cover caution label shown in Figure 1 is installed on the power supply of the 3534 Model F08.

   CAUTION:
   Do not remove cover, do not service, no serviceable parts. (2)



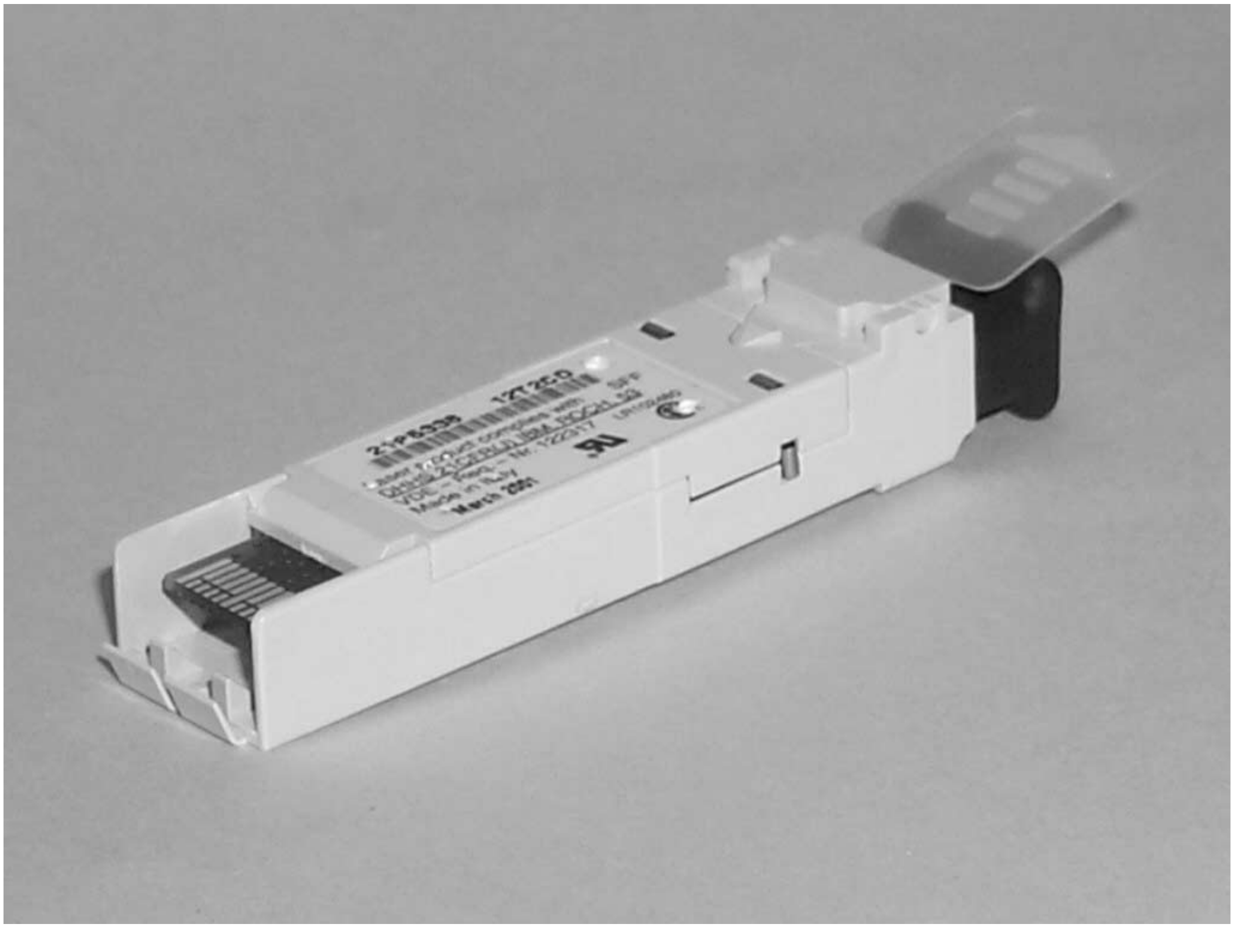
SJ000337

Figure 1. Power supply cover caution label

2. Verify that the small form-factor pluggable device (SFP) label shown in Figure 2 and Figure 3 on page xv is installed on the 3534 Model F08.

SJ000317

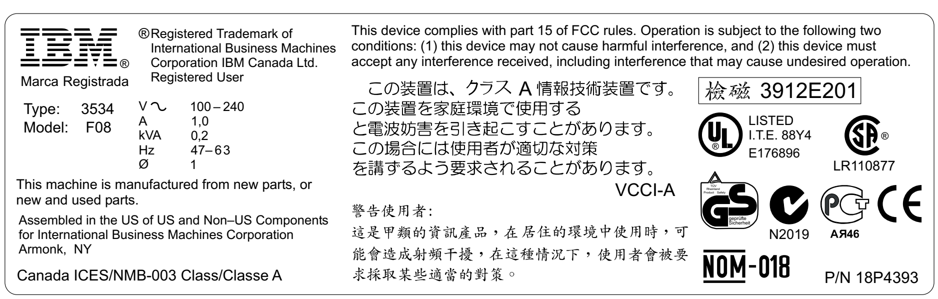
Figure 2. SFP label (front view)



SJ000314

Figure 3. SFP label (back view)

3. Verify that the safety label shown in Figure 4 is installed on the 3534 Model F08, and that the voltage specified on the label matches the voltage at the power source.



SJ000347

Figure 4. Safety label on the 3534 Model F08

Checking ac grounding

DANGER

An electrical outlet that is not correctly wired could place a hazardous voltage on the 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. (1)

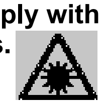
Environmental notices and statements

This section describes the environmental notices and statements.

Battery notice

CAUTION:
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 cell contents to water. Keep away from children. Replace only with the part number specified for your system. Use of another battery may 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. (3)

Laser safety

CAUTION:
In the United States use only GBIC units or Fibre-Optic products that comply with FDA radiation performance standards, 21 CFR Subchapter J. Internationally use only GBIC units or Fibre-Optic products that comply with IEC standard 825-1. Optical products that do not comply with these standards may produce light that is hazardous to the eyes.  **(4)**

SJ000338

This unit might contain a single-mode or a multimode transceiver Class 1 laser product. The transceiver complies with IEC 825-1 and FDA 21 CFR 1040.10 and 1040.11. The transceiver must be operated under the recommended operating conditions.

This equipment contains Class 1 laser products, and complies with FDA radiation Performance Standards, 21 CFR Subchapter J and the international laser safety standard IEC 825-2.

Usage restrictions

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

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.

Product disposal

This unit might contain batteries. Remove and discard these batteries, or recycle them, according to local regulations.

About this book

This publication introduces the IBM TotalStorage™ SAN Fibre Channel Switch 3534 Model F08 (hereafter referred to as the 3534 Model F08). It also provides an overview of the features of the switch and information about installing and using those features.

Who should read this book

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

Before using this publication you should know how to service the switch hardware, including how to analyze, isolate, report, and resolve problems. You must also know how to safely work with electrical components. Throughout this publication, the term *switch* applies to any IBM 3534 Model F08 switch, unless the reference is to a specific model.

Additional information

This section contains information about the 3534 Model F08 library, Web sites, and how to get help and software updates.

3534 Model F08 library

Information related to this product can be found in the following publications:

- *IBM TotalStorage SAN Fibre Channel Switch 3534 Model F08 Installation Guide*, SY27-7631
- *IBM TotalStorage SAN Fibre Channel Switch 3534 Model F08 User's Guide*, GC26-7454
- *IBM TotalStorage SAN Fibre Channel Switch 3534 Model F08 Command Reference*, GC26-7455
- *IBM TotalStorage SAN Fibre Channel Switch 3534 Model F08 Translated Safety Notices*, GC26-7459

Web sites

To get specific details about models and firmware that the switch supports, see the following Web site:

www.ibm.com/storage/fcswitch/

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

www.fibrechannel.com/

For a directory of worldwide contact information, including technical support, see the following Web site:

www.ibm.com/contact/

Getting help

Contact your switch supplier for technical support. This includes hardware and software support, all product repairs, and ordering of spare components.

Be prepared to provide the following information to the support personnel:

- The switch serial number
- The switch worldwide name
- The topology configuration
- Any output from the **supportShow** Telnet command
- A detailed description of the problem
- Any troubleshooting steps that have already been performed

Getting software updates

Contact your switch supplier for software updates and maintenance releases. New switch firmware can be installed from the following host operating systems:

- UNIX®
- Microsoft® Windows NT®
- Windows 98
- Windows 95

For utility programs to facilitate loading firmware, sample Fabric Watch configurations, and MIB files for switch management by SNMP, see the following Web site:

www.storage.ibm.com/ibmsan/products/sanfabric.htm

How to send your comments

Your feedback is important to help us provide the highest quality of information. If you have any comments about this book, you can submit them in one of the following ways:

- E-mail

  Submit your comments electronically to:

  starpubs@us.ibm.com

  Be sure to include the name and order number of the book and, if applicable, the specific location of the text that you are commenting on, such as a page number or table number.
- Mail or fax

  Fill out the Readers' Comments form (RCF) at the back of this book and return it by mail or fax (1-800-426-6209) or give it to an IBM representative. If the RCF has been removed, you may address your comments to:

  International Business Machines Corporation
  RCF Processing Department
  Dept. M86/Bldg. 050-3
  5600 Cottle Road
  San Jose, CA 95193-0001
  U.S.A.

Chapter 1. Introduction

This chapter describes the TotalStorage SAN Fibre Channel Switch 3534 Model F08, hereafter referred to as the 3534 Model F08. It provides the following information:

Product overview

Figure 5 shows the 3534 Model F08.

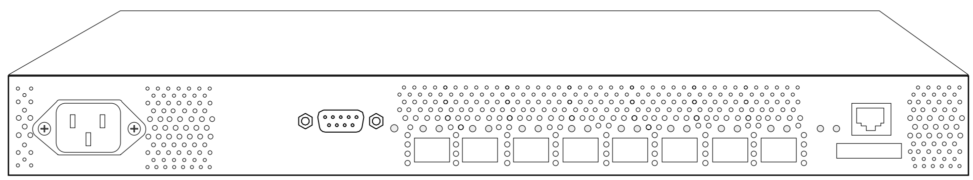


Figure 5. 3534 Model F08

The 3534 Model F08 is an 8-port, dual speed, auto-sensing fibre-channel switch, with one E_port. It is functionally compatible and interoperable with the current series of 2109 and 3534 switches. The 3534 Model F08 is an enterprise class switch that is designed to handle the large scale SAN requirements of an enterprise. You can use the 3534 Model F08 to address the SAN requirements of a small to medium-size workgroup. The 3534 Model F08 is a flexible switching platform that meets both low-latency and high-throughput demands. Based on Application Specific Integrated Circuit (ASIC) technology that is called the Bloom, the 3534 Model F08 provides high levels of reliability, availability, and port density.

The 3534 Model F08 provides the following:

- Nonblocking ports that provide full-duplex, throughput bandwidth at either 1.0625 Gbps or 2.125 Gbps.
- Fibre-channel autosensing ports that self-negotiate to the highest speed that the attached devices support.
- Universal ports that self-configure as F_ports or FL_ports.
- One port can be used as an E_port (the switch can be upgraded to eight E_port capability with an optional license).
- Trunking, which allows up to four ports to be grouped together to create high-performance 8 Gbps inter-switch links (ISLs) between switches.
- Hardware zoning that permits or denies delivery of frames to any particular destination port address.

- Frame filtering, which augments the hardware zoning capabilities of the second-generation ASIC. The second-generation ASIC implements hardware zoning at the port level of the switch. The expanded capabilities of the third-generation ASICs include the following: worldwide name (WWN), device-level zoning, protocol-level zoning, and logical unit number (LUN)-level zoning. Thus third-generation ASICs provide the flexibility of second-generation software zoning with the enhanced security of hardware zoning.

  Note: Fabric OS version 3.1 is required for protocol-level and LUN-level zoning support.
- Phantom loop addressing that allows private 8-bit loop addresses to be treated as equivalent to public loop addresses.
- Support for unicast, multicast (up to 256 groups), and broadcast data traffic types.
- Extensive diagnostics, system monitoring capabilities, and dual redundant, hot-swappable power supplies and cooling units that provide high reliability, availability, and serviceability.
- A single system board design with a 100 MHz 80960VH reduced instruction set computer (RISC) CPU with integrated peripherals that provide high performance.
- Small form factor pluggable (SFP) media that supports short wavelength (SWL) optical, and long wavelength (LWL) optical.
- An operating system (Fabric OS) that delivers distributed intelligence throughout the network and enables a wide range of applications.
- A flexible topology that allows up to 239 switches to be interconnected to create a medium to large fibre-channel fabric. The topology can change dynamically as new switches or links are added to the fabric or as your needs change.
- Central memory architecture that maximizes switch throughput and guarantees full transmit and receive bandwidth to all fibre-channel ports at all times. It also enables a number of sophisticated queuing, messaging, and buffer pool management schemes to optimize switch performance characteristics in heavily loaded systems.
- Cut-through frame routing that minimizes port-to-port latency.

Hardware components

The 3534 Model F08 system board is a single-board design with a highly integrated CPU. The Intel® 80960VH CPU is a RISC core processor and is the top choice for this platform. It provides over 70% of the functionality for the digital section of the system board. The system uses three types of memory devices: DRAM, Flash File, and Boot Flash. On the fibre-channel section of the system board, the following three components provide high-speed data transfer:

- The Bloom ASICs
- The Serializer/Deserializer (SERDES)
- The SFP media. SFP media interfaces support SWL and LWL.

CPU subsystem

An Intel 80960VH CPU is used for management functions and switch initialization. The CPU runs the Fabric OS and is responsible for switch initialization, configuration, and management. Switching functionality is provided by the ASIC.

The following peripherals are supported as well:

- An Ethernet port
- A serial port
- Three digital thermometers
- A real-time clock
- General I/O

The CPU subsystem is a mixed voltage system using 1.8 V, 2.5 V, 3.3 V, and 5 V depending on the device. The maximum board power consumption is 50 W.

Features

The 3534 Model F08 CPU subsystem includes the following:

- A 80960VH-100 MHz CPU
- An SDRAM controller with parity check at 33 MHz
- A peripheral control interconnect (PCI) bus arbiter
- Main Memory (SDRAM): 32 MB
- Flash Memory: Dual 8 MB
- Boot flash; 512 bytes of 8–bit for system start
- 10BASE-T or 100BASE-T port for management connection with RJ45 connector
- One RS232 port with DB9 connector
- Eight LEDs to indicate the status for each port
- Eight LEDs to indicate the link speed for each port
- One LED on the front panel to indicate the overall switch status
- One LED on the back panel to indicate the overall switch status
- Two LEDs for the Ethernet port to indicate port status and link speed information
- Three digital thermometers for temperature sensing
- One 3.3 V to 1.8 V dc/dc converter for Bloom ASIC core supply
- One Bloom ASIC supporting up to eight nonblocking ports
- Eight SERDES
- One real-time clock with a battery

Embedded processor

The embedded processor is an Intel 80960VH processor with a clock speed of 100 MHz. It contains the following:

- A high-performance RISC processor core (compatible with the 2109 and 3534 series of switches)
- An integrated EDO memory controller (for DRAM, SRAM, ROM, and Flash memory)
- A PCI bus interface
- A complex programmable logic device (CPLD) for SDRAM control
- Two direct memory access (DMA) channels
- An I2C interface
- General purpose I/O

You access system memory through the local bus. The external CPLD SDRAM device provides SDRAM controller functionality at 33 MHz. It supports parity checking to enhance the data integrity of the system. The CPU communicates with the ASIC and the 10BASE-T or 100BASE-T Ethernet media access controller (MAC) through the PCI interface. An external PCI bus arbiter enables the Ethernet device to be a bus master.

You can also access the RS232 Universal Asynchronous Receiver Transmitter (UART) serial port through the local bus. Other I/O peripherals, such as the real-time clock, the LEDs, the three digital thermometers, and miscellaneous I/O are handled by the I2C bus of the CPU. The CPU is the only I2C bus master in the system. The RS232 port and drivers, Ethernet MAC/PHY, and LEDs are external components to the CPU. An RJ45 connector provides Ethernet connection to external systems. The DB9 RS232 is a ribbon-cable connection through the on-board 10-pin header.

Bus operations

The interface between the embedded processor, the ASIC, and the 10BASE-T or 100BASE-T Ethernet MAC is implemented using a PCI bus. All PCI devices on the bus are PCI Revision 2.2 compliant. The PCI bus interface operates at 32-bit, up to 33 MHz and has a worldwide even parity bit. A slave-only PCI interface is provided by each ASIC to allow the processor to program various registers, routing tables, and so on within the chip. An external PCI bus arbiter enables the Ethernet device to be a bus master.

The local bus, a 32-bit multiplexed burst bus, provides the interface between the system memory and the I/O. Because the integrated EDO memory controller on the CPU allows only direct control for DRAM, SRAM, ROM, and Flash memory, the external CPLD controller is included to provide SDRAM controller functionality.

The I2C bus provides peripheral I/O control for the LEDs, the thermometers, and general I/O functions. The 80960VH CPU serves as the master on the I2C bus.

The Bloom ASIC is an eight-port fibre-channel switch controller. A proprietary 10-bit wide SSTL2 bus running at 106.25 MHz is used between the Bloom ASIC and the SERDES.

Memory

The system design uses three types of memory devices:

- DRAM
- Flash File
- Boot Flash

One on-board SDRAM chips provides up to 32 MB for system memory. One additional SDRAM chip provides data parity. The printed circuit board (PCB) SDRAM footprint is designed to be compatible with 64 MB, 128 MB, and 256 MB devices. An external CPLD device added to the local bus provides control functions for the 80960VH processor.

The system provides 4 MB of on-board redundant Flash File memory for software and data storage. The Boot Flash is an 8-bit Flash device socket that is used only for system start. The Boot Flash device contains a block area for startup code protection. The PLCC32 socket supports 3.3 V Boot Flash memory up to 512 KB.

Central memory: As with the 2019 series of switches and the 3534 1RU switch, the 3534 Model F08 is based on a central memory architecture. In this scheme, a set of buffers in the central memory is assigned to each port, to be used for receipt of frames. As an ASIC port receives and validates a frame, it stores the frame in one of its receive buffers in the central memory and forwards a routing request (a Put message) to the appropriate destination ports. When a destination port is capable of transmitting the frame, it reads the frame contents from central memory and forwards the frame to its transmit interface. It does not wait for the frame to be written in memory, unless the port is busy. After it has removed an entry for a frame from its internal transmit queue in preparation for transmitting a frame, the destination port sends a transmission complete message (a Finish message) to the port that received the frame. This allows the receiving port to reuse the buffer for subsequent frames received.

The central memory is also incorporated into the ASIC. Frames received on the ports in an ASIC are written into the portion of central memory.

The ASIC contains a RAM device plus data path crossbar logic that is used to implement the central memory. Memory blocks are accessed in a time-sliced fashion. The buffer pool can be split into 2112-byte buffers or into 312-byte mini-buffers. If frames that need to be buffered are smaller than the maximum 2112 bytes, using mini-buffers effectively expands the buffer pool and increases the efficiency of memory usage by providing more (but smaller) receive buffers.

Additionally, the Bloom ASIC provides a special memory interface (SMI). The SMI provides the firmware with a mechanism to read and write frame contents to and from the ASIC. It also supports higher throughput transfers. The SMI includes a set of two buffers that are large enough for an entire maximum-sized frame to be transferred in a single operation. Additionally, because there are two buffers available, the firmware can perform a read or write on a frame in one of the buffers while the ASIC streams another frame into the other buffer.

ASIC

The ASIC provides eight fibre-channel ports that can be used to connect to external N_ports (as an F_port), external loop devices (as an FL_port). One port may be connected (as an E_port) to connect to another 3534 or 2109 series switch. With the fabric upgrade you may have up to eight (E_ports). See “Terminology” on page 201 for definitions of each port.

Each port can operate at either 1.0625 Gbps or 2.125 Gbps link speeds. The ASIC contains the fibre-channel interface logic, message and buffer queuing logic, receive buffer memory for the eight on-chip ports, and other support logic.

The Bloom ASIC is a PCI slave to the CPU. The ASIC interfaces through an inter-chip 10-bit SSLT2 bus connection clocked at 106.25 MHz. An 8-channel SERDES is used to support eight ports. The interface between ASIC and SERDES is also a 10-bit SSTL2 bus running at 106.25 MHz. The SERDES converts the 10-bit wide parallel data from the SSTL2 bus into high-speed serial data for the SFP media and vice versa. The SERDES supports single data rate (SDR) or double data rate (DDR) transfer between the SERDES and the SFP media. Implementing the SERDES external to the ASIC reduces the risk of silicon packaging as well as the risk of running 2.125 Gbps signals on a board with a long trace length.

The SFP media interfaces wirh external devices and enables support for shortwave laser and longwave laser. Two LEDs for each port provide port status and link speed information.

Control Message Interface (CMI): The 3534 Model F08 Control Message Interface (CMI) consists of a set of control signals that are used to pass hardware-level messages between ports. Recipient ports use these control signals to inform transmitting ports when a new frame needs to be added to the output queue of the transmitter. Transmitting ports also use the CMI to inform recipient ports that a frame transmission has been completed. A recipient port is free to reuse a receive buffer when it receives notification that the frame has been transmitted. In the case of multicast, multiple notifications are required to determine when a receive buffer is freed.

The CMI interface for the ASIC is connected inside the ASIC. Each chip time slices its output port to each possible destination chip in the switch. If it has a message to send to a particular destination during the corresponding time slot, the chip uses the time slot to send the message. Otherwise, the output port lines are driven to indicate that no message is present.

Ports

The 3534 Model F08 supports the following port types:

- Optical ports
- Ethernet port
- Serial port

The ASIC in the 3534 Model F08 connects up to eight SFP media. SFP devices are encased in metal to ensure low emissions and high thermal management. They are hot-swappable and use industry-standard local channel connectors. Each port provides ISL, loop, and fabric (E, F, and FL respectively) type connectivity that the 3534 Model F08 senses automatically; it requires no administration to identify the port type.

Optical ports

For optical ports, the 3534 Model F08 uses SFP fiber-optic transceivers that convert electrical signals to optical signals (and optical signals to electrical signals). Capable of transmitting at both 1 and 2 Gbps speeds, each SFP fiber-optic transceiver supports 850 nm SWL on multimode fiber-optic cable or 1310 nm LWL on single-mode fiber-optic cable. These miniature optical transceivers provide high port density and deliver twice the port density of standard removable GBIC transceivers.

Ethernet port

The 3534 Model F08 provides a fully IEEE-compliant 10BASE-T or 100BASE-T Ethernet port for switch management console interface. When a device is connected to the port, both ends negotiate to determine the optimal speed. The Ethernet port uses an RJ45 connector. There are two LEDs for the port. One LED indicates transmit and receive activity and one LED indicates speed (10 Mbps or 100 Mbps). The TCP/IP address for the port can be configured from the serial port.

Serial port

An RS232 serial port is provided on the 3534 Model F08. The serial port uses a DB9 connector. The connector is a header pin block on the system board. The parameters of the serial port are fixed at 9600 baud, 8 data bits, no parity, no hardware flow control, 1 start and 1 stop bit.

You use this connector to configure the internet protocol (IP) address and to recover the factory default settings of the switch should Flash memory contents be lost. The serial port connection should not be used to perform normal administration or maintenance functions. Accessible functions are limited to connecting a terminal to the port to reinitialize the switch defaults, which restores the switch to its factory configuration. This is required to restore the switch passwords to a known state and to allow you to set a specific switch IP address.

Enclosure

The 3534 Model F08 enclosure is designed to be mounted in a 19-inch rack, with a height of 1 RETMA unit, but it can also be used in a tabletop configuration.

The 3534 Model F08 enclosure has forced-air cooling. The fans push the air from the rear chassis intake through the enclosure and exhaust the air through venting holes in the front panel. The SFP media is hot-swappable so that it can be removed and replaced without interrupting the system power.

Other than SFP replacement, there are no user serviceable parts on the 3534 Model F08.

On the front of the unit, there are two port connections (an RS232 connection and an RJ45 connection). The RJ45 connection provides a 10BASE-T or 100BASE-T Ethernet port for a full system management console interface. The RS232 connection provides a serial port interface for setting the IP address of the switch and for resetting the switch to factory defaults

The fibre-optic cables, Ethernet cables, AC power input cables and serial port cables are located on the front of the switch.

Power supply

The 3534 Model F08 power supply is universal and capable of functioning worldwide without using voltage jumpers or switches. It meets IEC 61000–4–5 surge voltage requirements and is auto-ranging in terms of accommodating input voltages and line frequencies.

The power supply meets the following requirements:

Specification	**Value**
Outlet	Correctly wired and earth-grounded
Maximum output	75 watts
Maximum system power consumption	50 watts
Input voltage	90 – 264 V ac
Input line frequency	47 – 63 Hz
Harmonic distortion	Active power factor correction per IEC1000-3-2
BTU rating	60 watts x 3.412 BTU/Hr/watts = 204.72 BTU/hr
Inrush current	40 Amps maximum, cold start at 25 celsius
Input line protection	Fused in hot line

LEDs

The 3534 Model F08 provides several LEDs to indicate status on the switch. Each of the eight ports has two status indicators. The first LED for the port is a two-color (green and yellow) LED, and indicates the status for the port. Green indicates normal status and yellow indicates an error. The second LED is a single-color (green) LED and indicates the link speed for the port. Green indicates 2 Gbps; if the LED is not lit (dark), it indicates 1 Gbps.

A single-color (green) LED is located on the front of the switch and indicates system power-on status. On the back of the switch, there is a two-color (green and yellow) LED driven by an I2C I/O expander that indicates the mode of the unit. Green indicates normal mode and yellow indicates diagnostic mode. All LEDs are surface mount components with on-board light pipe and are visible externally with full chassis enclosure.

There are two LEDs for the Ethernet port located on the front panel. One LED indicates the transmit and receive activity, and one LED indicates speed (10 Mbps or 100 Mbps).

Software components

The 3534 Model F08 is supported by the Fabric OS version 3.02 or later.

The Fabric OS is implemented in firmware and manages the operation of the 3534 Model F08. The switch firmware is designed to make a 3534 Model F08 easy to install and use while retaining the flexibility needed to accommodate your requirements. A fabric that is constructed with cascaded 3534 Model F08 switches automatically assigns individual switch addresses, establishes frame routes, configures the internal name server, and so on. You can access internal management functions using standard host-based Simple Network Management Protocol (SNMP) software or Web browsers. You can access these functions using network connectivity through the Ethernet port or using IP over the fibre-channel ports. Small computer systems interface (SCSI) Enclosure Services (SES) is also supported as a management method. The management functions of the switch allow you to monitor frame throughput, error statistics, fabric topology, fans, cooling, media type, port status, IDs, and other information to aid in system debugging and performance analysis.

The Fabric OS includes all basic switch and fabric support software as well as optionally licensed software that is enabled using license keys. The fabric license is preinstalled on the 3534 Model F08 to ensure fabric operation.

The Fabric OS is comprised of two major software components:

- Firmware that initializes and manages the switch hardware
- Diagnostics that perform component self-testing algorithms for fault isolation during the manufacturing process and in your installation

The internal firmware can be viewed as a set of embedded applications running on top of a proprietary real-time operating system.

Additionally, host-based software includes the drivers, utilities, and applications that use the switch. Obtain these components from your system vendor or fibre-channel component supplier.

3534 Model F08 software

The 3534 Model F08 software consists of a set of embedded applications running on top of a real-time operating system kernel. The set of applications include the following:

- Name server

- Alias server
- SNMP agent

The set of applications also includes several tasks to manage the following:

- Address assignment
- Routing
- Link initialization
- Fabric initialization
- Link shutdown
- Switch shutdown
- Frame filtering
- Fabric watch
- Auto speed negotiation
- The user interface

All embedded applications are written in C, except for the SNMP agent (included with the real-time operating system package) and the Web Server.

Figure 6 on page 10 shows a block diagram of the various elements that comprise the 3534 Model F08 firmware.

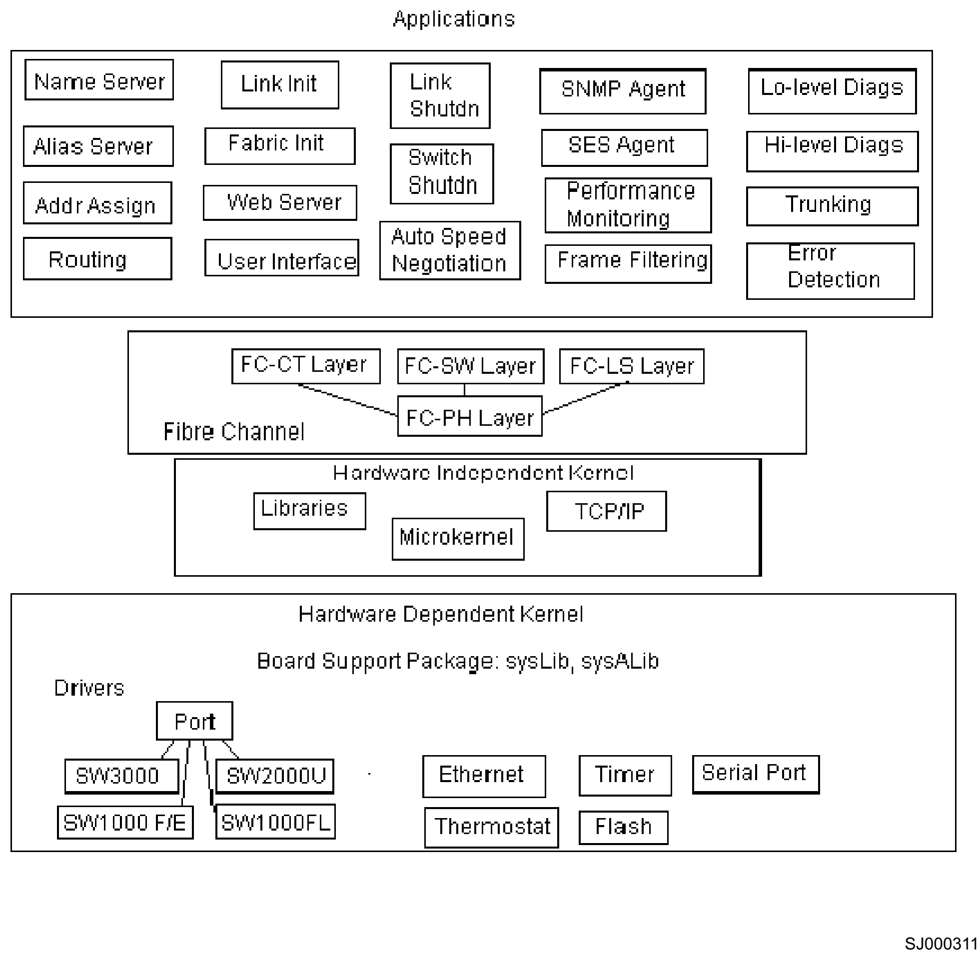


Figure 6. 3534 Model F08 firmware components

Applications

The 3534 Model F08 software applications implement a variety of functions. Switch applications exist to provide fabric services, such as name server and alias server functionality, to external devices. These particular applications process requests from fabric-attached external devices, and communicate with similar applications running on other switches within the fabric to obtain fabric-wide information to satisfy these requests. The applications present an interface to these standards-based services that provides access to information throughout the fabric while hiding the details of how the information is distributed across switches within the fabric from the external devices.

Other applications running in a switch implement functions used to manage internal fabric operation. One task allows for automatic address assignment throughout a fabric through a distributed algorithm run by participating switches. Another task, used to set up routes within the fabric, communicates with tasks that are running on other switches in the fabric to set up loop-free, lowest-cost routes.

The 3534 Model F08 provides an extensive set of diagnostics. A number of comprehensive low-level diagnostics can be used to detect failing switch hardware components by performing hardware-specific tests. In general, these diagnostics must be run when the switch is offline. However, an additional set of high-level diagnostics can be used to exercise individual ports, passing data through external media interfaces and cables. These allow various media, cable, and port faults to be detected while normal switch operation continues on other ports.

New features

The 3534 Model F08 software includes some new features and functionality. The Fabric OS enables the 3534 Model F08 to support the following new functionality:

Auto-sensing speed negotiation

The 3534 Model F08 ASIC supports link operation at either 2 Gbps or 1 Gbps. Auto-sensing negotiation allows easy configuration. The link speed is negotiated to the highest speed that is supported by the device. Speed selection is auto-negotiated by the ASIC driver on a per-port basis. After the speed is determined, the transmitter and receiver for the port are automatically set. If multiple devices are connected to a port (for example on an FL_port), the driver auto-negotiates for the highest common speed and sets the transmitter and receiver accordingly.

Frame filtering

Zoning is a licensed fabric management service that can be used to create logical subsets of devices within a SAN and enable partitioning of resources for management and access control purposes. Frame filtering is a new feature of the 3534 Model F08 ASIC that enables it to provide zoning functions with finer granularity. Frame filtering can be used to set up port level zoning, worldwide name zoning, device level zoning, protocol level zoning, and LUN level zoning. After the filter is set up, the complicated function of zoning and filtering can be achieved at wire speed.

Performance Monitoring

Performance Monitoring is a licensed feature that provides error and performance information to manage your storage environment. There are three types of monitoring:

- Arbitrated Loop Physical Address (AL_PA) monitoring: provides information about the number of cyclic redundancy check (CRC) errors.
- End-to-end monitoring: provides information about a configured source identifier to destination identifier (SID-DID) pair. Information includes the number of CRC errors for frames with the SID-DID pair, fibre-channel words transmitted from the port for the SID-DID pair, and fibre-channel words received for the port for the SID-DID pair.
- Filter-based monitoring: provides error information with a customer-determined threshold.

Trunking

Trunking is a licensed feature that enables traffic to be distributed across available ISLs while still preserving in-order delivery. On some fibre-channel protocol devices, frame traffic between a source device and destination device must be delivered in order within an exchange. This restriction forces current devices to fix a routing path within a fabric. Consequently, certain traffic patterns in a fabric can cause all active routes to be allocated to a single available path and leave other paths unused. The 3534 Model F08 ASIC creates a trunking group (a set of available paths linking two adjacent switches). Ports in the trunking group are called *trunking ports*. One trunking port is designated as the trunking master port and is used to set up all routing paths for the entire trunking group. The trunk provides an 8 Gbps single-aggregate ISL pipe between switches.

Real-time operating system

The 3534 Model F08 real-time operating system consists of a hardware-independent layer and a hardware-dependent section.

The hardware-independent portion of the operating system consists of a third-party real-time kernel plus a number of interfaces. The interfaces provide a structure for handling various layers in the fibre-channel protocol hierarchy.

In this collection of modules, the FC-PH layer provides FC-2 functionality, supporting reassembly of inbound frames into sequences. This layer also allows you to create a set of frames to transmit from an internal fibre channel sequence description.

The FC-LS layer handles various sorts of fibre-channel link services, including basic link services and extended link services.

Operations using the fibre-channel common transport interface, as defined in the FC-GS specification, use the interface provided by FC-CT code in the 3534 Model F08.

Switch-to-switch communications used to manage fabric initialization and routing use the services provided by the FC-SW layer to implement these functions.

Hardware-dependent functions of the real-time operating system contain a number of elements, including the Board Support package. This code is used to provide an interface between VxWorks and the 3534 Model F08-specific hardware related to supporting the 80960VH processor.

Drivers for specific hardware interfaces are also considered part of the hardware-dependent portion of the real-time operating system. A number of drivers support interface hardware that is used for fabric management purposes, such as the Ethernet port and serial port. Other drivers are used for miscellaneous internal functions, including temperature monitoring and power supply control.

Additional drivers, written for the fibre-channel interfaces of the switch, are managed through two layers. One of these, the port driver, creates a generic interface to the underlying switch hardware, and provides functions common to all switch implementations. Reporting to the port driver are the switch hardware-specific drivers, which handle the operations of individual types of switch ASICs. Three of these drivers, for the switch, flannel, and loom chips, are used for IBM's first and second-generation hardware. A fourth module implements the functionality required to drive the Bloom ASIC, which is used in the 3534 Model F08.

Initializing the switch

When the switch is started or restarted, the following operations are performed:

1. Early power-on self test (POST) diagnostics are run. POST is run before VxWorks is running.
2. VxWorks is initialized.
3. The hardware is initialized. The system is reset, the internal addresses are assigned to Loom chips, the Ethernet port is initialized, the serial port is initialized, and the front panel is initialized.
4. A full POST is run.

5. The links are initialized. Receiver and transmitter negotiation is run to bring the connected ports online.
6. A fabric exploration is run. This determines whether any ports are connected to other switches. If so, it determines the principal switch.
7. Addresses are assigned. After the principal switch is identified, port addresses are assigned. Each 3534 Model F08 tries to keep the same addresses that it used previously. Previous addresses are stored in the configuration Flash memory.
8. The routing table is constructed. After the addresses are assigned, the unicast routing tables are constructed.
9. Normal Nx_port operation is enabled.

Routing

The embedded processor maintains two routing tables, one for unicast and one for multicast. The unicast routing tables are constructed during fabric initialization. The multicast tables are initially empty, except for broadcast. After the tables have been constructed they are loaded into each ASIC.

The unicast tables change if ports or links come online or go offline, or if some other topology changes occur. When new paths become available, the embedded processor can change some routes in order to share the traffic load. The multicast tables change as ports register with the alias server to create, join, or leave a multicast group. Each time a table changes, it must be reloaded into the ASICs.

Service functions

The ASIC interrupts the embedded processor when a frame arrives that has an error (for example, incorrect source ID), when a frame times out, or when a frame arrives for a destination that is not in its routing tables. In the latter case, the frame might be addressed to an illegal destination ID, or it might be addressed to one of the service functions that are provided by the embedded processor such as SNMP, name server, or alias server.

SNMP

Simple Network Management Protocol (SNMP) allows network devices to be monitored, controlled, and configured remotely from a network management station running a network manager program.

SNMP agent code in the network device allows management by transferring data that is specified by a management information base (MIB).

The 3534 Model F08 agent supports the following:

- SNMPv1 manager
- Command-line utilities to access and command the agent
- MIB-II system group, interface group, and SNMP group
- Fabric-element MIB
- IBM-specific MIBs
- Standard generic traps
- IBM-specific traps

Diagnostics

The 3534 Model F08 supports a set of POSTs, as well as tests that can be invoked using Telnet commands. These diagnostics are used during the manufacturing process as well as for fault isolation of the product in your installation.

Diagnostic environment

Most diagnostics are written to run in the VxWorks environment. However, as VxWorks does not run without a working SDRAM, a SDRAM/boot EEPROM test is run as part of the pre-VxWorks startup code to verify that the basic processor-connected memories are functioning properly.

Hardware support

Loop-back paths for frame traffic are provided in the hardware for diagnostic purposes. A loop-back path within the ASIC, at the final stages of the fibre-channel interface, can be used to verify that the internal fibre-channel port logic is functioning properly, as well as paths between the interface and the central memory. Additionally, the SERIALLINK macro within the ASIC includes a serial data loop-back function that can be enabled through a register in the corresponding ASIC.

Diagnostics are provided to allow traffic to be circulated between two switch ports that are connected with an external cable. This allows the diagnostics to verify the integrity of the final stage of the SERDES interface, as well as the media interface module.

Diagnostic coverage

The POST and diagnostic commands concentrate on the fibre-channel ports and verify switch functionality of the 3534 Model F08.

Interoperability

This section includes information about interoperability.

Switch interoperability

The 3534 Model F08 supports both 1 Gbps and 2 Gbps transmit and receive rates with auto-negotiation. The actual data signaling rate that is used on a port is automatically sensed and is set to the rate that is supported by a device or devices that are attached to the port. The 3534 Model F08 has been tested and is compliant with the current FC standards. The 3534 Model F08 is compatible with most current-generation switches N_ports, NL_ports, and E_ports, as well as host adapters, Redundant Array of Independent Disks (RAID) storage devices, hubs, and Fibre-SCSI bridge devices, including the 3534 and 2109 series of switches.

Implementation in existing environments

Because the 3534 Model F08 has a compatible 1 Gbps auto-negotiated signaling rate on each port, it can be used as a replacement for current 3534 and 2109 series switches. As newer technology is added to existing systems that support 2 Gbps signaling, the ports can accept these devices and interoperate with existing 1 Gbps devices. If the 3534 Model F08 is connected to a third-party device but is unable to negotiate the signaling rate, the 3534 Model F08 allows you to manually set the speed of each port through the management interfaces.

Heterogeneous inter-switch operations

Fabric OS version 3.0 supports interoperability for the following functions:

- Basic switch functions
  - Link initialization
  - Principal switch selection
  - Routing fibre channel shortest path first (FSPF)
- Basic services
  - Simple name service
  - State change notification
  - WWN zoning (typically referred to as soft zoning or name server zoning)

The following facilities are switch-based facilities and will continue to function on any 3534 switch:

- SNMP facilities
- Simple QuickLoops with no zoning
- Translative mode (private target support on fabrics)
- Trunking (only functions between two IBM switches)
- Enhanced performance metrics

The following facilities are IBM value-added facilities that are not supported in a multi-vendor fabric. Use of these facilities causes the Fabric to segment.

- QuickLoop zones
- QuickLoop Fabric assist mode
- Port, protocol, or LUN zoning

IBM is not aware of any areas of noncompliance with any ratified standards at this time.

Host bus adapter interoperability

For a list of host bus adapters (HBAs) that have been tested and approved for use with the 3534 Model F08, go to the following Web site:
www.storage.ibm.com/ibmsan/products/2109/san_switch_solu.html

Operating system support

Fabric OS versions 2.x and 3.x have no specific OS dependencies. The Fabric OS in the switches allows for any fibre-channel-compliant device to attach to the switches as long as it conforms to the standards for device login, name service, and related fibre-channel features. Regardless of the operating environment, proper interface to the fabric requires a fibre-channel HBA with a standards-compliant driver.

Reliability

The 3534 Model F08 provides the following features to ensure reliability:

- POST
- Error detection and fault isolation (internal and external CRC checking, parity checking, checksum, and illegal address checking)
- Continuous monitoring of environmental components (fan status and temperature)
- DC power in proper range monitoring

- Low component count

Because buffering is integrated into the ASICs in the 3534 Model F08, there is no need for external SRAM chips on the system board.

The 3534 Model F08 utilizes a highly integrated 80960VH processor that incorporates a memory controller, PCI bus arbiter, and I2C controller in the processor chip, reducing the parts count for the processor functions. Because a single system board contains all circuitry, the 3534 Model F08 requires no interboard connections.

Support services and documentation

IBM provides a wide array of support services for its products. This section provides information about how to report a problem.

Problem reporting procedures

To report problems about the machine, 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 might be required to present proof of purchase.

To assist your support team with diagnosing a resolution, have the following data available when you call for support:

- Switch serial number
- Error codes
- Symptoms
- Topology configuration

Additionally, if you have a general switch question, have an open Telnet connection prior to placing your telephone call.

Specifications

The 3534 Model F08 is designed as a piece of network equipment. Its primary operating environments are server rooms, network equipment closets, and office environments. Table 1 lists the performance, mechanical, environmental, and power specifications for the 3534 Model F08.

Table 1. Performance, mechanical, environmental, and power specifications for the 3534 Model F08

Performance specifications	
Routing capacity	A minimum aggregate routing capacity of 10 million frames per second is provided for Class 2, Class 3 and Class F frames in an 8-port switch.

Table 1. Performance, mechanical, environmental, and power specifications for the 3534 Model F08 (continued)

Performance specifications	
Latency	The maximum latency for Class 2, Class 3 and Class F frames from input F_port to output F_port within a single switch is less than 2 microseconds when the destination port is free. Cut-through routing: transmission can begin as the frame arrives. Same latency as the 3534 and the 2109 series of switches.
Mechanical specifications	
Enclosure	1U, 48.26 cm (19 in.), EIA compliant Power from front Air flow back to front Height: 4.2 cm (1.69 in.) Width: 42.8 cm (16.9 in.) Depth: 26.4 cm (10.4 in.)
Weight	3.9 kg (8.5 lbs)
Environmental specifications	
Temperature (operating)	10° - 40°C (50° - 104°F)
Temperature (nonoperating)	-25° - 70°C (-13° - 158°F)
Vibration (operating)	0.5 G, 5–500–5 Hz
Vibration (nonoperating)	2.0 G, 5–500–5 Hz
Humidity (operating)	20% - 85% noncondensing at 40°C (104°F)
Humidity (nonoperating)	90% RH noncondensing at 40°C (104°F)
Altitude	Up to 3000 m (9800 ft) above sea level
Shock (operating)	150 G, 2.7 ms half-sine
Shock (nonoperating)	60 G, 13 ms trapezoid
Input voltage	90 – 264 V ac
Frequency	47 - 63 Hz
Power consumption	50 W maximum

Chapter 2. Fabric OS

This chapter provides the following information about Fabric OS:

- “Setting the initial configuration”
- “Basic configuration procedures” on page 21
- “Working with the management server” on page 29
- “Displaying port status and error logs” on page 31
- “Displaying the switch status” on page 33

This chapter contains various Telnet commands. For a complete description of these commands, see the *IBM TotalStorage SAN Fibre Channel Switch 3534 Model F08 Command Reference*.

Setting the initial configuration

This section provides information about the initial configuration tasks for a switch.

Logging into a switch

Perform the following steps to log into a switch:

1. Open a Telnet connection to the switch. The login prompt is displayed if the Telnet connection successfully found the switch in the network.

   Note: The switch must be connected to your IP network through the RS232 port to enable connection through Telnet. See “Configuring the IP and fibre-channel address” on page 20 for more information about connecting the switch to your IP network.
2. At the login prompt, type the user ID that you are logging in as. For example:
   ```
   login: admin
   ```
   The password prompt is displayed if the user ID is valid.
3. Type the password for the user:
   ```
   password: xxxxxx
   ```
   The default password is `password`.
4. If the login is successful, a prompt is displayed showing the switch name and the user ID you are logged in as. For example:
   ```
   switch55>admin:
   ```

Enabling licensed features

Though licensed features such as zoning, Fabric Watch, Trunking, QuickLoop, and TotalStorage Specialist are already loaded onto the switch firmware, they must be enabled with a license key. After you have purchased these features, you are provided with a key to unlock the feature. Perform the following steps to enable a licensed feature:

1. Login to the switch as the admin user.
2. At the command line, type the following command:
   ```
   licenseAdd "aaaBbbCcc"
   ```
   where `aaaBbbCcc` is the license key for a particular feature.

   Note: You must type a license key for each feature that you want to activate. License keys are case sensitive.

Displaying the installed feature licenses

Perform the following steps to display the features that have been enabled on a switch:

1. Login to the switch as the admin user.
2. At the command line, type the following command:

   `licenseShow`

   This command displays the license keys that have been entered for the switch and the features that are enabled by those licenses.

Changing the admin user ID and password

For security reasons, you are requested to change the admin user ID and system password the first time that you log into the Fabric OS.

Perform the following steps to change the admin user ID and password:

1. Login to the switch as the admin user.
2. At the command line, type the following command:

   `passwrd "admin"`

   An interactive session opens, and you are prompted for configuration values.
3. At the `New username` prompt, type a new name for the admin user. You can change the name of the admin user without changing the password. Press Enter to leave the name as is.
4. At the `Old password` prompt, type the old password.
5. At the `New password` prompt, type the new password. The new password must be 8 - 40 characters in length.
6. At the `Re-enter new password` prompt, type the new password exactly as you typed it in the previous prompt.
7. Press Enter to commit the configuration to the firmware.

Configuring the IP and fibre-channel address

The switch is shipped with a default IP address of 10.77.77.77. Perform the following steps to change the default IP address and to configure the fibre-channel IP address of the switch:

1. Login to the switch as the admin user.
2. At the command line, type the following command:

   `ipAddrSet`

   An interactive session opens, and you are prompted for configuration values. Press Enter without entering a value to skip a prompt and leave the parameter value as is.
3. At the `Ethernet IP Address` prompt, type the new IP address for the Ethernet port on the switch and press Enter.
4. At the `Ethernet Subnetmask` prompt, type the address of the subnetmask and press Enter.
5. At the `Fibre Channel IP address` prompt, type the fibre-channel IP address for the switch and press Enter.
6. At the `Fibre Channel Subnetmask` prompt, type the address of the subnetmask and press Enter.
7. At the `Gateway Address` prompt, type the IP address of the gateway and press Enter.

   The configuration is then committed to the switch firmware.

8. You are then prompted whether to make the IP address changes active now or at the next restart. Type `y` at the prompt to change the IP addresses immediately (without restarting).

Displaying the fabric-wide device count

To verify that you have fabric-wide connectivity when you install a new switch, display the fabric-wide device count from the newly installed switch.

Perform the following steps to display the fabric-wide device count from a switch:

1. Login to the switch as the admin user.
2. At the command line, type the following command:

   `nsAllShow`

   This command displays all the connected devices in the fabric.

Basic configuration procedures

This section provides information about the basic configuration tasks for a switch.

Setting the Telnet timeout value

Perform the following steps to set a new Telnet timeout value:

1. Login to the switch as the admin user.
2. At the command line, type the following command:

   `timeout x`

   where `x` is the number of minutes before the Telnet connection times out. If you specify `0`, the Telnet connection never times out. Timeout is disabled by default.

Displaying the firmware version

Perform the following steps to display the firmware version:

1. Login to the switch as the admin user.
2. At the command line, type the following command:

   `version`

   This command displays the kernel version, the Fabric OS release number, and other information about the firmware.

Setting the switch date and time

All switches maintain the current date and time in nonvolatile memory. Date and time are used for logging events. Switch operation does not depend on the date and time; a switch with an incorrect date and time value still functions properly.

Perform the following steps to set the date and time of a switch:

1. Login to the switch as the admin user.
2. At the command line, type the following command:

   `date "MMDDhhmmYY"`

   where `MM` is the month, `DD` is the date, `hh` is the hour, `mm` is minutes, and `YY` is the year.

Valid values for date ″MMDDhhmmYY″

MM	01 - 12
DD	01 - 31
hh	00 - 23
mm	00 - 59
YY	00 - 99

Note: Year values greater than 69 are interpreted as 1970 - 1999; year values less than 70 are interpreted as 2000 - 2069. The date function does not support daylight saving time or time zones.

Displaying the system configuration settings

Perform the following steps to display the system configuration settings:

1. Login to the switch as the admin user.
2. At the command line, type the following command:

   ```
   configShow
   ```

   The system configuration settings are displayed.

Note: For more information about the system configuration settings, see the *IBM TotalStorage SAN Fibre Channel Switch 3534 Model F08 Command Reference Guide*.

Backing up the system configuration settings

The two supplied utilities, RSHD.EXE and CAT.EXE, currently do not support uploads for Windows, only downloads. Therefore, FTP must be used on Windows workstations to backup the system configuration, and the FTP server must be running before an upload can occur.

Perform the following steps to upload a backup copy of the configuration settings to a host computer:

1. Verify that the RSHD service (on a UNIX machine) or the FTP service (on a Windows machine) is running on the host workstation.
2. Login to the switch as the admin user.
3. At the command line, type the following command:

   ```
   configUpload "hostIPaddr", "user", "path_filename","password"
   ```

   where:

   - `"hostIPaddr"` is the IP address of the host computer
   - `"user"` is the user ID used to log into this computer
   - `"path_filename"` is the path location and filename of the system configuration file
   - `"password"` is the password for the user ID specified

   Note: The `password` operand is only required if you are using FTP.

Restoring the system configuration settings

Perform the following steps to restore the system configuration settings from a backup copy:

1. Verify that the RSHD service (on a UNIX machine) or the FTP service (on a Windows machine) is running on the host workstation.
2. Login to the switch as the admin user.
3. Shut down the switch by typing the following command at the command line:

   `switchDisable`
4. At the command line, type the following command:

   `configDownload "hostIPaddr", "user", "path_filename","password"`

   where:
   - `"hostIPaddr"` is the IP address of the host computer
   - `"user"` is the user ID used to log into this computer
   - `"path_filename"` is the path location and filename of the system configuration file
   - `"password"` is the password for the user ID specified

   Note: The `password` operand is only required if you are using FTP.
5. Restart the switch by typing the following command:

   `fastboot`

Upgrading or restoring the switch firmware

Perform the following steps to upgrade or restore the switch firmware:

1. Verify that the RSHD service (on a UNIX machine) or the FTP service (on a Windows machine) is running on the host workstation.
2. Login to the switch as the admin user.
3. At the command line, type the following command:

   `firmwareDownload "hostIPaddr", "user", "path_filename", "password"`

   where:
   - `"hostIPaddr"` is the IP address of the host computer
   - `"user"` is the user ID used to log into this computer
   - `"path_filename"` is the path location and filename of the new firmware file
   - `"password"` is the password for the user ID specified

   Note: The `password` operand is only required if you are using FTP.
4. Restart the switch by typing the following command:

   `fastboot`

Disabling a switch

Perform the following steps to disable a switch:

1. Login to the switch as the admin user.
2. At the command line, type the following command:

   `switchDisable`

All fibre-channel ports on the switch are taken offline. If the switch was part of a fabric, then the remaining switches are reconfigured.

Enabling a switch

Perform the following steps to enable a switch:

1. Login to the switch as the admin user.
2. At the command line, type the following command:

   `switchEnable`

All fibre-channel ports that passed the POST are enabled. If the switch was part of a fabric, it rejoins the fabric.

Disabling a port

Perform the following steps to disable a port:

1. Login to the switch as the admin user.
2. At the command line, type the following command:

   `portDisable portnumber`

   where `portnumber` is the number of the port that you want to disable. If the port is connected to another switch, the fabric might reconfigure. If the port is connected to one or more devices, these devices are no longer available to the fabric.

Enabling a port

Perform the following steps to enable a port:

1. Login to the switch as the admin user.
2. At the command line, type the following command:

   `portEnable portnumber`

   where `portnumber` is the number of the port that you want to enable. If the port is connected to another switch, the fabric might reconfigure. If the port is connected to one or more devices, these devices become available to the fabric.

Changing a switch name

Perform the following steps to change the name of a switch:

1. Login to the switch as the admin user.
2. At the command line, type the following command:

   `switchName new_name`

   where `new_name` is the new name for the switch. Switch names can be up to 19 characters long, they must begin with a letter, and they can contain letters, numbers, or the underscore character.

Setting the switch status policy

There are seven parameters that determine the status of a switch:

- Number of faulty ports
- Missing gigabit interface converters (GBICs)
- Power supply status
- Temperature in the enclosure
- Fan speed
- Port status
- Sgroup ISL status

Each parameter can be adjusted so that a specific threshold must be reached before that parameter changes the overall status of a switch to MARGINAL or DOWN. Only one parameter needs to pass the MARGINAL or DOWN threshold to change the overall status of the switch.

Viewing the policy threshold values

Perform the following steps to view the switch status policy threshold values:

1. Login to the switch as the admin user.
2. At the command line, type the following command:

   ```
   switchStatusPolicyShow
   ```

Configuring the policy threshold values

Perform the following steps to set the switch status policy threshold values:

1. Login to the switch as the admin user.
2. At the command line, type the following command:

   ```
   switchStatusPolicySet
   ```

   The current switch status policy parameter values are displayed.
3. You are prompted to type values for the DOWN and MARGINAL thresholds for each parameter:
   a. Type the number of faulty ports that are required to change the switch status to DOWN and press Enter.
   b. Type the number of faulty ports that are required to change the switch status to MARGINAL and press Enter.
   c. Type the number of missing GBICs that are required to change the switch status to DOWN and press Enter.
   d. Type the number of missing GBICs that are required to change the switch status to MARGINAL and press Enter.
   e. Type the number of bad power supply warnings that are required to change the switch status to DOWN and press Enter.
   f. Type the number of bad power supply warnings that are required to change the switch status to MARGINAL and press Enter.
   g. Type the number of temperature warnings that are required to change the switch status to DOWN and press Enter.
   h. Type the number of temperature warnings that are required to change the switch status to MARGINAL and press Enter.
   i. Type the number of fan speed warnings that are required to change the switch status to DOWN and press Enter.
   j. Type the number of fan speed warnings that are required to change the switch status to MARGINAL and press Enter.
   k. Type the number of port down warnings that are required to change the switch status to DOWN and press Enter.
   l. Type the number of port down warnings that are required to change the switch status to MARGINAL and press Enter.
   m. Type the number of ISL status down warnings that are required to change the switch status to DOWN and press Enter.
   n. Type the number of ISL status down warnings that are required to change the switch status to MARGINAL and press Enter.

   Note: By setting the DOWN and MARGINAL values for a parameter to 0,0 that parameter is ignored in setting the overall status for the switch.

4. Verify the threshold settings that you have configured for each parameter. Type the following command to view your current switch status policy configuration:

   ```
   switchStatusPolicyShow
   ```

Enabling the track changes feature

Perform the following steps to enable the track changes feature:

1. Login to the switch as the admin user.
2. At the command line, type the following command:

   ```
   trackChangesSet 1
   ```

A prompt is displayed, verifying that the track changes feature is on. The output from the track changes feature is dumped to the error log for the switch. Use the **errdump** command or the **errshow** command to view the error log.

Trackable changes are:

- Successful login
- Unsuccessful login
- Logout
- Config file change from task
- Track-changes on
- Track-changes off

Items in the error log that are created and that are from the track changes feature are labeled `Error TRACK`. For example:

```
Error 08
---------
0x102cf710 (tShell): May 2 16:12:10
   Error TRACK-LOGIN, 4, Successful login
```

Displaying whether track changes is enabled

Perform the following steps to display the status of the track changes feature:

1. Login to the switch as the admin user.
2. At the command line, type the following command:

   ```
   trackChangesShow
   ```

The status of the track changes feature is displayed as either `on` or `off`. This also displays whether the track changes feature is configured to send SNMP traps. For example:

```
switch:admin> trackChangesShow
Track changes status: ON
Track changes generate SNMP-TRAP: NO
```

Configuring a static route between two ports

Perform the following steps to configure a static route between two ports:

1. Login to the switch as the admin user.
2. At the command line, type the following command:

```
uRouteConfig port, domain, outputport
```

where:

- `port` is the port to be statically routed (this can be either an F_port or an E_port)
- `domain` is the domain ID of the specified target switch
- `outputport` is the output port where traffic is to be forwarded

After this command is issued, and if the output port is a usable port, all frames coming in from a specified port addressed to the specified domain are routed through the specified output port.

If the output port is not usable, the routing assignment is not affected. When the output port becomes usable, the static route assignment for the port is enforced.

Note: Using static routes can affect load sharing. If a large number of routes are statically configured to the same output port, the ability of the switch to achieve optimum load sharing can be impaired.

Configuring the in-order delivery option

In a stable fabric, frames are always delivered in order, even when the traffic between switches is shared among multiple paths. However, when topology changes occur in the fabric (for instance, a link goes down), traffic is rerouted around the failure. When topology changes occur, some frames might be delivered out-of-order.

The default behavior enables out-of-order delivery of frames during fabric topology changes. This enables fast rerouting after a fabric topology change.

Forcing in-order delivery of frames

Perform the following steps to force in-order delivery of frames during fabric topology changes:

1. Login to the switch as the admin user.
2. At the command line, type the following command:

   ```
   iodSet
   ```

   Note: This command can cause a delay in establishing a new path when a topology change occurs and should be used with care.

Disabling in-order delivery of frames

Perform the following steps to disable in-order delivery of frames during fabric topology changes:

1. Login to the switch as the admin user.
2. At the command line, type the following command:

   ```
   iodReset
   ```

Displaying help information for a Telnet command

Perform the following steps to display help information about a Telnet command:

1. Login to the switch.
2. At the command line, type the following command:

   ```
   help command
   ```

   where `command` is the command name that you would like help with.

Reading hexadecimal port diagrams

Many of the commands return port diagrams in hexadecimal format. For example:

```
switch:admin> bcastShow
Group    Member Ports    Member ISL Ports   Static ISL Ports
256      0x00012083      0x00002080              0x00000000
```

To read the hexadecimal port diagrams, they must be converted into binary notation. Each hexadecimal value represents four binary values. Each hexadecimal value is converted into a group of four binary values that represent four ports, as listed in Table 2.

Table 2. Hex and binary values

Hex value	**Binary value**
0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001
A	1010
B	1011
C	1100
D	1101
E	1110
F	1111

After the hexadecimal value is converted into a binary bit map, each bit represents a port, where a value of “1” means “yes” and a value of “0” means “no”. The bit map is read from right to left, that is, the least significant bit represents port 0.

For example, if the member port value is displayed in hex as:

```
0x00012083
```

This corresponds to a binary bit map of the member ports as follows:

```
0000 0000 0000 0001 0010 0000 1000 0011
```

This bit map displays the member ports as port 0, 1, 7, 13, and 16.

Working with the management server

This section provides information about working with the management server platform database.

The management server allows a SAN management application to retrieve and administer the fabric and interconnect elements such as switches, servers, and storage devices. It is located at the fibre-channel address FFFFFAh.

Configuring access to the management server

An access control list (ACL) of WWN addresses determines which systems have access to the management server platform database. If the ACL is empty (default), the management server is accessible to all systems that are connected in-band to the fabric. For a more secured access, an administrator can specify WWNs in the ACL. These WWNs are usually associated with the management applications. If any WWNs are entered into the ACL, then access to the management server is restricted to only those WWNs listed in the ACL.

Displaying the access control list

Perform the following steps to display the management server ACL:

1. Login to the switch as the admin user.
2. At the command line, type the following command:

   `msConfigure`
3. At the prompt, type `1` to display the access list.

   A list of WWNs that have access to the management server are displayed. For example:

```
MS Access List consists of (3):{

 20:01:00:60:69:00:60:10
 20:02:00:60:69:00:60:10
 20:03:00:60:69:00:60:10
```

Adding a WWN to the access control list

Perform the following steps to add a WWN to the ACL:

1. Login to the switch as the admin user.
2. At the command line, type the following command:

   `msConfigure`
3. At the prompt, type `2` to add a member based on its port or node WWN.
4. At the prompt, type the WWN of the member that you would like to add to the ACL. For example:

   `20:02:00:60:69:00:60:03`

   After the action is complete, the main menu is displayed.
5. At the prompt, type `1` to verify that the WWN that you entered was added to the ACL.
6. After you have verified that the WWN was added correctly, type `0` at the prompt to end the session.
7. The following prompt is displayed:

   `Update the FLASH? (yes, y, no, n): [yes]`
8. Press Enter to update the Flash memory and to end the session.

Deleting a WWN from the access control list

Perform the following steps to delete a WWN from the ACL:

1. Login to the switch as the admin user.
2. At the command line, type the following command:

   `msConfigure`
3. At the prompt, type `3` to delete a member based on its port or node WWN.
4. At the prompt, type the WWN of the member that you would like to delete from the ACL. For example:

   `20:02:00:60:69:00:60:03`

   After the action is complete, the main menu is displayed.
5. At the prompt, type `1` to verify that the WWN that you entered was deleted from the ACL.
6. After you have verified that the WWN was deleted correctly, type `0` at the prompt to end the session.
7. The following prompt is displayed:

   `Update the FLASH? (yes, y, no, n): [yes]`
8. Press Enter to update the Flash memory and to end the session.

Displaying the management server platform database

Perform the following steps to view the contents of the management server platform database:

1. Login to the switch as the admin user.
2. At the command line, type the following command:

   `msPlatShow`

The contents of the management server platform database are displayed. For example:

```
---------------------------------------------------------
Platform Name: [9] "first obj"
Platform Type: 5 : GATEWAY
Number of Associated M.A.: 1
Associated Management Addresses:
  [35] "http://java.sun.com/products/plugin"
Number of Associated Node Names: 1
Associated Node Names:
  10:00:00:60:69:20:15:71
---------------------------------------------------------
Platform Name: [10] "second obj"
Platform Type: 7 : HOST_BUS_ADAPTER
Number of Associated M.A.: 1
Associated Management Addresses:
  [30] "http://java.sun.com/products/1"
Number of Associated Node Names: 2
Associated Node Names:
  10:00:00:60:69:20:15:79
  10:00:00:60:69:20:15:75
```

Clearing the management server platform database

Perform the following steps to clear the management server platform database:

1. Login to the switch as the admin user.
2. At the command line, type the following command:

```
msPlClearDB
```

The following message is displayed:

```
Fabric-wise Platform DB Delete operation in progress...
done ...
```

Displaying the capability of a fabric for management server support

Perform the following steps to display the capability of a fabric for management server support:

1. Login to the switch as the admin user.
2. At the command line, type the following command:

   ```
   msPlCapabilityShow
   ```

The name, WWN, and specific management server capability is displayed for each switch in the fabric.

Activating the management server

Perform the following steps to activate the management server for a fabric:

1. Login to the switch as the admin user.
2. At the command line, type the following command:

   ```
   msPlMgmtActivate
   ```

The following message is displayed:

```
Committing configuration...done.
Request Fabric to activate Platform Management services....
Done.
```

Deactivating the management server

Perform the following steps to deactivate the management server for a fabric:

1. Login to the switch as the admin user.
2. At the command line, type the following command:

   ```
   msPlMgmtDeactivate
   ```

3. At the prompt, type `y` and press Enter.

The following message is displayed:

```
This will erase all Platform entries. Are you sure? (yes, y, no, n): [no] y
Committing configuration...done.
Request Fabric to Deactivate Platform Management services....
Done.
```

Displaying port status and error logs

This section provides information about displaying port status and information about errors.

Note: For more information, see the *IBM TotalStorage SAN Fibre Channel Switch 3534 Model F08 Command Reference*.

Displaying the port status

There are two types of statistics that you can view for a port:

- Software statistics
- Hardware statistics

Displaying software statistics for a port

Software statistics for a port include information such as the port state, the number of interrupts, the number of link failures, the number of loss of synchronization warnings, and the number of loss of signal warnings.

Perform the following steps to display the software statistics for a port:

1. Login to the switch as the admin user.
2. At the command line, type the following command:

   `portShow portnumber`

   where `portnumber` is the number of the port that you want to view. A table of software statistics for the port is displayed.

Displaying hardware statistics for a port

Hardware statistics for a port include information such as the number of frames received, the number of frames sent, the number of encoding errors received, and the number of Class 2 and Class 3 frames received.

Perform the following steps to display the hardware statistics for a port:

1. Login to the switch as the admin user.
2. At the command line, type the following command:

   `portStatsShow portnumber`

   where `portnumber` is the number of the port that you want to view. A table of hardware statistics for the port is displayed.

Displaying a summary of port errors

Perform the following steps to display a summary of port errors for a switch:

1. Login to the switch as the admin user.
2. At the command line, type the following command:

   `portErrShow`

A summary of port errors for all the ports in a single switch is displayed.

The display contains one output line per port. Table 3 explains the types of errors counted.

Table 3. Port error summary

Error type	Description
frames tx	Frames transmitted.
frames rx	Frames received.
enc in	Encoding errors inside frames.
crc err	Frames with CRC errors.
too shrt	Frames shorter than minimum.

Table 3. Port error summary (continued)

Error type	Description
too long	Frames longer than maximum.
bad eof	Frames with bad end-of-frame delimiters.
enc out	Encoding error outside of frames.
disc c3	Class 3 frames discarded.
link fail	Link failures (LF1 or LF2 states).
loss sync	Loss of synchronization.
loss sig	Loss of signal.
frjt	Frames rejected with F_RJT.
fbsy	Frames busied with F_BSY.

Displaying a port error log

There are two ways to display the error log for the fibre-channel frames of all ports on a switch:

- Display the error log one page (22 entries) at a time
- Display the entire error log

Perform the following steps to display the error log one page (22 entries) at a time:

1. Login to the switch as the admin user.
2. At the command line, type the following command:
   ```
   portLogShow
   ```

Perform the following steps to display the entire error log:

1. Login to the switch as the admin user.
2. At the command line, type the following command:
   ```
   portLogDump
   ```

Clearing a port error log

Clearing a port error log is useful when conducting diagnostics on a port. For example, you might want to clear the port log before triggering an activity so that the port log only contains information about that activity.

Perform the following steps to clear a port error log:

1. Login to the switch as the admin user.
2. At the command line, type the following command:
   ```
   portLogClear
   ```
3. Verify that the port log was cleared by running the **portLogShow** command.

Displaying the switch status

The switch status can be either Healthy/OK, Marginal/Warning, or Down. The overall status of a switch is determined by the status of several individual components within the switch. For more information about how the overall switch status is determined, see the *IBM TotalStorage SAN Fibre Channel Switch 3534 Model F08 Command Reference*.

Perform the following steps to display the overall status of a switch:

1. Login to the switch as the admin user.
2. At the command line, type the following command:

   ```
   switchStatusShow
   ```

   The status of the switch should be Healthy/OK. If the status is Marginal/Warning or Down, the components contributing to this status are displayed.

Displaying information about a switch

Perform the following steps to display information about a switch:

1. Login to the switch as the admin user.
2. At the command line, type the following command:

   ```
   switchShow
   ```

The **switchShow** command displays the following information for a switch:

switchName
The name of the switch.

switchName
The symbolic name of the switch.

switchType
The model and firmware version numbers of the switch.

switchState
The state of the switch. Valid states are: Online, Offline, Testing, or Faulty.

switchRole
The role of the switch. Valid roles are: Principal, Subordinate, or Disabled.

switchDomain
The domain ID of the switch.

switchId
The embedded port destination ID (DID) of the switch.

switchWwn
The worldwide name of the switch.

switchBeacon
The beaconing state of the switch. Valid states are: On, Off.

zoning mode
The zoning mode of the switch. Valid modes are: On, Off.

The **switchShow** command also displays the following information for ports on the specified switch:

Module type
The GBIC type, if a GBIC is present.

Port status
The port status.

Displaying the uptime of a switch

Perform the following steps to display the uptime for a switch:

1. Login to the switch as the admin user.
2. At the command line, type the following command:

   ```
   uptime
   ```

This command displays the length of time that the system has been running, the total cumulative amount of up time since the system was first started, the date and time of the last restart, and the reason for the last restart.

The reason for the last switch restart is also recorded in the error log.

Displaying the fan status

Perform the following steps to display the fan status of a switch:

1. Login to the switch as the admin user.
2. At the command line, type the following command:

   ```
   fanShow
   ```

The possible values for fan status are:

OK The fan is functioning correctly.

below minimum
The fan is present, but is rotating too slowly or has stopped.

Displaying the temperature status

Perform the following steps to display the temperature status of a switch:

1. Login to the switch as the admin user.
2. At the command line, type the following command:

   ```
   tempShow
   ```

This command displays the current temperature readings from each of the five temperature sensors located on the main printed circuit board of the switch. The sensors are located, approximately, one in each corner and one at the center of the printed circuit board.

Displaying a switch error log

There are two ways to display a switch error log:

- Display the error log one page (22 entries) at a time
- Display the entire error log

Perform the following steps to display the switch error log one page (22 entries) at a time:

1. Login to the switch as the admin user.
2. At the command line, type the following command:

   ```
   errShow
   ```

Perform the following steps to display the entire switch error log:

1. Login to the switch as the admin user.
2. At the command line, type the following command:

   ```
   errDump
   ```

Running diagnostic tests on the switch hardware

There are several diagnostic tests that you can run on a switch. Every time a switch is started, these tests are generally run during the POST. For more information on these tests, see the *IBM TotalStorage SAN Fibre Channel Switch 3534 Model F08 Command Reference Guide*.

- camTest
- centralMemoryTest
- cmemRetentionTest
- cmiTest
- crossPortTest
- portLoopbackTest
- sramRetentionTest
- turboRamTest
- statsTest
- spinSilk

Chapter 3. TotalStorage Specialist

This chapter provides the following information about TotalStorage Specialist:

TotalStorage Specialist overview

TotalStorage Specialist provides a graphical interface that allows you to monitor and manage entire fabrics and individual switches and ports from a standard workstation. It runs on Fabric OS. All switches in the fabric are displayed in the main window of TotalStorage Specialist, including switches that do not have a TotalStorage Specialist license. However, only switches that have a TotalStorage Specialist license installed can be managed through TotalStorage Specialist. Other switches must be managed using Telnet or SES.

Advantages of TotalStorage Specialist

TotalStorage Specialist is an excellent partner to the traditional Telnet commands, and in many ways can provide faster and more effective results than can be achieved strictly through a command-line interface.

Following are some of the features that make TotalStorage Specialist an important part of the switch management and administration process.

TotalStorage Specialist:

- Can be used simultaneously with Telnet commands.
- Can help you find the appropriate Telnet command to perform a desired function. For instance, you can perform a function using TotalStorage Specialist, and watch in a second window as the Telnet commands are displayed.
- Simplifies the zoning process.
- Provides the Performance Monitor feature. This feature allows you to view the status and traffic of a switch or port in seconds by easily creating a variety of effective graphs.
- Is easy and intuitive to use.

Capabilities of TotalStorage Specialist

TotalStorage Specialist provides the following information and capabilities:

- Monitoring and managing the entire fabric
  - Status of all switches in the fabric
  - Access to event logs for entire fabric
  - Zoning functions (optionally licensed)
  - Access to the Name Server Table
  - Telnet functions
  - Switch beaconing for rapid identification in large fabric environments
  - Ability to name and zone QuickLoops

- Monitoring and managing individual switches
  - Summary information about each switch
  - Access to event logs for individual switches
  - Switch configuration and administration
  - Ability to upgrade Fabric OS and license key administration
  - Report capability for switch configuration information
- Monitoring and managing individual ports
  - Port status
  - Information about GBIC serial IDs
  - Information about connected devices
  - Loop information
  - Port performance including frame counts (frames in, frames out) and error counts

When monitoring and managing the entire fabric, TotalStorage Specialist allows you to perform the following functions:

- View the status of all the switches in the fabric.

  For more information, see “Fabric view” on page 49.
- Access event logs for the entire fabric.

  For more information, see “Fabric Events view” on page 52.
- Set up and manage zoning functions (optionally licensed).

  For more information, see “Zone Administration view (optional software required)” on page 57.
- Access the Name Server Table.

  For more information, see “Name Server Table view” on page 55.
- Access Telnet functions.

  For more information, see “Telnet interface” on page 150.
- Use switch beaconing for rapid identification in large fabric environments.

  For more information, see “Switch Events view” on page 86.
- Name and zone QuickLoops (optionally licensed).

  For more information, see “QuickLoop tab” on page 146.

When monitoring and managing individual switches, TotalStorage Specialist allows you to perform the following functions:

- View summary information about each switch.

  For more information, see “Config tab” on page 82.
- View event logs for individual switches.

  For more information, see “Switch Events view” on page 86.
- Perform switch configuration and administration.

  For more information, see “Administrative Interface” on page 126, “Switch Settings tab” on page 128, “Current Settings tab” on page 97, and “Fabric Watch view (optional software required)” on page 88.
- Use the ability to upgrade Fabric OS and license key administration.

  For more information, see “Firmware/Upgrade tab” on page 131.
- Use report capability for switch configuration.

  For more information, see “Report tab” on page 137.

When monitoring and managing individual ports, TotalStorage Specialist allows you to perform the following functions:

- View the port status.

  For more information, see “PortStats tab” on page 99.
- View information about GBIC serial IDs.

  For more information, see “GBIC tab” on page 101.
- View and manage loop information.

  For more information, see “Loop tab” on page 104, “QuickLoop tab” on page 146, or “Name Server Table view” on page 55.
- View port performance, including frame counts (frames in, frames out) and error counts.

  For more information, see “Current Settings tab” on page 97.

TotalStorage Specialist main views

TotalStorage Specialist provides access to and information about the fabric through a number of separate windows called *views*, making it possible to manage and monitor several aspects of the fabric at the same time.

The main views available through TotalStorage Specialist are:

- Fabric view
- Switch view
- Port Information view

Note: Each main view has several layers, or subviews, that allow for more complex functionality. For more information about what you can do with these views, see “Fabric view” on page 49, “Switch view” on page 84, or “Port Information view” on page 97.

Following is a brief summary of each view. These views are discussed in detail in following sections.

Fabric view

The initial display after launching TotalStorage Specialist is the Fabric view, as shown in Figure 7 on page 40.

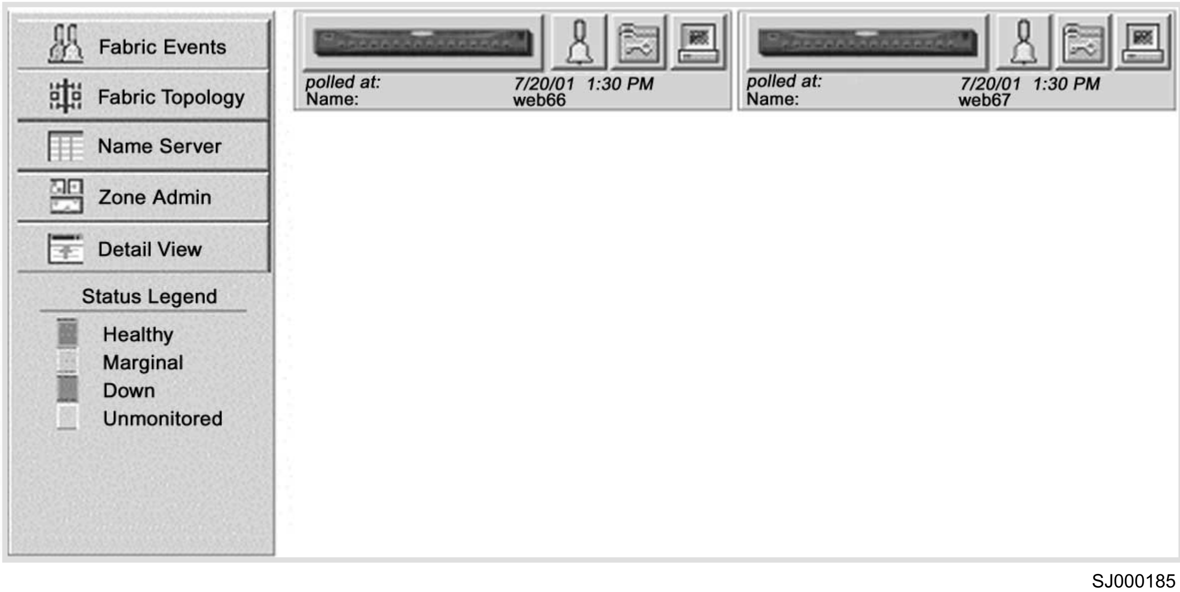


Figure 7. Fabric view

Fabric view displays a control panel that provides access to fabric-wide options, a panel for each switch in the fabric, plus a legend that explains the meaning of the background colors on the **Switch** icons. Each panel contains an icon that represents the switch itself, in addition to icons for Switch Events and the Administrative and Telnet interfaces. The background color of the switch icon represents the status of that particular switch or integrated fabric.

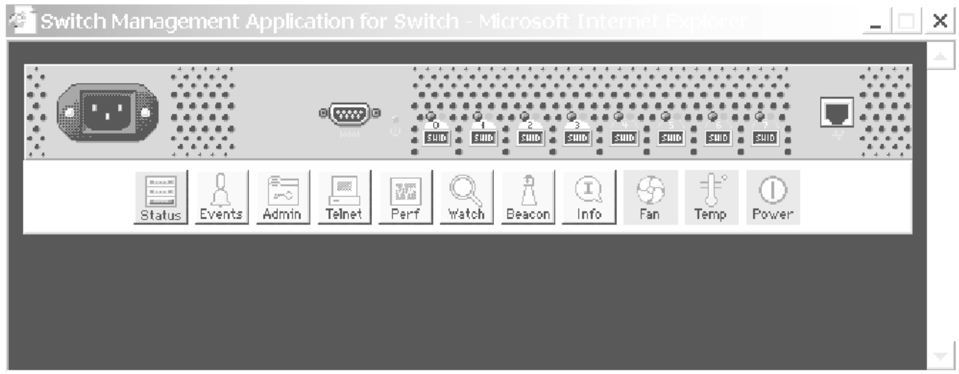
Switch status is calculated approximately once per second; however, the initial calculation does not occur until 30 - 60 seconds after the switch is started. It is calculated from the status of data structures in the switch, and is stored as the variable “switchStatus”.

Note: For all statuses that are based on errors per time interval, any errors cause the status to show faulty until the entire sample interval has passed.

For more information about the functions that are accessible through Fabric view, see “Fabric view” on page 49.

Switch view

Switch view is accessible from Fabric view, as shown in Figure 8 on page 41.



SJ000349

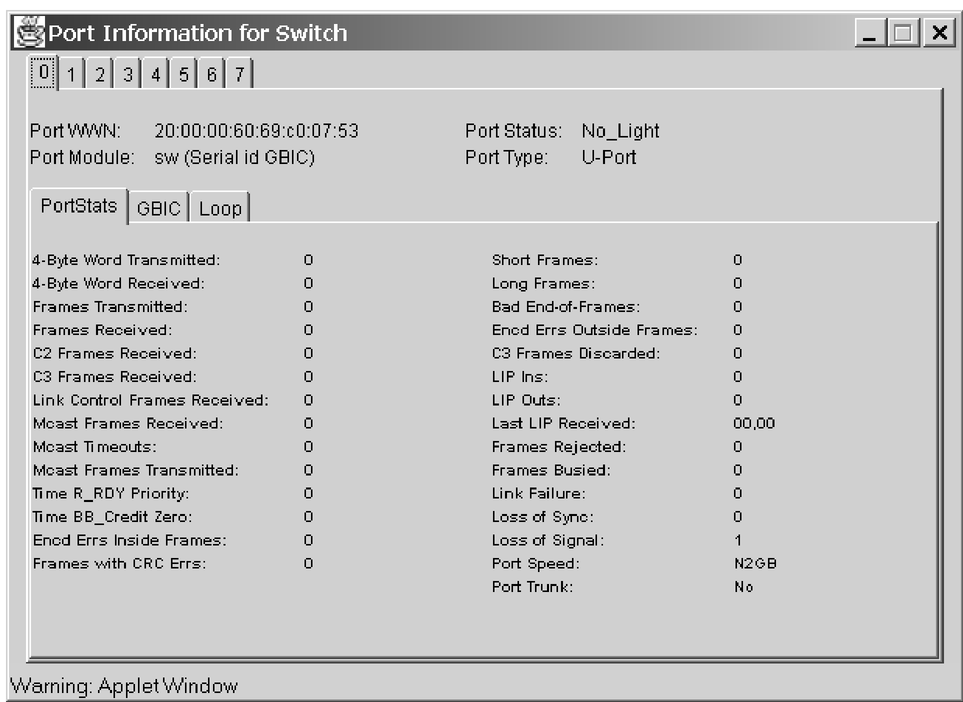
Figure 8. Switch view

The Switch view displays information about individual switches, including a real-time view of switch status. This information is accessed by selecting the Switch icon on a switch panel. The **Switch** view is also the launch point for the Switch Events view, the Telnet interface, the Fabric Watch view, the Administrative interface, the Performance view, and the Port Information view. It includes icons that display the status of the switch fans, temperature monitors, and beacon.

For more information about the functions that are accessible through the Switch view, see “Switch view” on page 84.

Port Information view

The Port Information view is accessible from the Switch view, as shown in Figure 9.



SJ000351

Figure 9. Port Information view

The Port Information view displays statistics and status for the selected port, GBIC, or loop. This information is accessed by selecting the icon for the relevant port in Switch view.

For more information about the functions that are accessible through the Port Information view, see “Port Information view” on page 97.

Table 4 provides a summary of the views that TotalStorage Specialist provides access to, including information about the fabric through a number of separate windows.

Table 4. Summary of TotalStorage Specialist views

View	Description
Initial display upon launching TotalStorage Specialist	
Fabric view	Displays a control panel that provides access to fabric-wide options, a panel for each switch in the fabric, plus a legend that explains the meaning of the background colors on the **Switch** icons. Each panel contains an icon that represents the switch itself, in addition to icons for Switch Events and the Administrative and Telnet interfaces. The background color of the **Switch** icon represents the status of that particular switch or integrated fabric.
Accessible from the Fabric view:	
Fabric Events view	Displays the error log for the fabric, which is the combination of the error logs of all the switches in the fabric. Accessed by selecting the **Fabric Events** icon on the control panel.
Fabric Topology view	Displays physical configuration, including active domains, paths, and routing information. Accessed by selecting the **Fabric Topology** icon on the control panel.
Name Server Table view	Displays the Name Server Table for the fabric. Use to view information about the devices that are attached to the fabric. Accessed by selecting the **Name Server** icon on the control panel.
Zone Administration view	Provides an interface to zoning, including zone settings, zone aliases, QuickLoops, and zone configurations. Accessed by selecting the **Zone Admin** icon on the control panel. A switch must have a zoning license for this interface to be available.
Summary view/Detail view	Toggles between summarized and detailed versions of the Fabric view.
Switch view	Displays information about individual switches, including a real-time view of switch status. Accessed by selecting the **Switch** icon on a switch panel. The Switch view is also the launch point for the Switch Events view, the Telnet interface, the Fabric Watch view, the Administrative Interface, the Performance view, and the Port Information view. It includes icons that display the status of the switch fans, temperature monitors, and beacon.
Switch Events view	Displays the error log for the switch. Accessed by selecting the **Events** icon on the switch panel. This view can also be accessed through the Switch view (see “Switch Events view” on page 86).

Table 4. Summary of TotalStorage Specialist views (continued)

View	Description
Telnet Interface	Provides an interface for using Telnet commands for switch diagnostics, troubleshooting, and fabric management. Accessed by selecting the **Telnet** icon on the switch panel. This view can also be accessed through the Switch view (see "Telnet interface" on page 150).
Administrative Interface	Provides an interface for performing functions such as upgrading firmware versions or reconfiguring a switch. Accessed by selecting the **Admin** icon on the switch panel. This view can also be accessed through the Switch view (see "Administrative Interface" on page 126).
Accessible from the Switch view:	
Port Information view	Displays statistics and status for the selected port, GBIC, or loop. Accessed by selecting the icon for the relevant port in the Switch view.
Power Supply Status	Green indicates that the power supply is on.
Switch Events view	Displays the error log for the switch. Accessed by selecting the **Events** icon in the Switch view. This view can also be accessed through the Fabric view (see "Fabric view" on page 49).
Telnet Interface	Provides an interface for using Telnet commands for switch diagnostics, troubleshooting, and detailed fabric management. Accessed by selecting the **Telnet** icon in the Switch view. This view can also be accessed through the Fabric view (see "Fabric view" on page 49).
Fabric Watch view	Monitors fabric elements and displays error and performance counter status, issuing an alert when conditions are out of acceptable ranges. Accessed by selecting the **Watch** icon in the Switch view. A switch must have a Fabric Watch license for this interface to be available.
Fan icon	Indicates the number of fans in the switch that are within normal range by the changing color of the icon (see the color legend in "Fabric view" on page 49).
Administrative Interface	Provides an interface for performing functions such as upgrading firmware versions or reconfiguring a switch. Accessed by selecting the **Admin** icon in the Switch view. This view can also be accessed through the Fabric view (see "Fabric view" on page 49).
Performance view	Portrays real-time data throughput for each port and displays total switch bandwidth utilization through a graphic representation. Accessed by selecting the **Perf** icon in the Switch view.
Beacon icon	Select to turn the beacon, which is an indicator light on the front panel of the switch, on or off. Appearance of icon indicates whether beacon is lit.
Temperature icon	Indicates the number of temperature sensors in the switch that are within range by the changing color of the icon (see the color legend in "Fabric view" on page 49).

Installing TotalStorage Specialist

This section provides information about installing TotalStorage Specialist.

Installation requirements

The switch and the workstation must both meet specific requirements for the correct installation and operation of TotalStorage Specialist.

Switch requirements

TotalStorage Specialist can be used to manage switches that meet the following requirements:

- 3534 and 2109 series switches
- Fabric OS version 3.0 or later installed

Workstation requirements

The following items are required for the correct installation and operation of TotalStorage Specialist:

- Supported operating systems
  - Solaris 2.61 or later
  - Windows 95, 98, or 2000
  - Windows NT 4.0
- Adequate random access memory (RAM) (Windows operating systems only)
  - 128 MB for fabrics containing 21 switches or less
  - 256 MB for fabrics containing more than 21 switches
- 5 MB of free disk space
- A compatible Web browser
  - Netscape Communicator 4.51 or later
  - Internet Explorer 4.01 or later

    Note: The browser must be configured to work with TotalStorage Specialist. For information about how to do this, see "Installing a supported Web browser".
- The correct version of the Java™ plug-in for the operating system:
  - For Windows 95, 98, 2000, or NT, use Java plug-in version 1.2.2-006 or later.
  - For Solaris, use Java plug-in version 1.2.2-02 for Solaris, including the Java plug-in patch created by Sun Microsystems for Solaris.

Pre-installation steps

Before you install TotalStorage Specialist, you must do the following:

1. Install a supported Web browser.
2. Configure the Web browser.
3. Install the Java plug-in on the workstation.

Installing a supported Web browser

If you do not already have a Web browser installed, install one of the following browsers:

- Netscape Communicator 4.51 or later, available from the Web site at:

  www.netscape.com
- Internet Explorer 4.01 or later, available from the Web site at:

  www.microsoft.com

Configuring the Web browser

You must configure either Netscape Communicator or Internet Explorer with specific browser settings.

Configuring Netscape Communicator: The Web browser cache must be cleared after Fabric OS version 3.0 is installed. Some browsers use local cache copies of jar files and image files to improve performance (depending on the options that are selected in the browser), which can cause incorrect display in TotalStorage Specialist.

Perform the following steps to remove cached files from Netscape Communicator:

1. Select **Edit —> Preferences**.
2. Click **Advanced** in the left text box to expand it, then click **Cache**.
3. On the Cache panel, click **Clear Memory Cache**.
4. Click **Clear Disk Cache**.
5. Click **OK**.
6. Exit and relaunch the browser.

Configuring Internet Explorer: For TotalStorage Specialist with Internet Explorer to run correctly, you must clear the browser cache after installation, and specify the appropriate settings for browser refresh frequency and process model.

- The browser cache must be cleared after Fabric OS version 3.0 is installed. The browser can use local cache copies of jar files and image files to improve performance (depending on the options that are selected in the browser), which can cause incorrect display.

  Perform the following steps to remove cached files from Internet Explorer:

  1. Select **Internet Options** from the View menu if using Internet Explorer 4.x, or from the Tools menu if using Internet Explorer 5.x.
  2. Click the **General** tab.
  3. Click **Delete Files...** (under Temporary Internet Files).
  4. Click **OK**.
  5. Exit and relaunch the browser.
- Browser pages must be refreshed at every visit to ensure the correct operation of the Switch Admin feature.

  Perform the following steps to set the refresh frequency:

  1. Select **Internet Options** from the View menu if using Internet Explorer 4.x, or from the Tools menu if using Internet Explorer 5.x.
  2. Click the **General** tab.
  3. Click **Settings** (under Temporary Internet Files).
  4. Under Check for newer versions of stored pages, select **Every visit to the page**.
- The correct browser process model must be selected.

  Perform the following steps to select the browser process model:

  1. Select **View —> Internet Options** if using Internet Explorer 4.x, or **Tools —> Internet Options** if using Internet Explorer 5.x.
  2. Click the **Advanced** tab to expand the Browsing category.
  3. Under Browsing, select **Browse in a new process** if using Internet Explorer 4.x, or **Launch browser windows in a separate process** if using Internet Explorer 5.x.

Installing the Java plug-in on the workstation

A Java plug-in must be installed on the workstation for the correct operation of TotalStorage Specialist. The required plug-in version depends on the operating system.

Installing the Java plug-in on a Solaris workstation: Solaris workstations require both the Java plug-in version 1.2.2-02 for Solaris and the patch created by Sun Microsystems for use with the Java plug-in on Solaris.

Perform the following steps to install the Java plug-in on Solaris:

1. Locate the Java plug-in at the Sun Microsystems Web site at:

   www.sun.com
2. Follow the instructions to install the Java plug-in for Solaris.
3. Open the .cshrc file and set the path to the Java plug-in executable file. For example, the following could be added to the .cshrc file:

   ```
   NPX_PLUG-IN_PATH=/opt/NSCPcom/plug-in
   export NPX_PLUG_IN_PATH
   ```

Perform the following steps to install the patch on Solaris:

1. Go to the Sun Web site at:

   www.sun.com
2. Using the SEARCH option, type the string `108593` in the search field and press Enter.
3. Follow the link to download the patch.
4. Exit the browser when the download is complete.
5. Install the patch.
6. Restart the system.
7. Relaunch the browser.
8. Enter the IP address of the switch.

Installing the Java plug-in on a Windows workstation: Windows 95, 98, 2000 and NT workstations require Java plug-in version 1.2.2-006 or later.

Perform the following steps to determine the version of the Java plug-in that is installed on the Windows workstation:

1. Launch the Java plug-in Control Panel from **Start —> Programs —> Java plug-in Control Panel**.
2. Turn on the Java console.
3. Launch the Web browser.
4. Type the name or IP address of a switch running Fabric OS version 2.2 or later and press Enter.

   The switch launches the Java plug-in console, displaying the Java plug-in version that is currently installed.

If the correct version of TotalStorage Specialist is installed, it is ready to use. If the correct version of TotalStorage Specialist is not installed, perform the following steps to install it:

1. If no Java plug-in is installed:
   a. Point the browser towards a switch running Fabric OS version 3.0.
   b. Follow the link to the Sun Microsystems Web site.

c. Download the correct Java plug-in.
d. Double-click the downloaded file to install the plug-in.
2. If an outdated version of the Java plug-in is currently installed:
   a. Uninstall the outdated version.
   b. Relaunch the browser.
   c. Type the address of a switch running Fabric OS version 3.0 or later.
   d. Follow the link to the Sun Microsystems Web site.
   e. Download the new Java plug-in.

Installing TotalStorage Specialist on the switch

TotalStorage Specialist can be installed either through Telnet or from the Web browser. Installing TotalStorage Specialist requires installing a license on each switch that will be managed from TotalStorage Specialist.

To determine whether a license is already installed on a switch, see "Installing TotalStorage Specialist through Telnet" and "Installing TotalStorage Specialist from the Web browser" on page 48. If a license is not installed, contact your switch supplier to obtain a license key.

Installing TotalStorage Specialist through Telnet

To install TotalStorage Specialist through Telnet:

1. Login to the switch through Telnet, using an account that has administrative privileges.
2. Type `licenseShow` on the Telnet command line to determine whether a TotalStorage Specialist license is already installed on the switch .

   A list of all the licenses that are currently installed on the switch displays. For example:

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

   If the TotalStorage Specialist license is correctly listed, the feature is installed and is immediately available.

   If the TotalStorage Specialist license is not included in the list or is incorrect, continue with step 3.
3. Type the following on the command line:

   `licenseAdd "key"`

   where `"key"` is the license key. 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 TotalStorage Specialist license is not listed, repeat step 3.

   Note: The Java plug-in must also be installed on the client machine to access TotalStorage Specialist.

Installing TotalStorage Specialist from the Web browser

If none of the switches in the fabric have a TotalStorage Specialist license, a license dialog is automatically displayed when you access any of the switches from the Web browser. If the fabric already contains at least one licensed switch, you can use TotalStorage Specialist to view and license other switches from the licensed switch.

Perform the following steps to install the first license from the Web browser:

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

   If a license is already installed on the switch, TotalStorage Specialist launches. If no license is installed, a license dialog displays.
3. If the license dialog displays, follow the instructions in the dialog.

Perform the following steps to install additional licenses from the Web browser:

1. Launch the Web browser.
2. Type the name or IP address of the licensed switch in the **Location/Address** field (for example: `http://111.222.33.1`) and press Enter. TotalStorage Specialist opens, displaying the Fabric view.
3. Click the icon for the switch that you want to license. A licensing window opens.
4. Follow the instructions in the licensing window.

Launching TotalStorage Specialist

You can launch TotalStorage Specialist after the license is installed on the switch and the Java plug-in is installed on the client machine.

Perform the following steps to launch TotalStorage Specialist:

1. Launch the Web browser.
2. Type the switch name or IP address in the **Location/Address** field and press Enter.

TotalStorage Specialist launches, displaying the Fabric view.

Using TotalStorage Specialist

This section describes the views and interfaces that are available through TotalStorage Specialist. These views and interfaces are:

- Fabric view
- Fabric Events view
- Fabric Topology view
- Name Server Table view
- Zone Administration view (optional software)
- Switch view
- Switch Events view
- Fabric Watch view (optional software)
- Port Information view
- Administrative interface
- Telnet interface

Note: Switches can be accessed using different methods, such as from the front panel, Telnet, SNMP, and the Web browser, any of which can occur simultaneously. To verify that modifications are correctly applied, ensure that the switch is modified from only one connection at a time.

Fabric view

The Fabric view is the first view that displays when you connect to a switch. It provides access to specific information about each switch, in addition to other options and a legend explaining the colors used to indicate switch status. Every switch in the fabric, including any unlicensed switches, is represented by a switch panel in the Fabric view. However, only switches with a TotalStorage Specialist license can be managed from TotalStorage Specialist. To add a license for an unlicensed switch, select the corresponding **Switch** icon in Fabric view, and a license window automatically displays.

Perform the following steps to launch TotalStorage Specialist and access the Fabric view:

1. Launch the Web browser.
2. Type the switch name or IP address in the **Location/Address** field and press Enter.

   Note: This switch is assumed to be the local domain. For information that is specific to QuickLoop to be available, the QuickLoop switch must be the host domain.

TotalStorage Specialist launches, displaying Fabric view. The Fabric view consists of two logical parts:

- The Control panel
- The Switch panel

Figure 10 on page 50 shows the full detail version of the Fabric view.

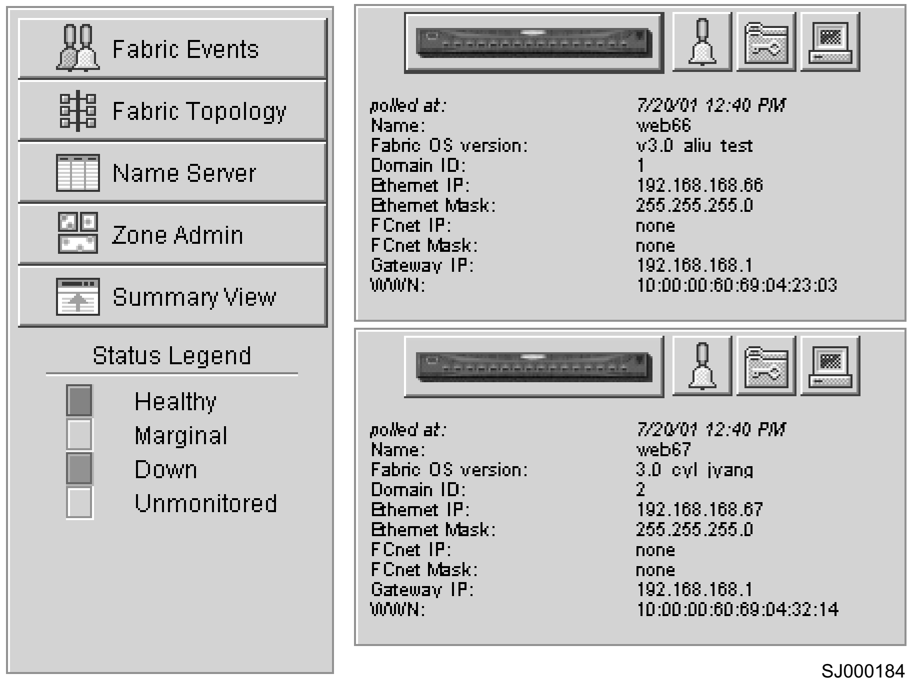


Figure 10. Detailed version of the Fabric view

To see the Summary version of the Fabric view, click **Summary View** on the left side of the Fabric view.

Figure 11 shows the summary version of the Fabric view.

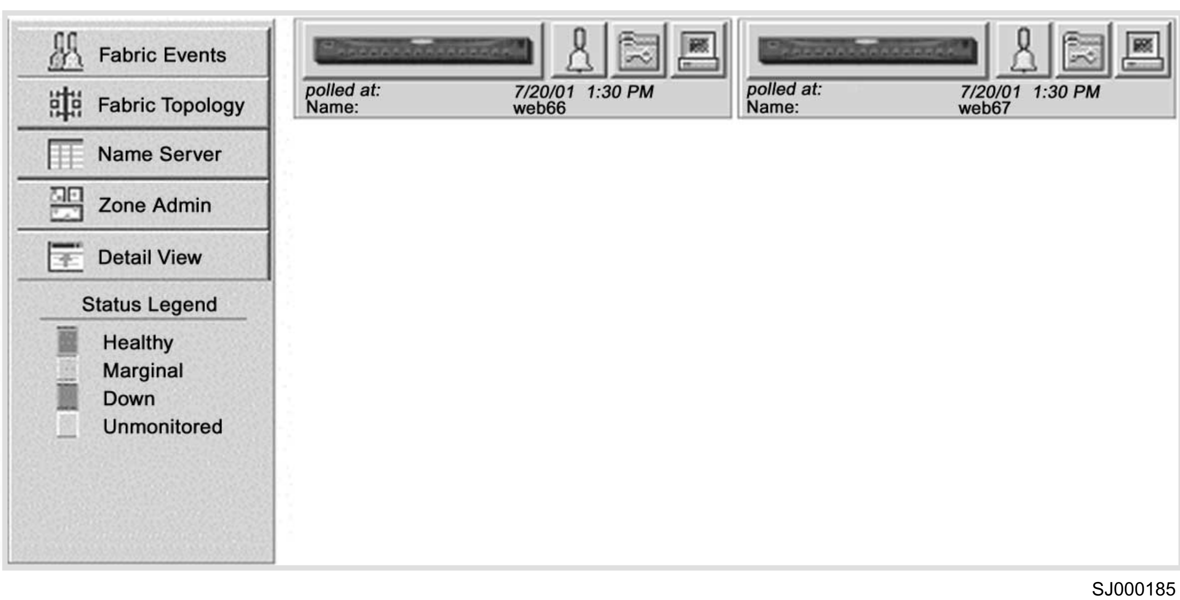


Figure 11. Summary version of the Fabric view

Table 5 on page 51 describes the buttons that are displayed in the Control panel portion (left side) of the Fabric view.

Table 5. Control panel of the Fabric view

Button	Description
Fabric Events	Select to open the Fabric Events view. The Fabric Events view provides a running log of events in the fabric. For additional information, see "Fabric Events view" on page 52.
Fabric Topology	Select to open the Fabric Topology view. The Fabric Topology view summarizes the physical configuration of the fabric from the perspective of the local domain (the domain of the switch entered as a URL in the Web browser). For additional information, see "Fabric Topology view" on page 53.
Name Server	Select to open the Name Server Table view. The Name Server Table view provides the name server entries listed in the Simple Name Server database. For additional information, see "Name Server Table view" on page 55.
Zone Admin	Select to open the Zone Administration view. This view is available only if a zoning license is installed. For additional information, see "Zone Administration view (optional software required)" on page 57.
Summary and Detail View	Toggle to view either the Summary or Detail version of the Fabric view. The Summary version shows abbreviated switch panels. The default view is Detail.
Status Legend	Defines the meaning of the colors that are visible in the background of the switch icons. Each color indicates a different operational state: **Green** Healthy **Yellow** Marginal (mix of good and faulty readings) **Red** Down (more than two faulty readings) **Gray** Unknown or unmonitored If no data is available from a switch, the most recent background color remains displayed. **Note:** For all statuses that are based on errors per time interval, any error causes the status to show faulty until the entire sample interval has passed.

Table 6 describes the icons and fields that are displayed in the Switch panel portion (right side) of the Fabric view.

Table 6. Switch panel of the Fabric view

Icon or field	Description
Switch icon	Select to open the Switch view for the switch. Each switch type is represented by a different icon. The background color around the icon indicates the status of the switch. For more information about this view, see "Switch view" on page 40.

Table 6. Switch panel of the Fabric view (continued)

Icon or field	Description
Events icon	Select to open the Switch Events view. The Switch Events view displays the switch events log. For more information about this view, see "Switch Events view" on page 86.
Admin icon	Select to open the Switch Administration view. For more information about this view, see "Administrative Interface" on page 126.
Telnet icon	Select to launch the Telnet Interface for the switch. For more information about this view, see "Telnet interface" on page 150.
polled at: or unreachable since:	Time of the last status check, or if currently unavailable, the time of the last successful status check.
Name:	The name of the switch.
Fabric OS version:	The version of Fabric OS installed on the switch.
Domain ID:	A number that uniquely identifies the switch within the fabric.
Ethernet IP:	The Ethernet IP address.
Ethernet Mask:	The Ethernet subnetmask.
FCnet IP:	The fibre-channel IP address.
FCnet Mask:	The fibre-channel subnetmask.
Gateway IP:	The gateway IP address.
WWN:	Unique numeric identifier for the switch; assigned by the manufacturer.

Fabric Events view

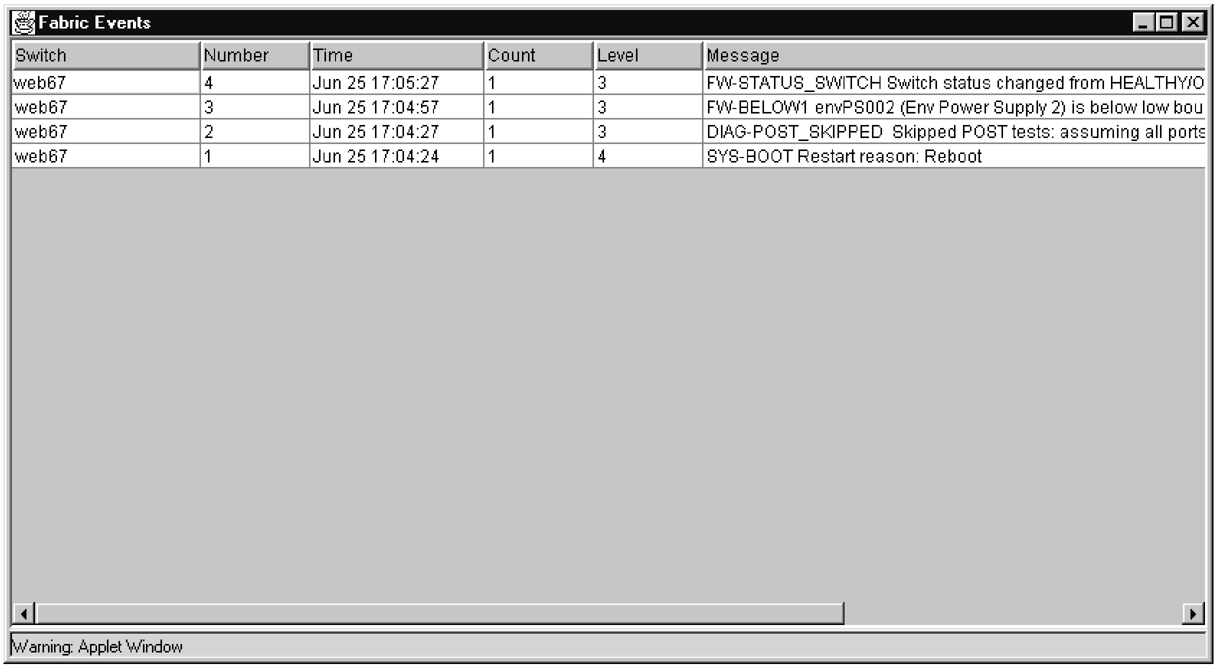
The Fabric Events view provides a running log of events for all switches in the fabric.

Perform the following steps to access the Fabric Events view:

1. Launch the Web browser.
2. Type the switch name or IP address in the **Location/Address** field and press Enter.

   TotalStorage Specialist launches, displaying the Fabric view.
3. Click **Fabric Events**.

   The Fabric Events view displays, as shown in Figure 12 on page 53.



SJ000186

Figure 12. Fabric Events view

Note: To sort the events by a particular column, click the column header. To resize a column, drag the column divider.

Following is a description of the fields in the Fabric Events view.

Switch
The name of the switch.

Number
The event number for the affected switch.

Time The time of the event.

Count The number of consecutive occurrences of the same event.

Level The severity level of the event. Valid levels are:

0 panic (switch restarts)

1 critical

2 error

3 warning

4 information

5 debug

Message
A description of the event.

Fabric Topology view

The Fabric Topology view summarizes the physical configuration of the fabric from the perspective of the local domain (the domain of the switch entered as a URL in the Web browser). This includes information about the destination domains (all other domains in the fabric) and the paths between each destination domain and the local domain.

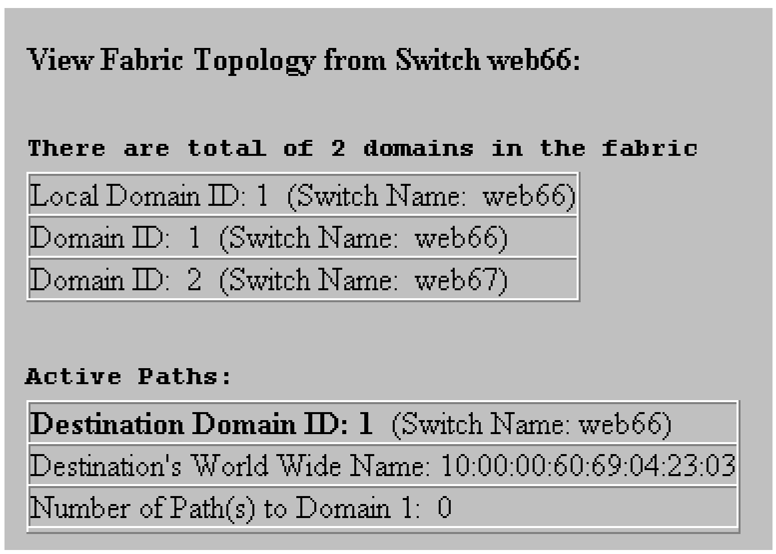
Perform the following steps to access the Fabric Topology view:

1. Launch the Web browser.
2. Type the switch name or IP address in the **Location/Address** field and press Enter.

   Note: The switch entered into the Web browser is identified by TotalStorage Specialist as the local domain.

   TotalStorage Specialist launches, displaying the Fabric view.
3. Click **Fabric Topology**.

   The Fabric Topology view displays, as shown in Figure 13.



SJ000187

Figure 13. Fabric Topology view

Following is a description of the fields in the Fabric Topology view.

View Fabric Topology from Switch [switch name]
: Lists the switch in the domain that is assumed to be the local domain.

There are a total of [n] domains in the fabric
: The number of domains in the fabric.

Local domain ID
: A number that uniquely identifies the local switch within the fabric, and the name of the switch.

Domain ID (can be more than one)
: A number that uniquely identifies the switch within the fabric, and the name of the switch.

Active Paths
: This line is followed by information about each destination domain, including information about each of the paths between that domain and the local domain.

Destination Domain ID
The ID of the destination domain that is described in the lines following the ID. This information and the two lines following it are displayed for each destination domain in the fabric.

Destination's World Wide Name
The WWN of the destination domain.

Number of Paths:
The number of active paths between the destination domain and the local domain.

Name Server Table view

The Name Server Table view provides the name server entries listed in the Simple Name Server database. This includes all name server entries for the fabric, not only those that are local to the local domain. Each row in the table represents a different device.

Perform the following steps to access the Name Server Table view:

1. Launch the Web browser.
2. Type the switch name or IP address in the **Location/Address** field and press Enter.

   TotalStorage Specialist launches, displaying the Fabric view.
3. Click **Name Server**.

The Name Server Table view displays, as shown in Figure 14 on page 56.

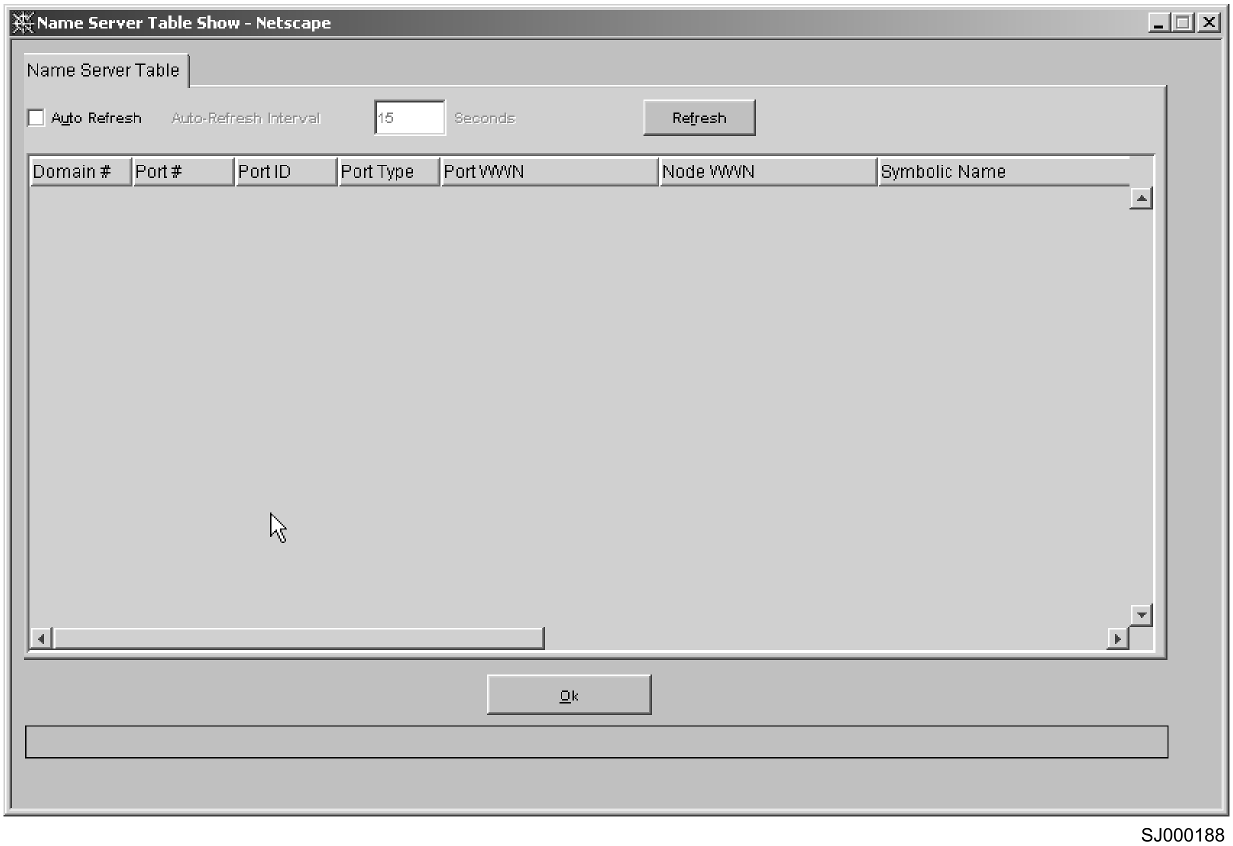


Figure 14. Name Server Table view

Note: To sort the events by a particular column, click the column header. To resize a column, drag the column divider.

Following is a description of the fields in the Name Server Table view:

Auto Refresh
Select to enable Auto Refresh or clear to disable.

Auto Refresh Interval
If Auto Refresh is selected, type the number of seconds for the refresh interval.

Refresh
Click to refresh the window immediately.

OK Click to close the window.

Domain #
The domain ID of the switch to which the device is connected.

Port # The number of the switch port to which the device is connected.

Port ID
The port ID of the device (24-bit hexadecimal value).

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

Port WWN
The worldwide name of the device port.

Node WWN
The worldwide name of the device node.

Symbolic Name
The symbolic name of the device assigned through the SCSI Inquiry command.

FC4 Types
The fibre-channel FC4 layer types that are supported by the device, such as IP or fibre channel protocol (FCP).

COS The fibre-channel classes of services that are supported by the device.

Fabric Port Name
The name of the fabric port in use by the device.

Port IP Address
The IP address of the fabric port.

Hard Address
The hard address of the fabric port.

Member of Zones
The zones to which this device belongs. This column is not updated when the table is refreshed. To view updated zoning information, close and reopen the Name Server Table view.

Zone Administration view (optional software required)

A zoning license and administrative privileges are required to access this view. If a switch or device is added or removed from the network, it is necessary to save the changes and relaunch the Zone Administration view for the changes to take effect.

When administering zoning, the following tasks should be performed:

1. Define zone aliases to establish groupings.
2. Add zone members.
3. Place zones into one or more zone configurations.
4. Enable one of the zone configurations (only one can be enabled at a time).

There are three separate methods for adding members to a zone. Each method corresponds to a zoning mode, and the combination of the methods corresponds to an additional mode. After a mode is selected, all operations on zones must use the zoning object selected. Zoning operations must correspond to that mode, and any zones, aliases, and configuration files which do not correspond cannot be selected.

For more information about using Zoning, see Chapter 10, “Zoning” on page 253.

Perform the following steps to access the Zone Administration view:

1. Launch the Web browser.
2. Type the switch name or IP address in the **Location/Address** field and press Enter.

   This switch is assumed to be the local domain.

   Note: For information that is specific to QuickLoop to be available, the QuickLoop switch must be the local domain.

   TotalStorage Specialist launches, displaying the Fabric view.
3. Click **Zone Admin**.

   A prompt displays, requesting that you enter a user name and a password, as shown in Figure 15.

Figure 15. Enter Network Password menu

4. Type a user name and a password.
5. Click **OK**.

   The Zoning Selection menu displays, as shown in Figure 16 on page 59.

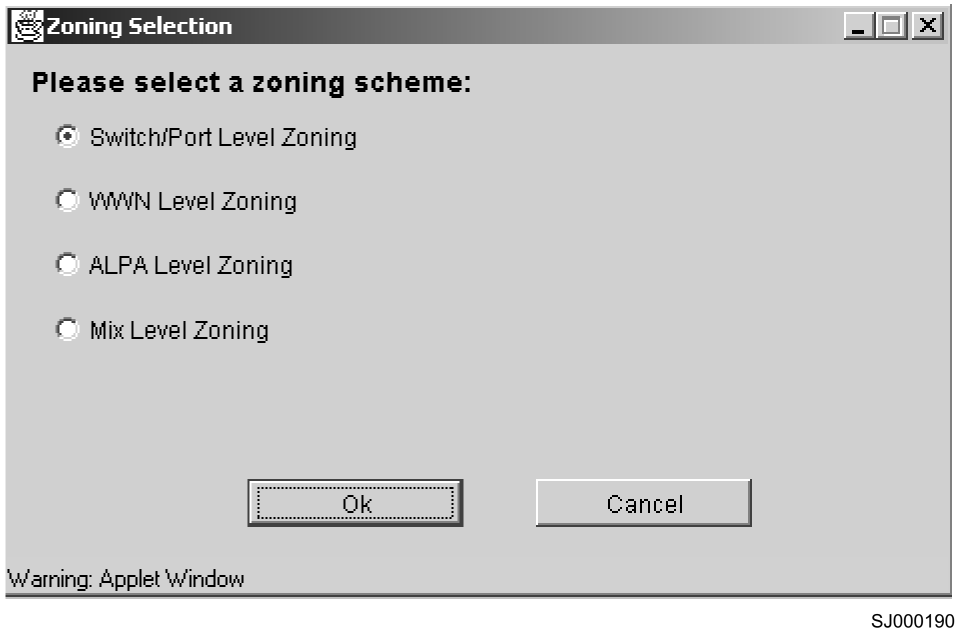


Figure 16. Zoning Selection menu

Following is a description of the zoning schemes contained in the Zoning Selection menu.

Switch/Port Level Zoning
All alias, zoning, and configuration file operations must be on ports. Aliases, zones, and configuration files which have objects other than ports cannot be selected or operated on.

WWN Level Zoning
All aliases, zoning, and configuration file operations must be on WWNs. Aliases, zones, and configuration files which have objects other than WWNs cannot be selected or operated on.

ALPA Level Zoning
All aliases, zoning, and configuration file operations must be on AL_PA in a QuickLoop. Aliases, zones, and configuration files which have objects other than AL_PAs in a QuickLoop cannot be selected or operated on.

Mixed Level Zoning
In this mode, any object can be selected to be a member of a zone, alias, or configuration file.

Following is a detailed description of each of these zoning schemes.

Switch or port level zoning

To access the Switch/Port Level Zoning menu, select **Switch/Port Level Zoning** from the Zoning Selection menu. Click **OK**. The Switch/Port Level Zoning menu displays, as shown in Figure 17 on page 60.

The following is a list of the tabs in the Switch/Port Level Zoning menu:

- Port Alias
- Port Zone
- QuickLoop
- Port Config

Port Alias tab

The **Port Alias** tab shows only Domain/Ports that are in the fabric. This tab is used to configure zones that consist only of Domain/Ports and aliases that contain only Domain/Ports. The **Port Alias** tab is shown in Figure 17.

SJ000191

Figure 17. Port Alias tab of the Switch/Port Level Zoning menu

Following is a description of the fields in the **Port Alias** tab.

Alias Name
: Select an existing alias name to be modified from the drop-down list.

Create Alias
: Click to create a new alias. A new alias dialog displays. Type a new alias name that is unique. The new alias name cannot contain spaces.

Delete Alias
: Click to delete the alias that is selected in the **Alias Name** field. Deleting an alias automatically removes it from all zones.

Rename Alias
: Click to rename the alias that is selected in the **Alias Name** field. A dialog displays in which you can edit the alias name. Renaming an alias automatically renames it in all zones.

Member Selection List
This field contains a list of potential alias members, including switches, ports, WWNs, and QuickLoop AL_PAs.

Search Mem
Click to search for a switch name, WWN, alias, zone, QuickLoop, or FA zone in the **Member Selection List** field based on the type of objects that are displayed in that list.

Add Mem
Click to add the item that is selected in the **Member Selection List** field to the **Alias Members** list. You can add individual ports or an entire switch. If a switch is added, all ports on the switch are added. To add a device WWN, select either a node WWN (folder icon) or port WWN (blue circle icon) from the WWN sub-tree.

Remove Mem
Click to remove the member that is selected from the **Alias Members** list.

Add Sw, Port
Click to add a switch or port combination that currently is not part of the fabric.

[Alias name] Members
This field lists the members of the alias that is selected in the **Alias Name** field. The name of this list depends on the name of the selected alias. If no alias is selected, the name displays as Null Members.

Ref Zone
Click to refresh the local zoning database that was copied from the switch. This button automatically flashes red or gray if the fabric zoning data is changed by another client.

A/D WWN
Click to add or delete a WWN to or from all the aliases, zones, or FA zones that are defined.

Rpl WWN
Click to replace a WWN with another WWN in all aliases, zones, or FA zones that are defined.

OK Applies the changes to the switch and exits the menu.

Apply Click to apply all changes made since the Zone Administration view was opened, including changes made on other tabs in the view. Changes cannot be cancelled after they have been applied.

Close Click to exit the menu without making any changes to the switch.

Clr All Click to clear all aliases, zones, configurations, or FA zones locally on the switch.

Port Zone tab

Use the **Port Zone** tab for the following tasks:

- To specify which ports on a switch are to be in the selected zone
- To create zones
- To manage zones

A zone can have one or multiple members, and can include switches, ports, WWNs, aliases, and QuickLoop AL_PAs. The **Port Zone** tab is shown in Figure 18 on page 62.

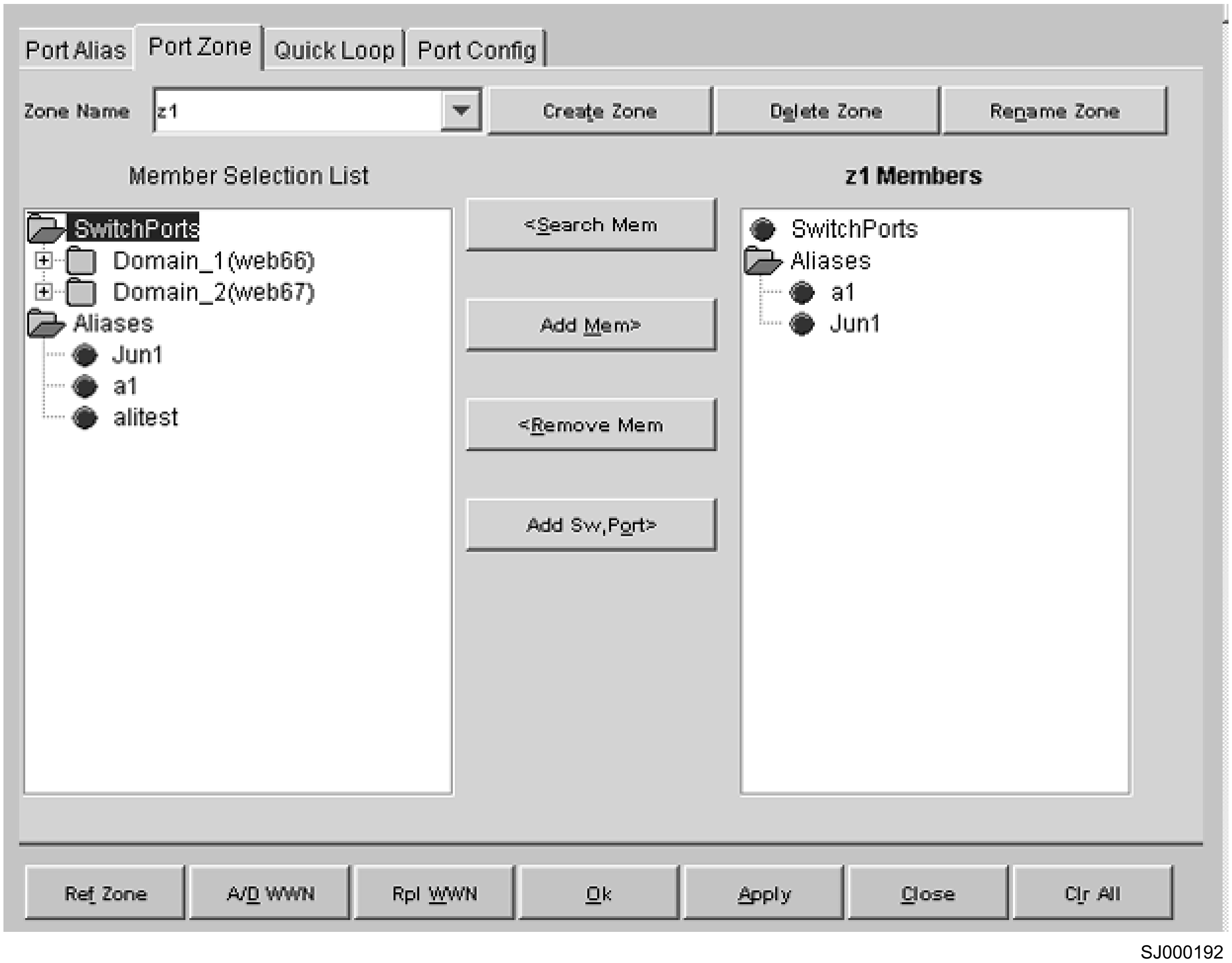


Figure 18. Port Zone tab of the Switch/Port Level Zoning menu

Following is a description of the fields in the **Port Zone** tab.

Zone Name
: Select an existing zone name to be modified from the drop-down list.

Create Zone
: Click to create a new zone. A dialog displays in which you can type the name of the new zone. All names must be unique and contain no spaces.

Delete Zone
: Click to delete the zone that is selected in the **Zone Name** field. Deleting a zone automatically removes it from all zone configurations.

Rename Zone
: Click to edit the name of the zone that is selected in the **Zone Name** field. A dialog displays in which you can edit the name of the zone.

Member Selection List
: A list of potential zone members, including switches, ports, WWNs, aliases, and QuickLoop AL_PAs.

Search Mem
: Click to search the list of potential zone members.

Add Mem
: Click to add the member that is selected in the **Member Selection List**

field to the **Zone Members** list. If an entire switch is selected, all ports on the switch are added to the zone. You can also select individual ports. To add a device WWN, select either a node WWN (folder icon) or port WWN (blue circle icon) from the WWN sub-tree. To add an alias to the zone, select it from the Aliases sub-tree (the alias must already exist).

Remove Mem
Click to remove the member that is selected from the **Zone Members** list.

Add Sw, Port
Click to add a switch or port combination that currently is not part of the fabric.

[Zone name] Members
This field lists the members of the zone that is selected in the **Zone Name** field. The name of this list depends on the name of the selected zone. If no zone is selected, the name displays as Null Members.

For a description of the **Ref Zone**, **A/D WWN**, **Rpl WWN**, **OK**, **Apply**, **Close**, and **Clr All** buttons, see “Port Alias tab” on page 60.

QuickLoop tab

A QuickLoop license is required to use this tab. You can use the **QuickLoop** tab to create and manage QuickLoops if used in conjunction with Zoning. For information on managing the QuickLoop feature separately, see “Loop tab” on page 104. The QuickLoop tab is shown in Figure 19 on page 64.

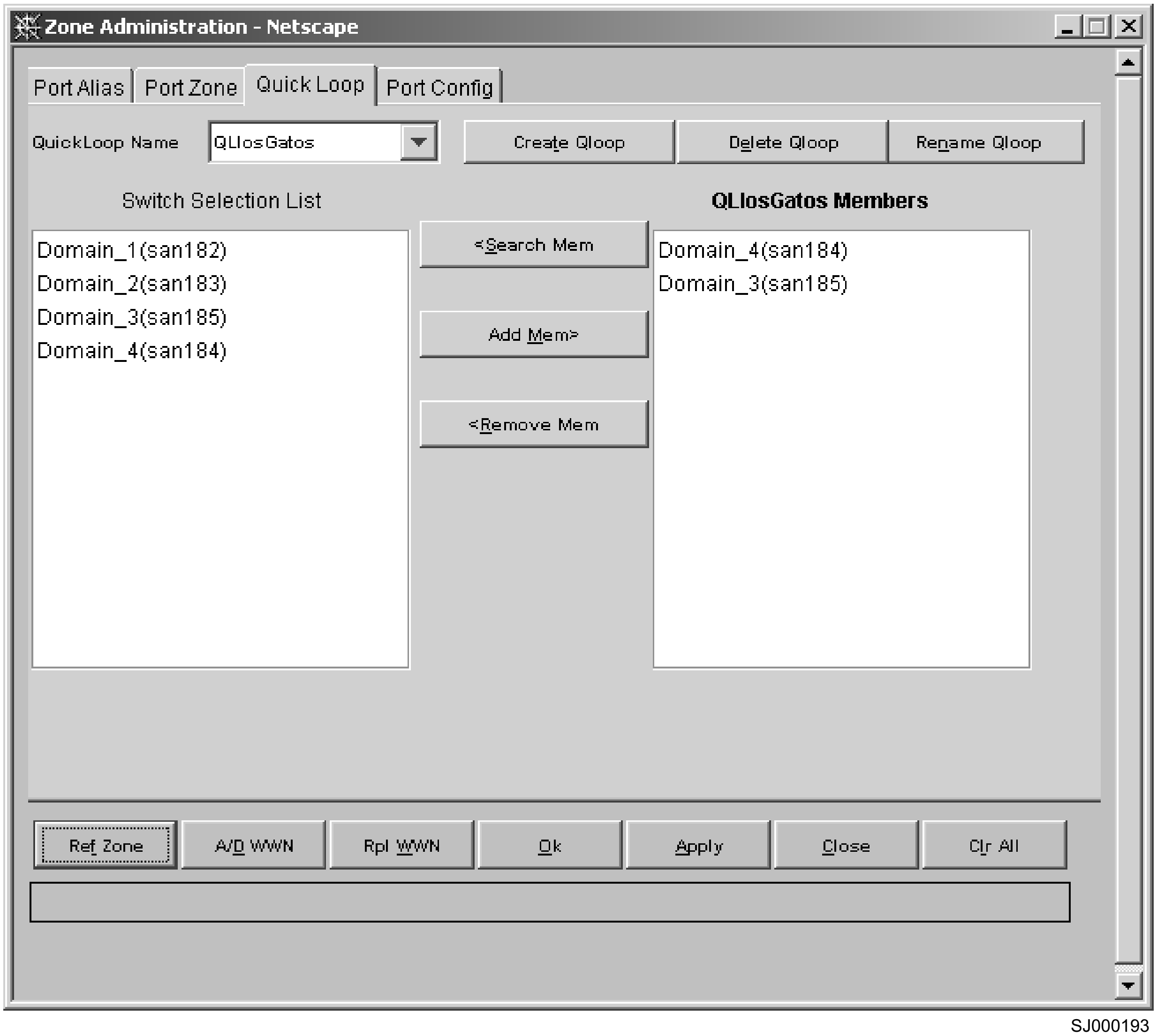


Figure 19. QuickLoop tab of the Switch/Port Level Zoning menu

Following is a description of the fields in the **QuickLoop** tab.

QuickLoop Name
Select a QuickLoop name to be modified from the drop-down list.

Create Qloop
Click to create a new QuickLoop. A dialog displays in which you can type the name of the new QuickLoop. All names must be unique and contain no spaces.

Delete Qloop
Click to delete the QuickLoop that is selected in the **QuickLoop Name** field. Deleting a QuickLoop automatically removes it from all aliases, zones, and zone configurations, including the associated AL_PAs.

Rename Qloop
Click to edit the name of the QuickLoop that is selected in the **QuickLoop Name** field. A dialog displays in which you can edit the name of the QuickLoop.

Switch Selection List
A list of the switches available to add to the QuickLoop.

Search Mem
Click to search for a switch name, WWN, alias, zone, QuickLoop, or FA zone in the **Switch Selection List** field based on the type of objects that are displayed in that list.

Add Mem
Click to add the switch that is selected in the **Switch Selection List** field to the **QuickLoop Members** list.

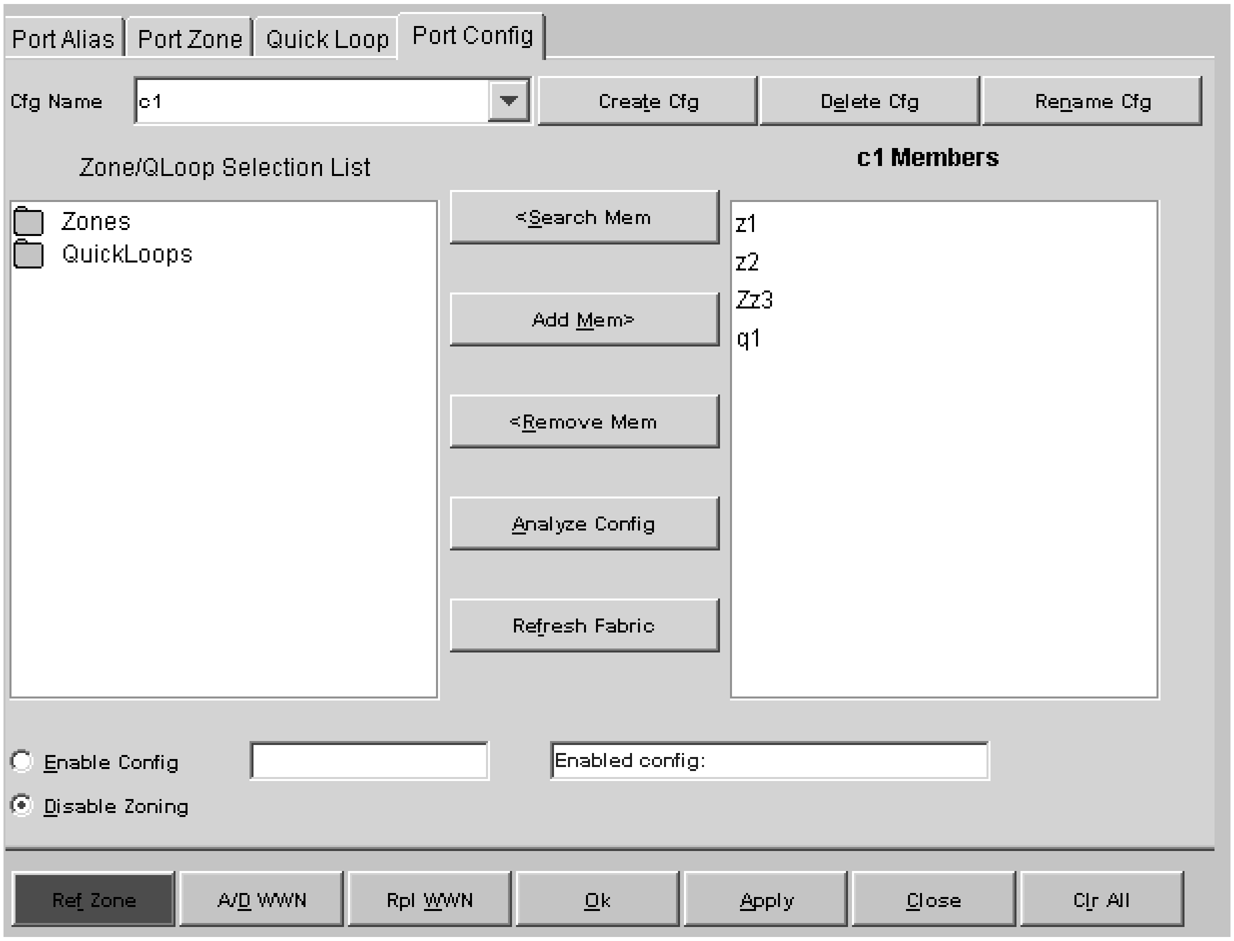
Remove Mem
Click to remove the member that is selected from the **QuickLoop Members** list.

[QuickLoop name] Members
A list of the members of the QuickLoop that is currently selected in the **QuickLoop Name** field. The name of this list depends on the name of the selected QuickLoop. If no QuickLoop is selected, the name displays as Null Members.

For a description of the **Ref Zone**, **A/D WWN**, **Rpl WWN**, **OK**, **Apply**, **Close**, and **Clr All** buttons, see “Port Alias tab” on page 60.

Port Config tab

Use the **Port Config** tab to create and manage zone configurations. Zone configurations are used to enable or disable a group of zones at the same time. The **Port Config** tab is shown in Figure 20 on page 66.



SJ000194

Figure 20. Port Config tab of the Switch/Port Level Zoning menu

Following is a description of the fields and buttons in the **Port Config** tab.

Cfg Name
Select an existing configuration to modify from the drop-down list.

Create Cfg
Click to create a new configuration. A dialog displays. Type the name of the new configuration. All names must be unique and contain no spaces.

Delete Cfg
Click to delete the configuration that is selected in the **Cfg Name** field.

Rename Cfg
Click to edit the name of the configuration that is selected in the **Cfg Name** field. A dialog in which you can edit the name of the configuration displays.

Zone/QLoop Selection List
This field provides a list of the zones and QuickLoops that are available to add to the configuration.

Search Mem
Click to search for a switch name, WWN, alias, zone, QuickLoop, or FA zone in the **Member Selection List** field based on the type of objects that are displayed in that list.

Add Mem
: Click to add the switch that is selected in the **Zone/QLoop Selection List** field to the **Config Members** list.

Remove Mem
: Click to remove the member that is selected from the **Config Members** list.

Analyze Config
: Click to analyze the configuration that is selected, along with its member zones and aliases. A zoning configuration error message is displayed in the event of a conflict.

Refresh Fabric
: Click to refresh the Fabric view with the latest Domain/Port and WWN changes.

[Config name] Members
: The members of the configuration that is selected in the **Cfg Name** field. The name of this list depends on the selection. Only one configuration can be enabled at a time; if none are enabled, zoning is not active in the fabric.

Enable Config
: Select to enable the configuration selected in the **Cfg Name** field or clear to disable the configuration.

Disable Zoning
: Select to disable zoning.

For a description of the **Ref Zone**, **A/D WWN**, **Rpl WWN**, **OK**, **Apply**, **Close**, and **Clr All** buttons, see "Port Alias tab" on page 60.

Zoning Configuration Analysis window

Click the **Analyze Config** button to view the Zoning Configuration Analysis window. This window displays a summary of the saved configuration and attempts to point out some of the zoning conflicts before applying the changes to the switch. Some of the potential errors it might catch are:

- Ports, WWNs, or devices that are part of the selected configuration, but not part of the fabric.
- Zones with only a single member.

WWN level zoning

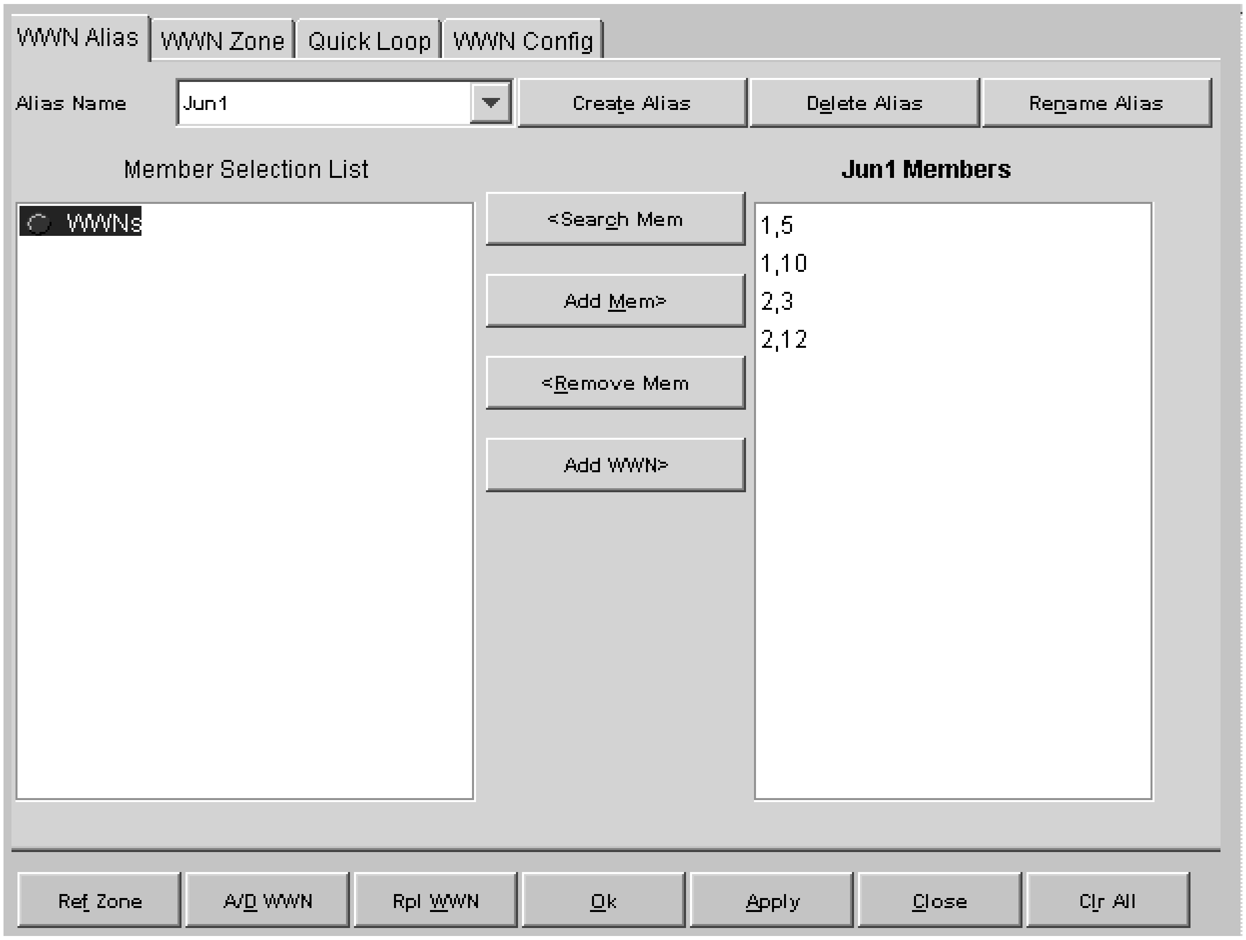
With WWN zoning, only worldwide names are displayed on the tabs. This window is used to configure aliases, zones, and configuration files. From the Zoning Selection menu, select **WWN Level Zoning** and click **OK**. The WWN Level Zoning menu displays, as shown in Figure 21 on page 68.

The following is a list of the tabs in the WWN Level Zoning menu:

- WWN Alias
- WWN Zone
- QuickLoop
- WWN Config

WWN Alias tab

Use the **WWN Alias** tab to configure WWN aliases. Figure 21 on page 68 shows the **WWN Alias** tab.



SJ000196

Figure 21. WWN Alias tab of the WWN Level Zoning menu

Following is a description of the fields in the **WWN Alias** tab.

Alias Name
Select an existing alias to modify from the drop-down menu.

Create Alias
Click to create a new alias. A dialog displays in which you can type the name of the new alias. All names must be unique and contain no spaces.

Delete Alias
Click to delete the alias that is selected in the **Alias Name** field. Deleting an alias automatically removes it from all zones.

Rename Alias
Click to rename the alias that is selected in the **Alias Name** field. A dialog displays in which you can edit the alias name. Renaming an alias automatically renames it in all zones.

Member Selection List
A list of potential alias members, including switches, ports, WWNs, and QuickLoop AL_PAs.

Search Mem
Click to add the item that is selected in the **Member Selection List** field to the **Alias Members** list. You can add individual ports or an entire switch. If

a switch is added, all ports on the switch are added. To add a device WWN, select either a node WWN (folder icon) or port WWN (blue-circle icon) from the WWN sub-tree.

Add Mem
Click to add the switch that is selected in the **Members Selection List** to the **Alias Members** list.

Remove Mem
Click to remove the selected member from the **Alias Members** list.

Add WWN
Click to add a WWN that currently is not part of the fabric.

[Alias name] Members
This field lists the members of the alias selected in the **Alias Name** field. The name of this list depends on the name of the selected alias. If no alias is selected, the name displays as Null Members.

For a description of the **Ref Zone**, **A/D WWN**, **Rpl WWN**, **OK**, **Apply**, **Close**, and **Clr All** buttons, see “Port Alias tab” on page 60.

WWN Zone tab

Use the **WWN Zone** tab to specify the members of the WWN zone. In this menu, only switches and WWN are available to be selected as members of the zone. The **WWN Zone** tab is shown in Figure 22 on page 70.

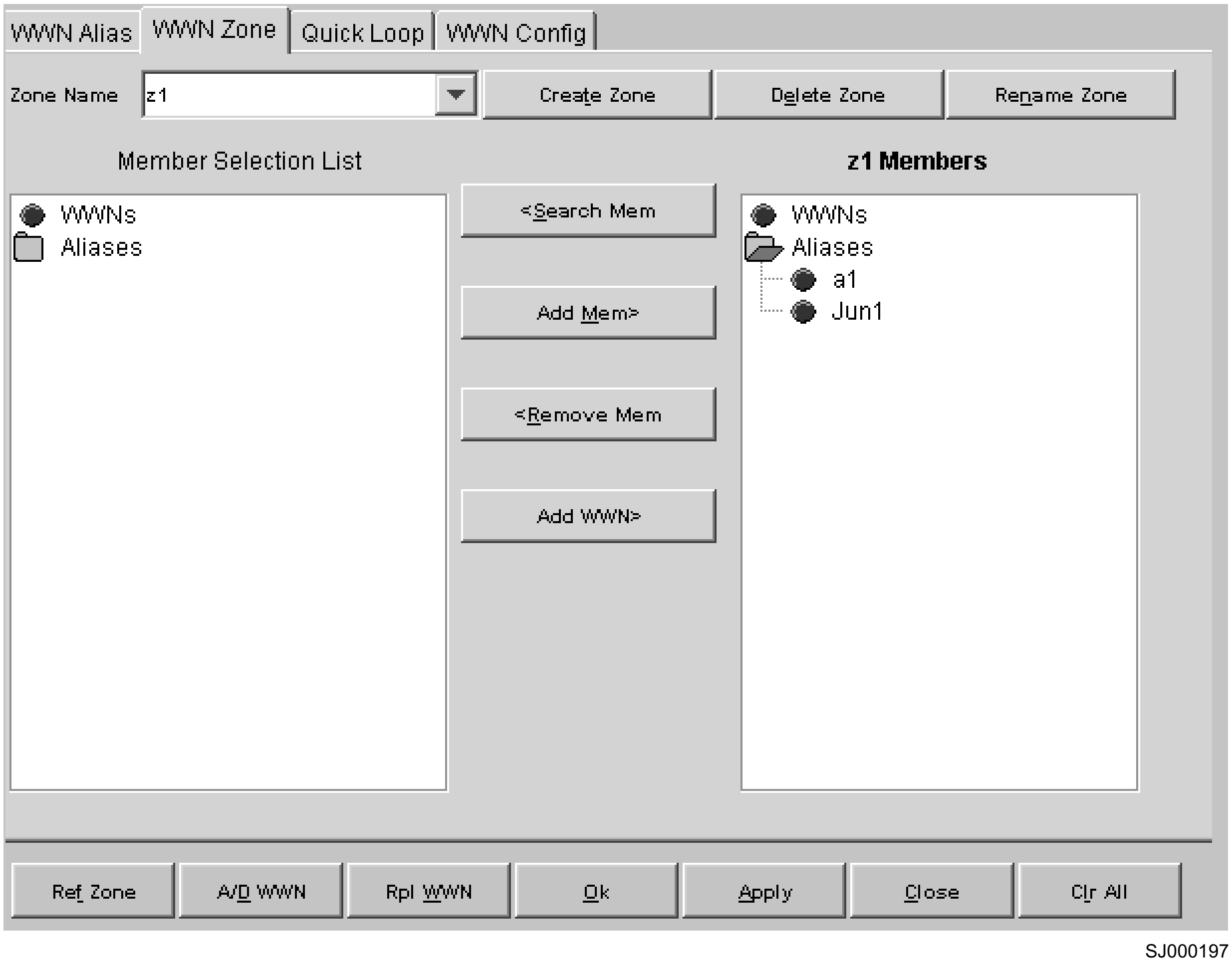


Figure 22. WWN Zone tab of the WWN Level Zoning menu

Following is a description of the fields in the **WWN Zone** tab.

Zone Name
Select an existing zone member to modify from the drop-down list.

Create Zone
Click to create a new zone member.

Delete Zone
Click to delete a zone member.

Rename Zone
Click to rename a zone member.

Member Selection List
This field displays a list of potential zone members, including switches, ports, WWNs, and QuickLoop AL_PAs.

Search Mem
Click to search for a switch name, WWN, alias, zone, QuickLoop, or FA zone in the **Member Selection List** field, based on the type of objects displayed in that list.

Add Mem
Click to add a member from the **Member Selection List** field into the **Zone Members** list.

Remove Mem
Click to remove a member from the **Zone Members** list.

Add WWN
Click to add a WWN that is not currently part of the fabric.

[Zone name] Members
This field lists the zone members selected in the **Zone Name** field. The name on this list depends on the name of the selected zone member. If a name is not selected, the name displays as Null Members.

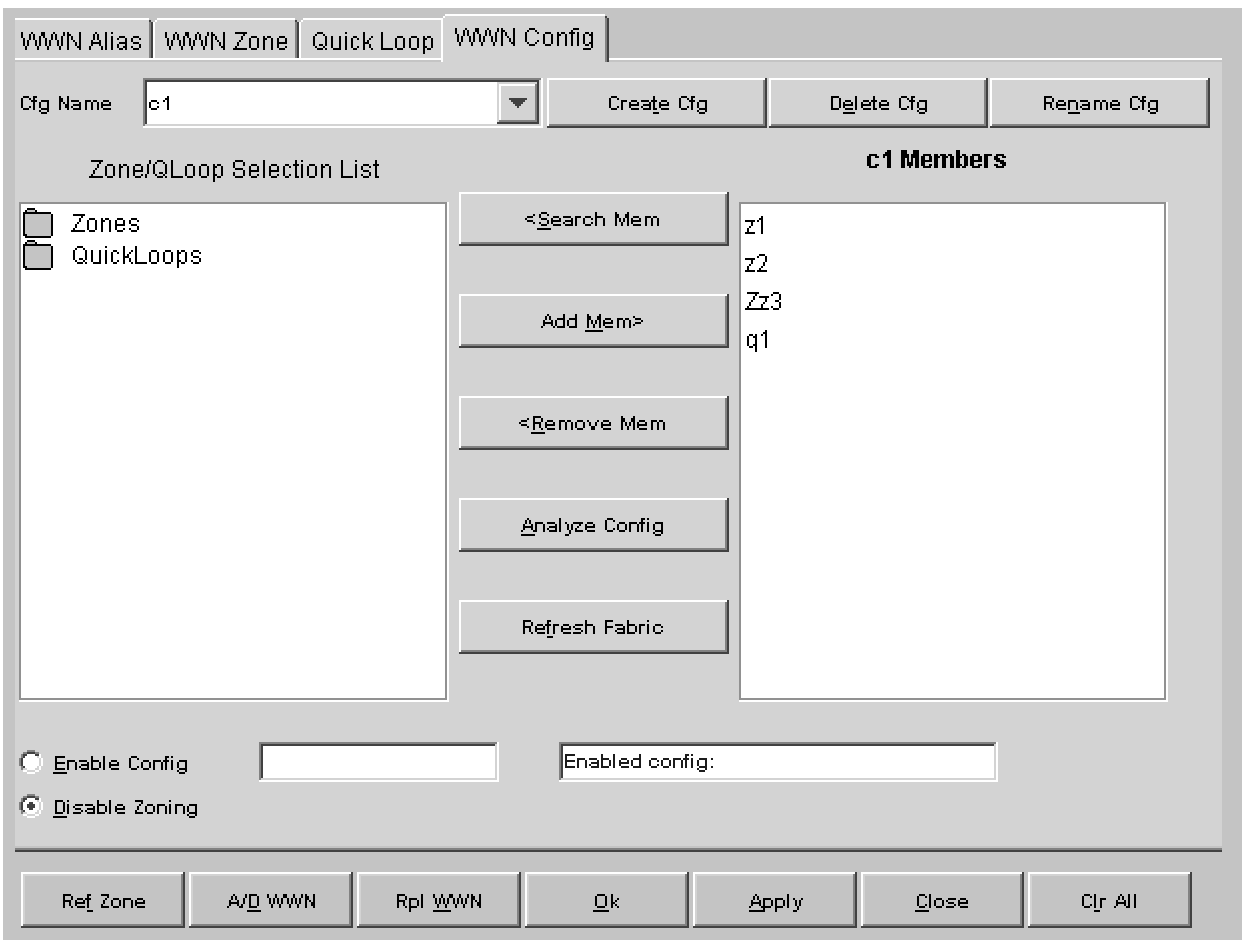
For a description of the **Ref Zone**, **A/D WWN**, **Rpl WWN**, **OK**, **Apply**, **Close**, and **Clr All** buttons, see “Port Alias tab” on page 60.

QuickLoop tab

A QuickLoop license is required to use this tab. You can use the **QuickLoop** tab to create and manage QuickLoops if used in conjunction with zoning. For information on managing the QuickLoop feature separately, see “Loop tab” on page 104. For a description of the **QuickLoop** tab, see “QuickLoop tab” on page 63.

WWN Config tab

Use the **WWN Config** tab to specify which zones comprise a WWN zone configuration file. The **WWN Config** tab is shown in Figure 23.



SJ000199

Figure 23. WWN Config tab of the WWN Level Zoning menu

Following is a description of the fields in the **WWN Config** tab.

Cfg Name
Select an existing WWN configuration name to be modified from the drop-down list.

Create Cfg
Click to create a new WWN configuration.

Delete Cfg
Click to delete a WWN configuration.

Rename Cfg
Click to rename a WWN configuration.

Zone/QLoop Selection List
This field displays a list of zone and QuickLoop members available to add to the WWN configuration.

Search Mem
Click to search for a switch name, WWN, alias, zone, QuickLoop, or FA zone in the **Zone Selection List** field, based on the type of objects displayed in that list.

Add Mem
Click to add a member from the **Zone Members** list field into the **Config Members** list.

Remove Mem
Click to remove a member from the **Zone Selection List**.

Analyze Config
Click to analyze the configuration that is selected along with its member zones and aliases. A Zoning Error window is displayed in the event of a conflict.

Refresh Fabric
Click to refresh the Fabric view with the latest domain, port, and WWN changes.

[Config name] Members
This field displays a list of the members that belong to the WWN configuration currently selected in the **Cfg Name** field. The name of this list depends on the name of the WWN configuration selected. If WWN configuration is not selected, the name displays as Null Members.

Enable Config
Select this option and click **Apply** to use the selected configuration for zoning the fabric.

Disable Zoning
Select this option and click **Apply** to disable the selected configuration for zoning the fabric.

For a description of the **Ref Zone**, **A/D WWN**, **Rpl WWN**, **OK**, **Apply**, **Close**, and **Clr All** buttons, see “Port Alias tab” on page 60.

AL_PA level zoning

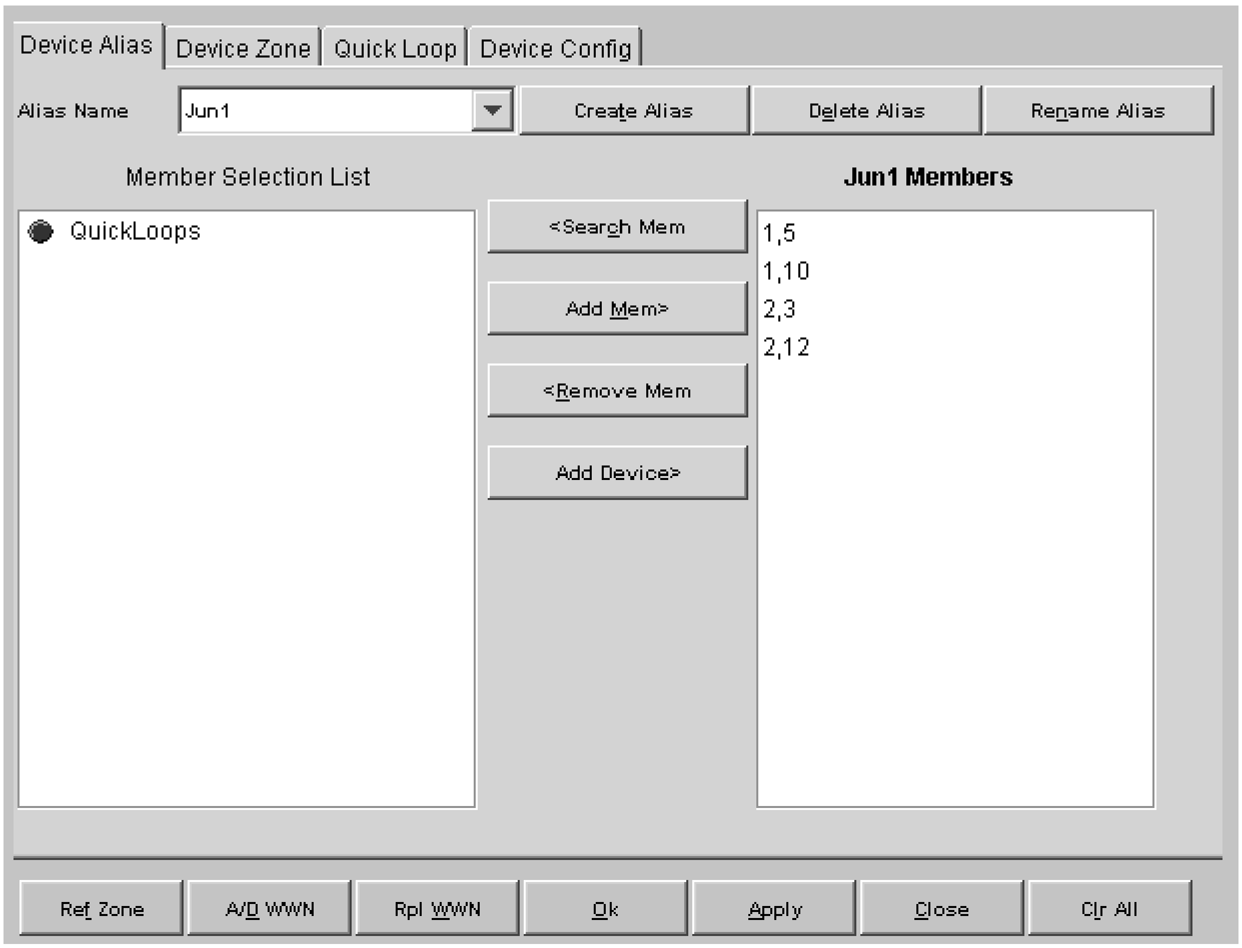
AL_PA level zoning is a replacement for QuickLoop zoning. With AL_PA level zoning, only members of a QuickLoop can be a member of the zone. Zone members are specified through their AL_PA. From the Zoning Selection menu, select **AL_PA Level Zoning** and click **OK**. The AL_PA Level Zoning menu displays, as shown in Figure 24 on page 73.

The following is a list of the tabs in the AL_PA Level Zoning menu:

- Device Alias
- Device Zone
- QuickLoop
- Device Config

Device Alias tab

Use the **Device Alias** tab to create and manage QuickLoop configurations. QuickLoop configurations are used to enable or disable a group of zones at the same time. The **Device Alias** tab is shown in Figure 24.



SJ000200

Figure 24. Device Alias tab of the AL_PA Level Zoning menu

Following is a description of the fields in the **Device Alias** tab.

Alias Name
: Select an existing alias name to modify from the drop-down list.

Create Alias
: Click to create a new alias. A dialog displays. Type the name of the new alias. All names must be unique and contain no spaces.

Delete Alias
: Click to delete the alias that is selected in the **Alias Name** field. Deleting an alias automatically removes it from all zones.

Rename Alias
Click to rename the alias that is selected in the **Alias Name** field. A dialog displays in which you can edit the alias name. Renaming an alias automatically renames it in all zones.

Member Selection List
This field displays a list of potential alias members, including switches, ports, WWNs, and QuickLoop AL_PAs.

Search Mem
Click to search for a switch name, WWN, alias, zone, QuickLoop, or FA zone in the **Member Selection List** field based on the type of objects displayed in that list.

Add Mem
Click to add a member from the **Member Selection List** field to the **Alias Members** list.

Remove Mem
Click to remove the selected member from the **Alias Members** list.

Add Device
Click to add a device that currently is not part of the fabric.

[Alias name] Members
This field lists the members of the alias selected in the **Alias Name** field. The name of this list depends on the name of the selected alias. If no alias is selected, the name displays as Null Members.

For a description of the **Ref Zone**, **A/D WWN**, **Rpl WWN**, **OK**, **Apply**, **Close**, and **Clr All** buttons, see “Port Alias tab” on page 60.

Device Zone tab

Use the **Device Zone** tab to select members of a device zone. Members are specified by their AL_PA. The **Device Zone** tab is shown in Figure 25 on page 75.

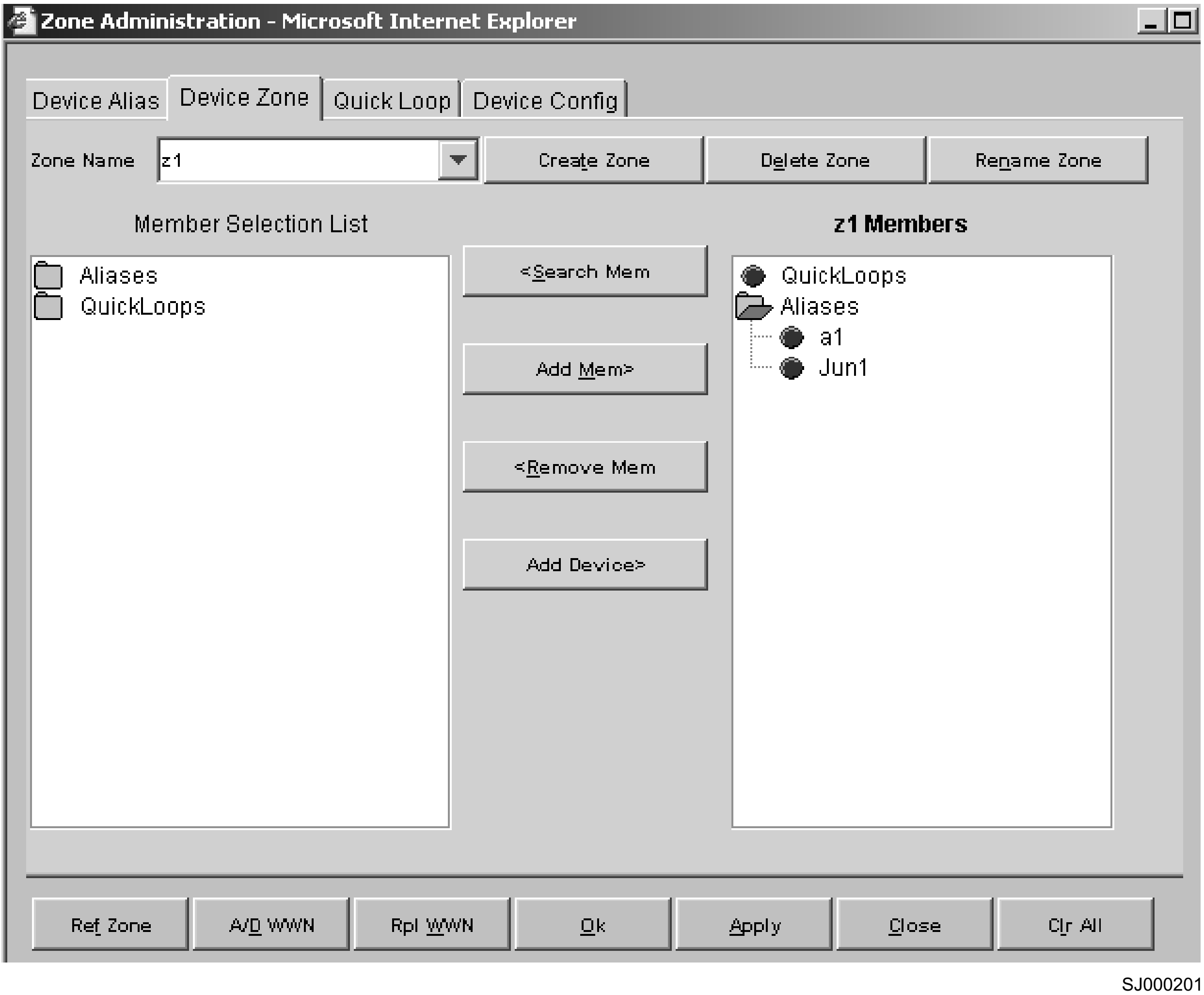


Figure 25. Device Zone tab of the AL_PA Level Zoning menu

Following is a description of the fields in the **Device Zone** tab.

Zone Name
: Select an existing zone member to modify from the drop-down list.

Create Zone
: Click to create a new zone member.

Delete Zone
: Click to delete a zone member.

Rename Zone
: Click to rename a zone member.

Member Selection List
: This field displays a list of potential zone members, including switches, ports, WWNs, and QuickLoop AL_PAs.

Search Mem
: Click to search for a switch name, WWN, alias, zone, QuickLoop, or FA zone in the **Member Selection List** field, based on the type of objects displayed in that list.

Add Mem
Click to add a member from the **Member Selection List** field into the **Zone Members** list.

Remove Mem
Click to remove a member that is selected from the **Zone Members** list.

Add Device
Click to add a device that currently is not part of the fabric.

[Zone name] Members
This field lists the zone members selected in the **Zone Name** field. The name on this list depends on the name of the selected zone member. If a name is not selected, the name displays as Null Members.

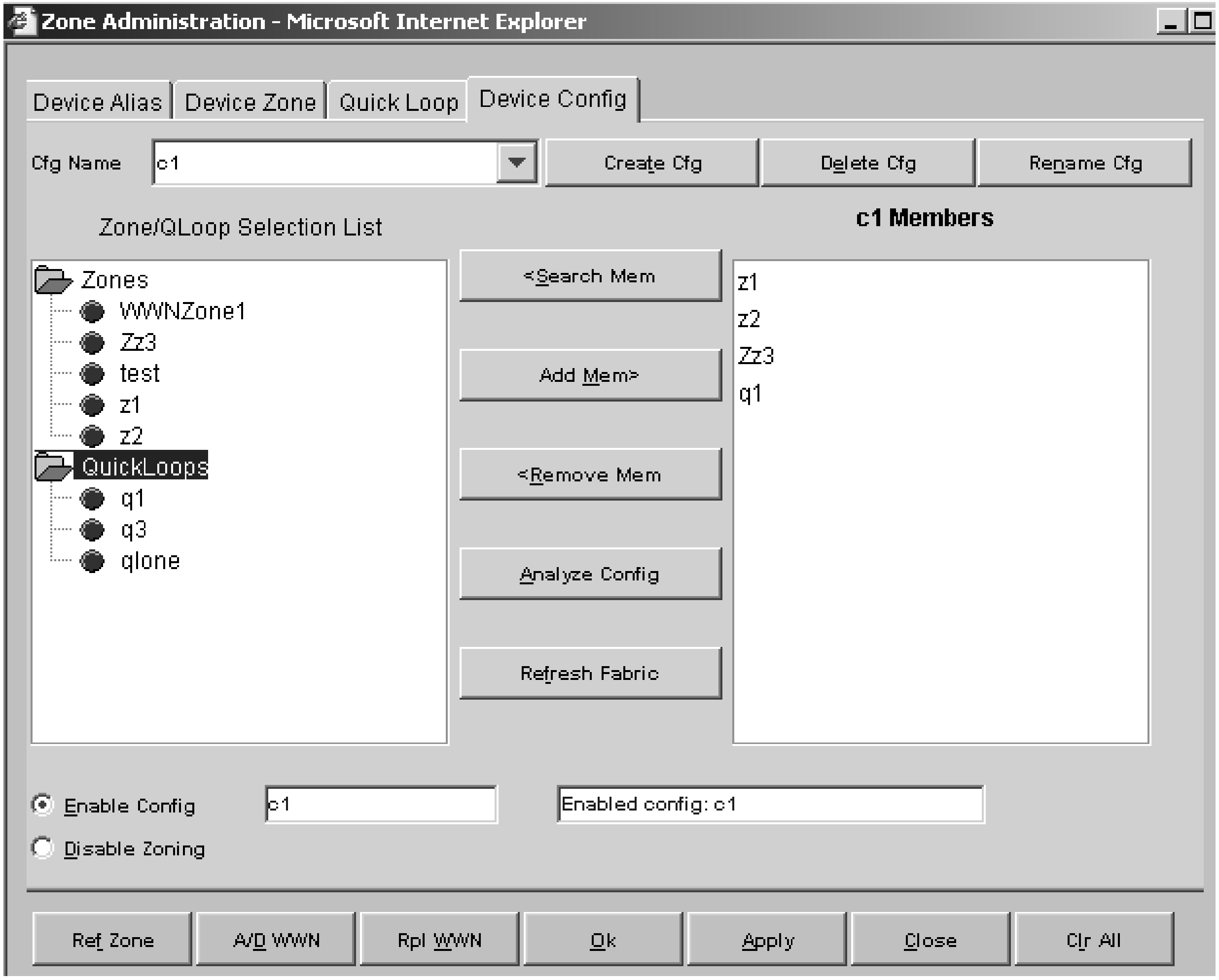
For a description of the **Ref Zone**, **A/D WWN**, **Rpl WWN**, **OK**, **Apply**, **Close**, and **Clr All** buttons, see “Port Alias tab” on page 60.

QuickLoop tab

A QuickLoop license is required to use this tab. Use the **QuickLoop** tab to create and manage QuickLoops. For information on managing the QuickLoop feature separately, see “Loop tab” on page 104. For a description of the **QuickLoop** tab, see “QuickLoop tab” on page 63.

Device Config tab

Use the **Device Config** tab to specify the device zone that belongs to the device zone configuration file. All members of this configuration file must be zones consisting entirely of AL_PAs in a QuickLoop. The **Device Config** tab is shown in Figure 26 on page 77.



SJ000203

Figure 26. Device Config tab of the AL_PA Level Zoning menu

Following is a description of the fields in the **Device Config** tab.

Cfg Name
Select an existing AL_PA configuration name to modify from the drop-down list.

Create Cfg
Click to create a new AL_PA configuration.

Delete Cfg
Click to delete an AL_PA configuration.

Rename Cfg
Click to rename an AL_PA configuration.

Zone/QLoop Selection List
A list of zone or QuickLoop members available to add to the AL_PA configuration.

Search Mem
Click to search for a switch name, WWN, alias, zone, QuickLoop, or FA zone in the **Zone/QLoop Selection List** field, based on the type of objects displayed in that list.

Add Mem
Click to add a member from the **Zone/QLoop Selection List** field into the **Configuration Members** list.

Remove Mem
Click to remove a member from the **Zone/QLoop Selection List** field.

Analyze Config
Click to analyze the configuration that is selected, along with its member zones and aliases. A Zoning Error window displays in the event of a conflict.

Refresh Fabric
Click to refresh the Fabric view with the latest domain, port, and WWN changes.

[AL_PA Config name] Members
This field displays a list of the members that belong to the AL_PA configuration currently selected in the **Cfg Name** field. The name of this list depends on the name of the AL_PA configuration selected. If an AL_PA configuration is not selected, the name displays as Null Members.

Enable Config
Select this option and click **Apply** to enable the selected configuration for zoning the fabric.

Disable Zoning
Select this option and click **Apply** to disable the selected configuration for zoning the fabric.

For a description of the **Ref Zone**, **A/D WWN**, **Rpl WWN**, **OK**, **Apply**, **Close**, and **Clr All** buttons, see “Port Alias tab” on page 60.

Mixed level zoning

Mixed level zoning is provided for backward compatibility with Fabric OS versions earlier than 3.0. From the Zoning Selection menu, select **Mixed Level Zoning** and click **OK**. The Mixed Level Zoning menu displays, as shown in Figure 27 on page 79.

The following is a list of the tabs in the Mixed Level Zoning menu:

- Alias
- Zone
- QuickLoop
- Config

Alias tab

Use the **Alias** tab to set up mixed aliases. The **Alias** tab is shown in Figure 27 on page 79.

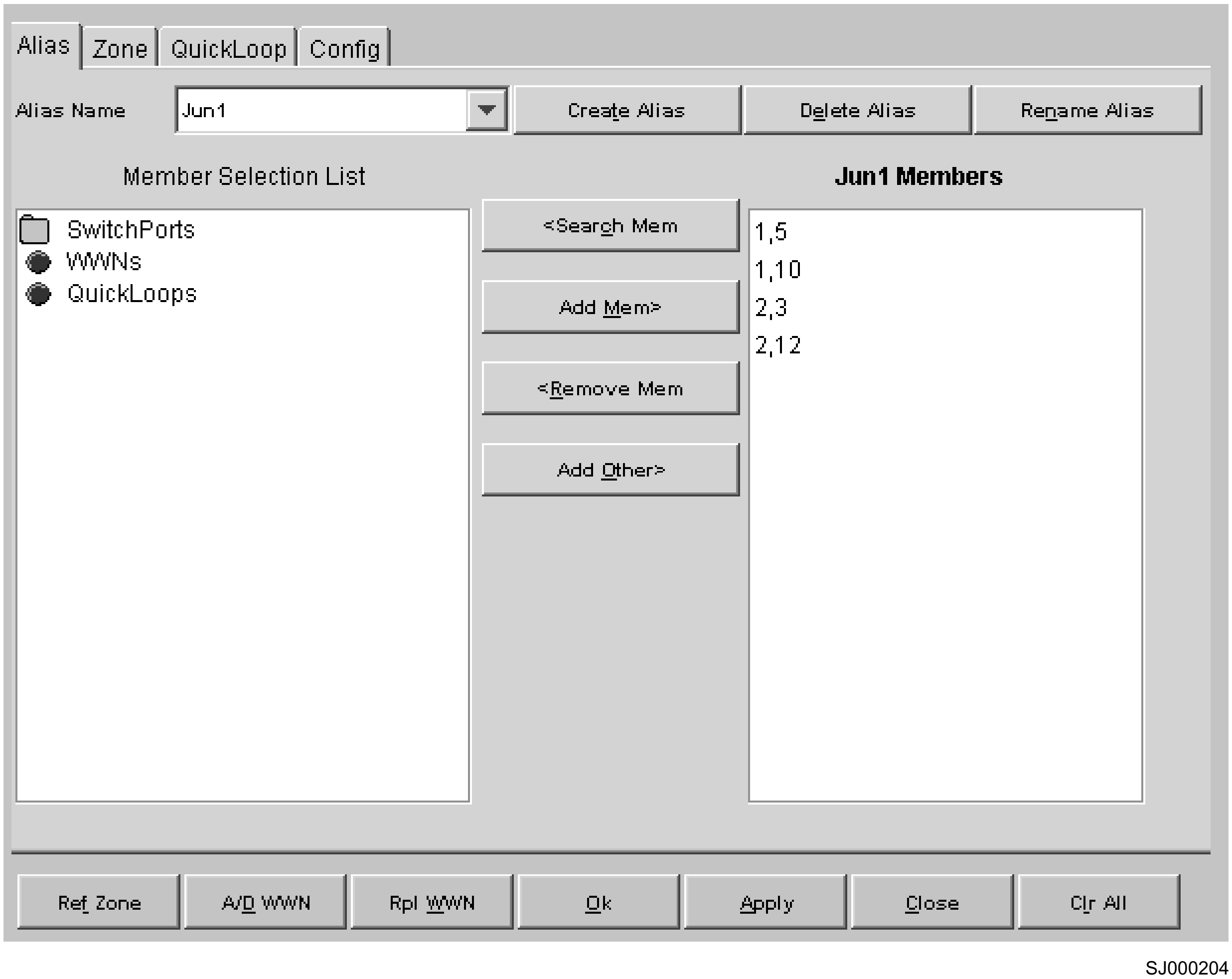


Figure 27. Alias tab of the Mixed Level Zoning menu

Following is a description of the fields in the **Alias** tab.

Alias Name
: Select an existing alias to modify from the drop-down list.

Create Alias
: Click to create a new alias. A dialog displays. Type the name of the new alias. All names must be unique and contain no spaces.

Delete Alias
: Click to delete the alias that is selected in the **Alias Name** field. Deleting an alias automatically removes it from all zones.

Rename Alias
: Click to rename the alias that is selected in the **Alias Name** field. A dialog displays in which you can edit the alias name. Renaming an alias automatically renames it in all zones.

Member Selection List
: This field displays a list of potential alias members, including switches, ports, WWNs, and QuickLoop AL_PAs.

Search Mem
Click to search for a switch name, WWN, alias, zone, QuickLoop, or FA zone in the **Member Selection List** field, based on the type of objects displayed in that list.

Add Mem
Click to add a member from the **Member Selection List** field to the **Alias Members** list.

Remove Mem
Click to remove the selected member from the **Alias Members** list.

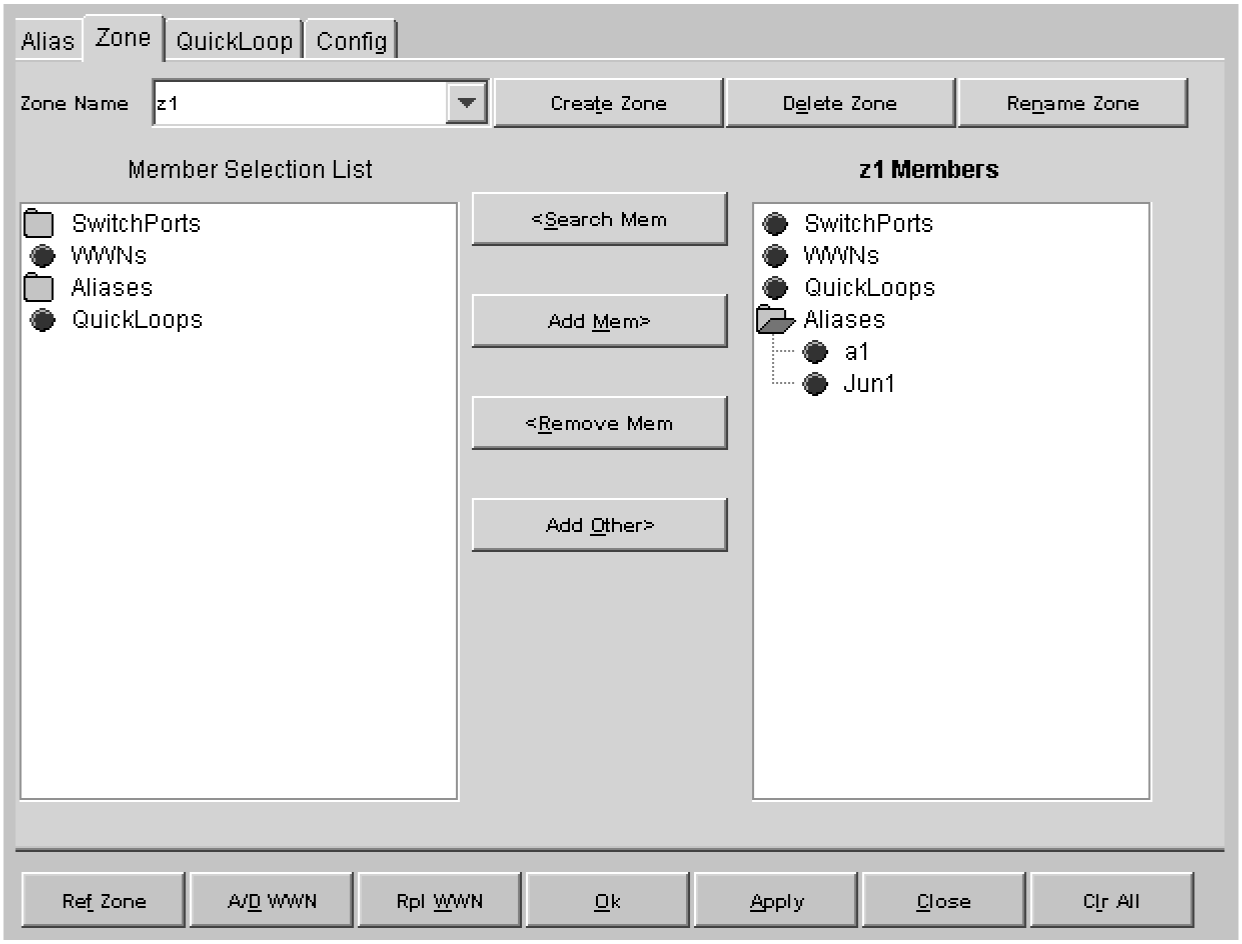
Add Other
Click to add a switch, port, WWN, or a device that currently is not part of the fabric.

[Alias name] Members
This field lists the members of the alias selected in the **Alias Name** field. The name of this list depends on the name of the selected alias. If no alias is selected, the name displays as Null Members.

For a description of the **Ref Zone**, **A/D WWN**, **Rpl WWN**, **OK**, **Apply**, **Close**, and **Clr All** buttons, see “Port Alias tab” on page 60.

Zone tab

Use the **Zone** tab to specify the member of a mixed zone. Mixed zone members can be AL_PAs, ports, and WWNs. The **Zone** tab is shown in Figure 28 on page 81.



SJ000205

Figure 28. Zone tab of the Mixed Level Zoning menu

Following is a description of the fields in the **Zone** tab.

Zone Name
Select an existing zone member to modify from the drop-down list.

Create Zone
Click to create a new zone member. A dialog displays. Type the name of the new zone member. All names must be unique and contain no spaces.

Delete Zone
Click to delete the zone member that is selected in the **Zone Name** field. Deleting a zone automatically removes it from all zone configurations.

Rename Zone
Click to edit the name of the zone that is selected in the **Zone Name** field. A dialog displays in which you can edit the zone name. Renaming a zone automatically renames it in all zone configurations.

Member Selection List
This field displays a of potential alias members, including switches, ports, WWNs, and QuickLoop AL_PAs.

Search Mem
: Click to search for a switch name, WWN, alias, zone, QuickLoop, or FA zone in the **Member Selection List** field, based on the type of objects displayed in that list.

Add Mem
: Click to add a member from the **Member Selection List** field into the **Zone Members** list.

Remove Mem
: Click to remove the selected member from the **Zone Members** list.

Add Other
: Click to add a switch, port, WWN, or a device that currently is not part of the Fabric.

[Zone name] Members
: This field displays a list of the zone members selected in the **Zone Name** field. The name on this list depends on the name of the selected zone member. If a name is not selected, the name displays as Null Members.

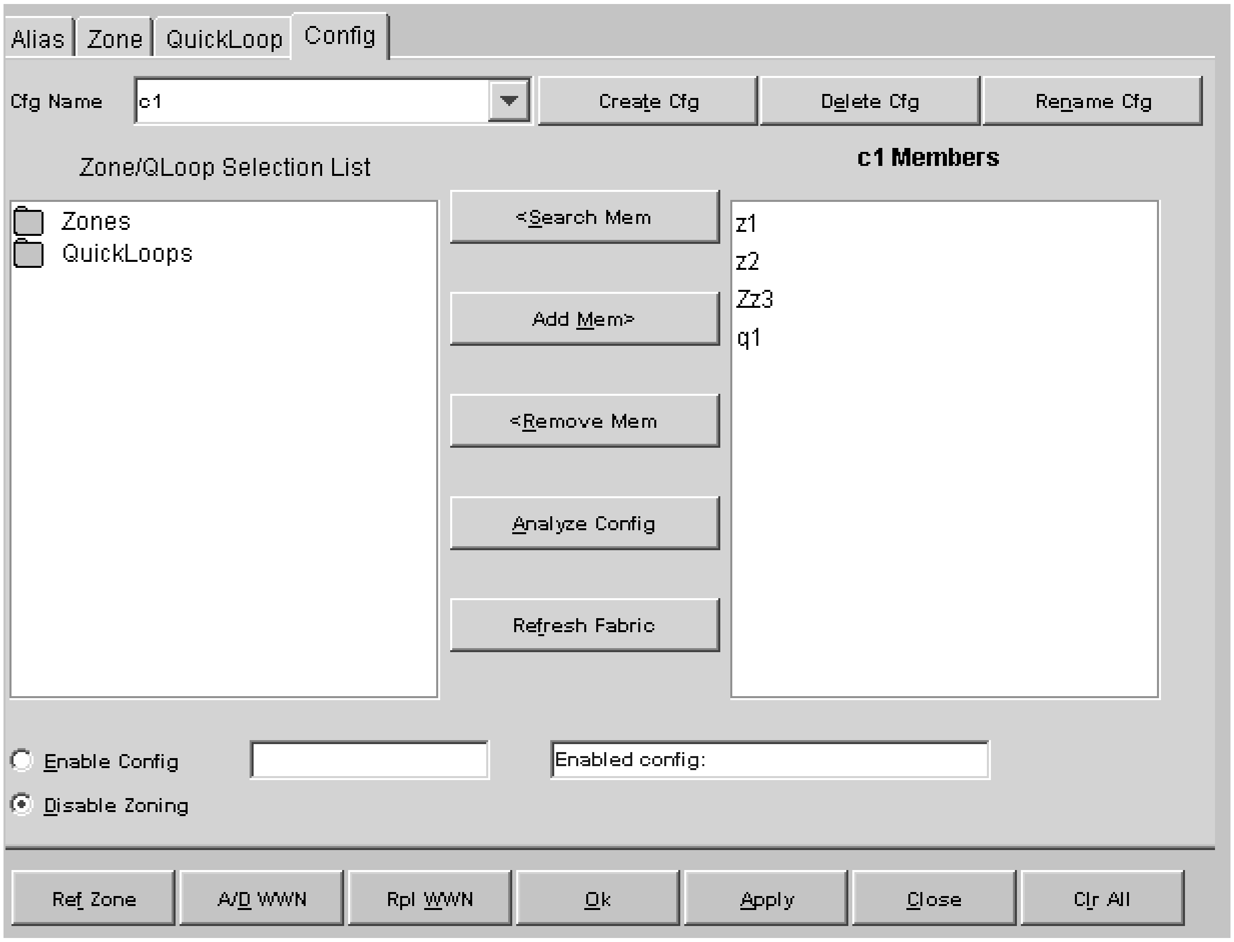
For a description of the **Ref Zone**, **A/D WWN**, **Rpl WWN**, **OK**, **Apply**, **Close**, and **Clr All** buttons, see “Port Alias tab” on page 60.

QuickLoop tab

A QuickLoop license is required to use this tab. In conjunction with zoning, use the **QuickLoop** tab to create and manage QuickLoops. For information on managing the QuickLoop feature separately, see “Loop tab” on page 104. For a description of the **QuickLoop** tab, see “QuickLoop tab” on page 63.

Config tab

Use the **Config** tab to save and enable a mixed zone configuration file. A mixed zone configuration file can contain any type of zoneable objects, ports, WWNs, and AL_PAs. The **Config** tab is shown in Figure 29 on page 83.



SJ000207

Figure 29. Config tab of the Mixed Level Zoning menu

Following is a description of the fields in the **Config** tab.

Cfg Name
Select an existing zoning configuration to modify from the drop-down list.

Create Cfg
Click to create a new configuration.

Delete Cfg
Click to delete a configuration.

Rename Cfg
Click to rename a configuration.

Zone/QLoop Selection List
A list of zone or QuickLoop members available to add to the configuration.

Search Mem
Click to search for a switch name, WWN, alias, zone, QuickLoop, or FA zone in the **Zone/QLoop Selection List** field, based on the type of objects displayed in that list.

Add Mem
Click to add a member from the **Zone/QLoop Selection List** field into the **Config Members** list.

Remove Mem
Click to remove a member from the **Config Members** list.

Analyze Config
Click to analyze the configuration that is selected along with its member zones and aliases. A Zoning Error window displays in the event of a conflict.

Refresh Fabric
Click to refresh the Fabric view with the latest domain, port, and WWN changes.

[Config name] Members
A list of the members that belong to the configuration currently selected in the **Cfg Name** field. The name of this list depends on the name of the configuration selected. If a configuration is not selected, the name displays as Null Members.

Enable Config
Select this option and click **Apply** to enable the selected configuration for zoning the fabric.

Disable Zoning
Select this option and click **Apply** to disable the selected zoning configuration.

For a description of the **Ref Zone**, **A/D WWN**, **Rpl WWN**, **OK**, **Apply**, **Close**, and **Clr All** buttons, see “Port Alias tab” on page 60.

Switch view

The Switch view represents the front panel of the switch, and displays when you click a **Switch** icon in the Fabric view. This view provides information about the overall status of the switch and the status of the individual elements in the switch. The information displayed is as close as possible to a real-time view of switch status. If the switch is not functioning properly, a message explains the problem detected.

Note: Switch status is stored as the variable *switchStatus*, and is calculated approximately once per second; however, the initial calculation does not occur until 30 - 60 seconds after the switch is started.

Perform the following steps to access the Switch view:

1. Launch the Web browser.
2. Type the switch name or IP address in the **Location/Address** field and press Enter.

   TotalStorage Specialist launches, displaying the Fabric view.
3. Click the **Switch** icon.

   The Switch view displays, as shown in Figure 30 on page 85.

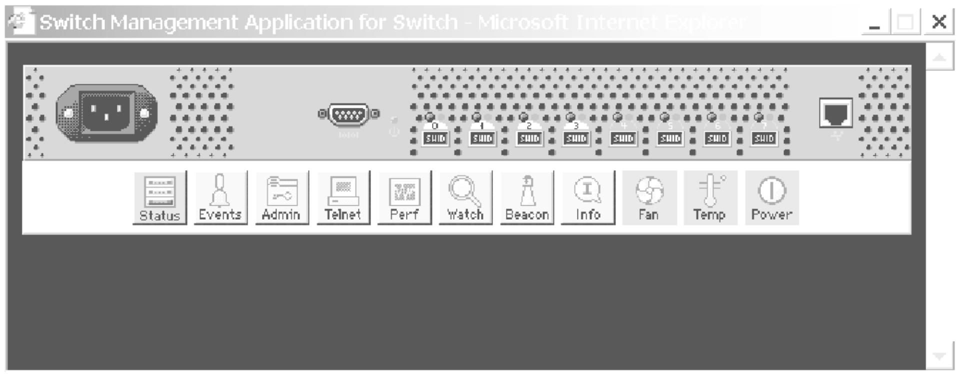


Figure 30. Switch view

Following is a description of the items that are displayed in the Switch view.

Port icons
The letters in the **Port** icon indicate the SFP type, as follows:

blank No SFP present

SW Shortwave SFP

LW Longwave SFP

CU Copper SFP

SWID Shortwave serial ID SFP

LWID Longwave serial ID SFP

CUID Copper serial ID SFP

A yellow outline around a **Port** icon indicates a port failure. For detailed information about a port, click the **Port** icon to see the Port Information view.

Port numbers (located above each port)
The number of the port.

LED status indicators (located above each port on the left side)
The color and state of the LED indicates the status of the port.

No light
No device is attached.

Steady yellow
Receiving light, but not online; check cable connections.

Slowly flashing yellow
Disabled (diagnostics or **portDisable** command).

Rapidly flashing yellow
Error, fault with port.

Steady green
Online (connected with device by cable).

Slowly flashing green
Online but segmented (loopback cable or incompatible switch).

Rapidly flashing green
Internal loopback (diagnostic).

Flickering green
Online and transmitting or receiving frames.

Status icon
Click to view the health status of the switch.

Events icon
Click to access the Switch Events view.

Admin icon
Click to display the Administrative Interface, where you can perform switch management functions.

Telnet icon
Click to access the Telnet interface.

Perf icon
Click to display the Performance Monitor, where you can monitor switch performance.

Fabric Watch icon
Click to access Fabric Watch, if a license is installed.

Beacon icon
Click to turn on the beaconing function. If on, this icon shows beams of light. The beaconing function helps to physically locate a switch by sending a signal to the specified switch, resulting in an LED light pattern flashing from side to side on the switch.

Info icon
Click to display the switch information.

Fan icon
The background color of the icon indicates the overall status of the fans:

Green Healthy

Yellow
Marginal (mix of good and faulty readings)

Red Down (more than two faulty readings)

Gray Unknown or unmonitored

Temp icon
The background color of the icon indicates the overall status of the temperature sensors.

Green Healthy

Yellow
Marginal (one faulty reading)

Red Down (more than two faulty readings)

Switch Events view

The Switch Events view displays a running log of events for the selected switch.

Perform the following steps to access the Switch Events view:

1. Launch the Web browser.
2. Type the switch name or IP address in the **Location/Address** field and press Enter.

   TotalStorage Specialist launches, displaying the Fabric view.

3. Click the **Switch** icon.

   The Switch view displays.

4. Click the **Events** icon.

   The Switch Events view displays, as shown in Figure 31.

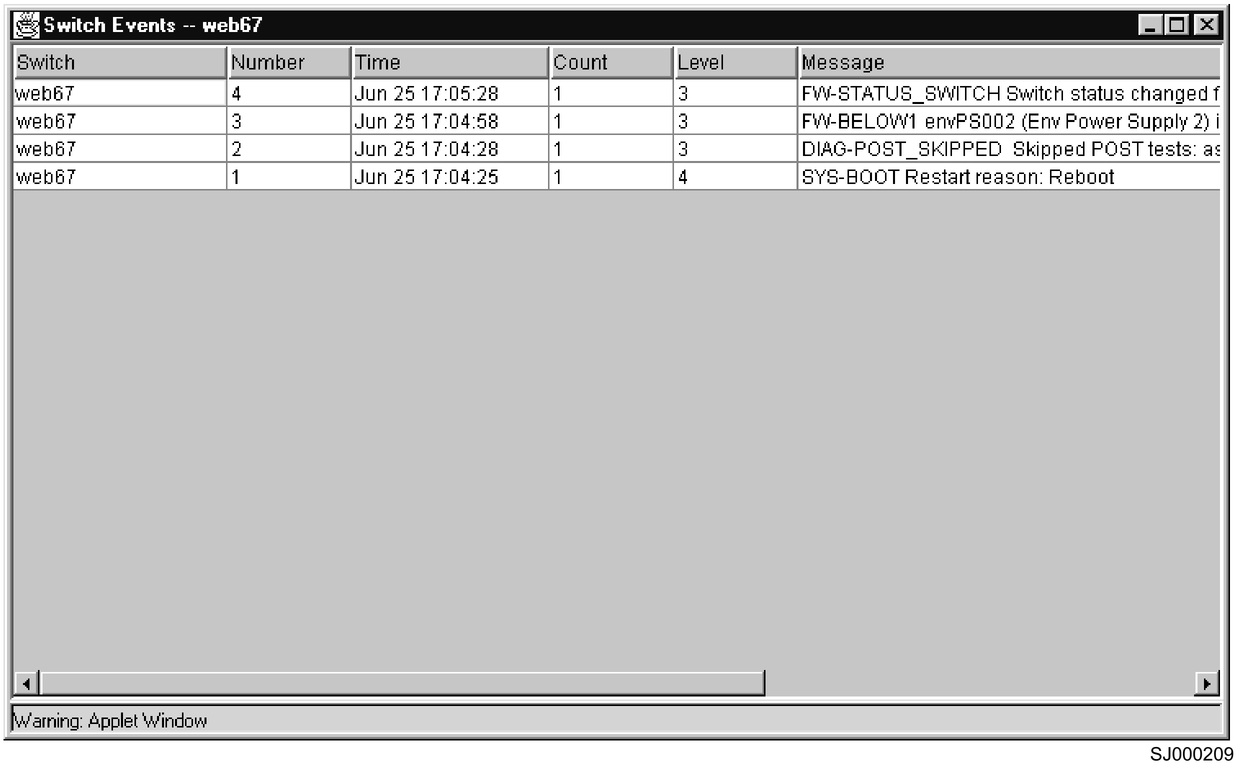


Figure 31. Switch Events view

Note: To sort the events by a particular column, click the column header. To resize a column, drag the column divider.

Following is a description of the fields in the **Switch Events** view.

Switch
: The name of the switch.

Number
: The event number.

Time
: The time of the event.

Count
: The number of consecutive occurrences of the same event.

Level
: The severity level of the event. Valid levels are:

  0 panic (switch restarts)

  1 critical

  2 error

  3 warning

  4 information

  5 debug

Message
A description of the event.

Fabric Watch view (optional software required)

You can use the Fabric Watch view to monitor fabric elements for potential problem conditions. This feature requires an active Fabric Watch license. For detailed information about Fabric Watch, see Chapter 6, “Fabric Watch” on page 179.

Perform the following steps to access the Fabric Watch view:

1. Launch the Web browser.
2. Type the switch name or IP address in the **Location/Address** field and press Enter.

   TotalStorage Specialist launches, displaying the Fabric view.
3. Click the **Switch** icon.

   The Switch view displays.
4. Click the **Watch** icon.

   The Fabric Watch view displays, with the **Alarm Notifications** tab selected by default.

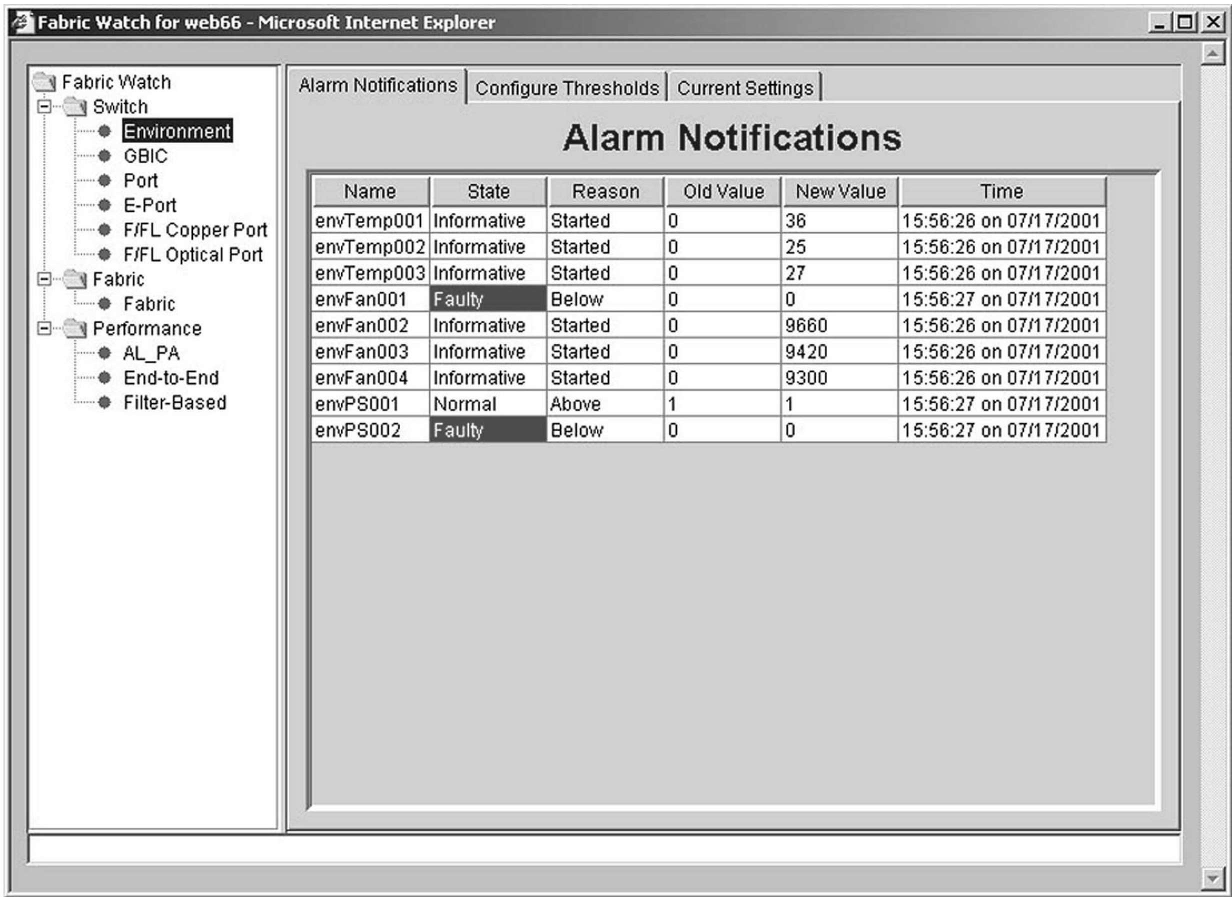
The Fabric Watch view contains the following tabs:

- Alarm Notifications
- Configure Thresholds
- Current Settings

In addition, an organizational tree is displayed on the left side of the view, showing all the Fabric Watch areas regardless of which tab is selected. To expand or contract a folder in the tree, double-click the folder icon.

Alarm Notifications tab

Use the **Alarm Notifications** tab to view the Fabric Watch notifications. The **Alarm Notifications** tab is shown in Figure 32.

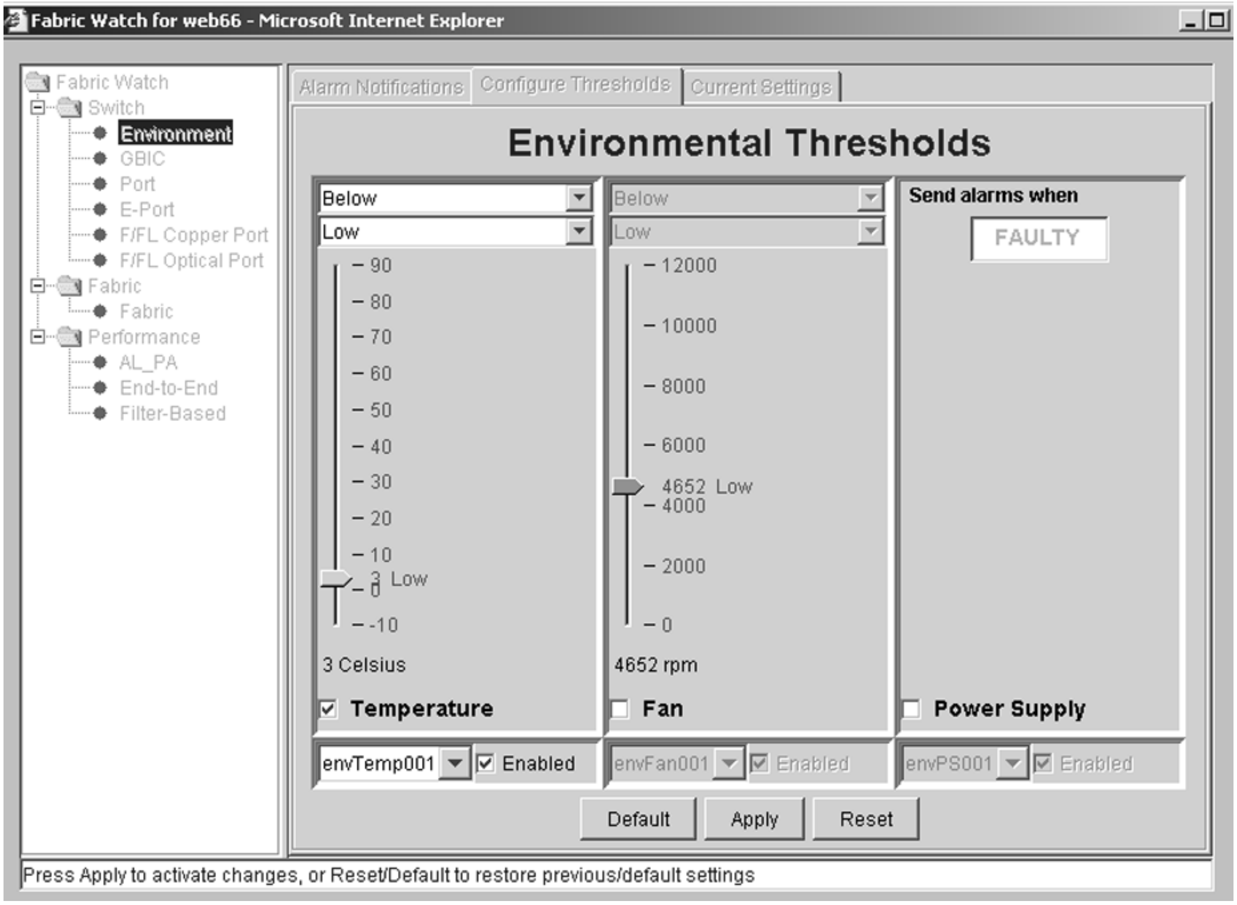


SJ000214

Figure 32. Alarm Notifications tab in the Fabric Watch view

Configure Thresholds tab

Use the **Configure Thresholds** tab to view and configure Fabric Watch thresholds for the Fabric Watch class that is currently selected in the organizational tree on the left side of the window. The **Configure Thresholds** tab is shown in Figure 33 on page 90.



SJ000215

Figure 33. Configure Thresholds tab with the environment class selected in the Fabric Watch view

The display of the **Configure Threshold** tab changes depending on the class and area that is selected in the organizational tree. Following is a description of the fields in the **Configure Thresholds** tab.

Default
: Click to return the settings to the default values.

Apply
: Click to apply the values that are specified in the current display. When you click **Apply** after a change, the Alarm Mechanisms dialog displays, as shown in Figure 34 on page 91. Check the appropriate boxes in this dialog box to specify alarm delivery mechanisms. When e-mail is chosen as one of the alarm delivery mechanisms, the **Mail Server**, **Mail Domain**, **Mail From**, and **Mail To** fields are enabled. This information is used to configure the e-mail alert by the Fabric Watch daemon. If e-mail is not chosen as one of the delivery mechanisms, these fields are grayed out.

  To continue, select the type of alarm that you want and click **Apply**.

Reset
: Click to undo the last changes that were applied.

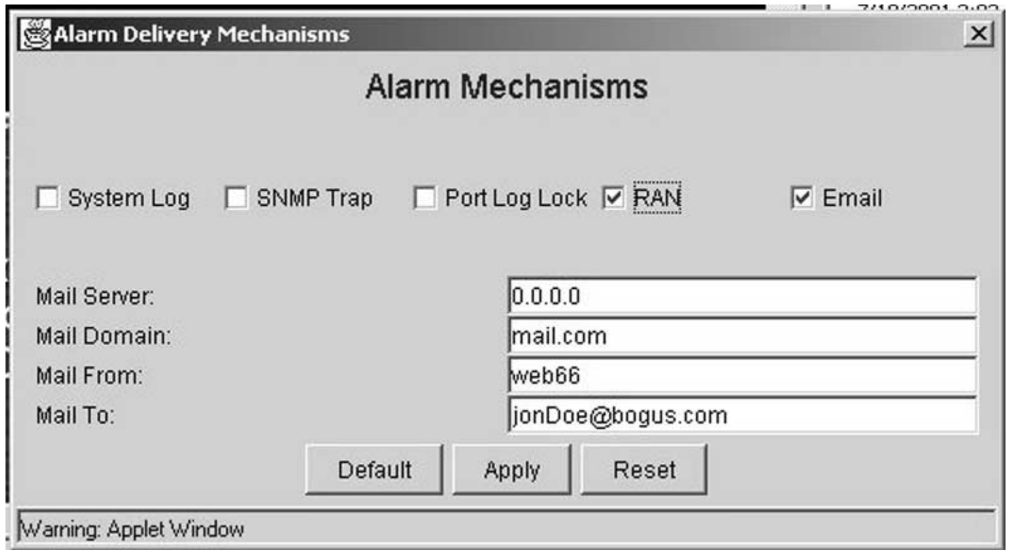


Figure 34. Alarm Mechanisms dialog box

Thresholds for Environmental classes

The environmental classes are displayed by selecting the Environmental file from organizational tree on the left side of the Configure Thresholds window. See Figure 33 on page 90.

Following is a description of the thresholds that can be set for the Environmental classes.

Threshold Type drop-down list
: Select the threshold type. Valid types are exceeded, above, in-between, below, or changed.

High and Low drop-down list
: Use the sliding scale to set the high and low settings for the threshold type that was selected in the Threshold Type drop-down list (not available for all areas).

Area Select checkbox
: Select a Fabric Watch area to configure. Only one area can be selected at a time.

Enabled checkbox
: Select or clear the checkbox to specify if you want this element to be monitored.

Send alarms when box
: Use this text box to specify whether you want to be notified when the area is in the acceptable range (OK) or is faulty (FAULTY).

Thresholds for GBIC classes

The GBIC classes are displayed by selecting the GBIC file from the organizational tree on the left side of the Configure Thresholds window.

Following is a description of the thresholds that can be set for the GBIC classes.

Threshold Type drop-down list
Select the threshold type. Valid types are exceed, above, in-between, below, or changed.

High and Low drop-down list
Use the sliding scale to set the high and low settings for the threshold type that was selected in the Threshold Type drop-down list (not available for all areas).

Area Select checkbox
Select a Fabric Watch area to configure. Only one area can be selected at a time.

Enabled checkbox
Select or clear the checkbox to specify if you want this element to be monitored.

Send alarms when box
Use this text box to specify whether you want to be notified when the area is in the acceptable range (OK) or is faulty (FAULTY).

Thresholds for all Port classes

The port classes (Port, E_port, F/FL Copper Port, and F/FL Optical Port) are displayed by selecting the individual port type from the organizational tree on the left side of the Configure Thresholds window.

The thresholds for the Port class are displayed in Figure 35 on page 93

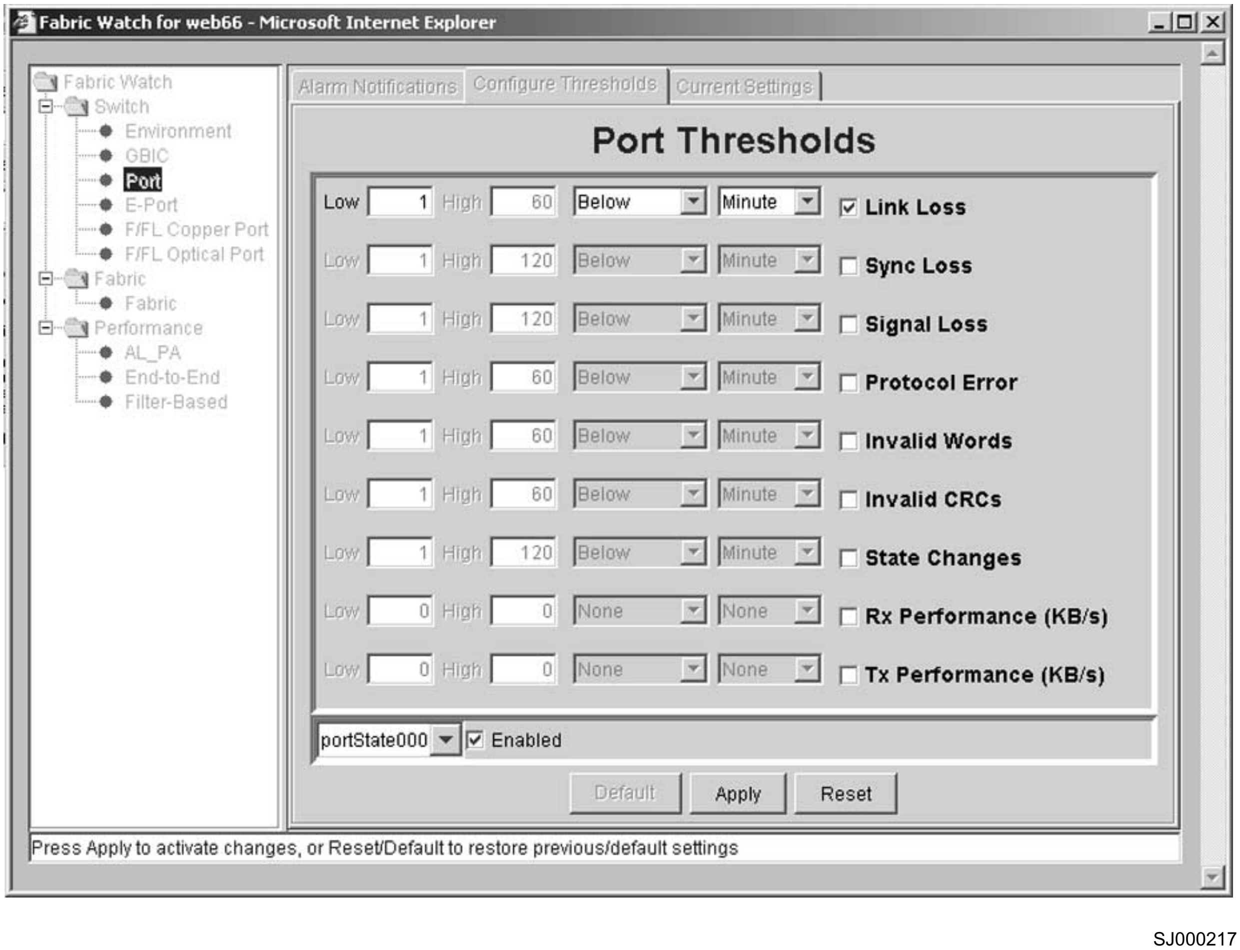


Figure 35. Configure Thresholds tab with the Port class selected in the Fabric Watch view

Following is a description of the thresholds that can be set for the Port classes.

Low text box
Type the low threshold boundary.

High text box
Type the high threshold boundary.

Threshold Type drop-down list
Select the threshold type. Valid types are exceeded, above, in-between, below, or changed.

Time period drop-down list
Select the time period for which you want a time-based count to be measured.

Area checkbox
Select or clear the checkbox or the area that you want the thresholds to apply.

Thresholds for Performance classes

Use the **Configure Thresholds** tab to view and configure AL_PA thresholds for the Performance class currently selected in the organizational tree on the left side of the window. The **Configure Thresholds** tab for AL_PA thresholds is shown in Figure 36.

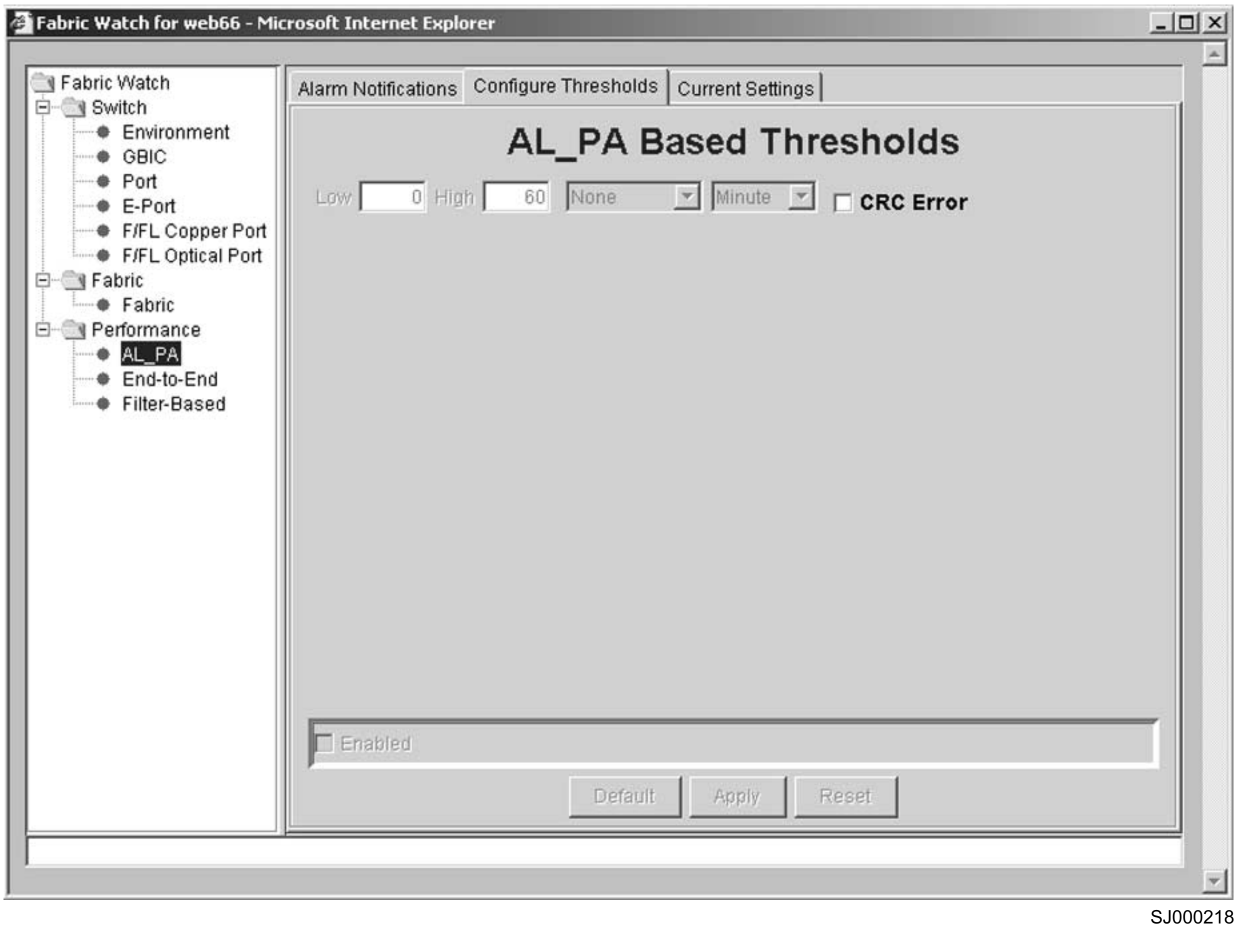


Figure 36. Configure Thresholds tab with AL_PA class selected in the Fabric Watch view

Note: The **AL_PA Configure Threshold** tab applies only to L_ports.

Use the **Configure Thresholds** tab to view and configure End-to-End thresholds for the Performance class currently selected in the organizational tree on the left side of the window. The **Configure Thresholds** tab for End-to-End thresholds is shown in Figure 37.

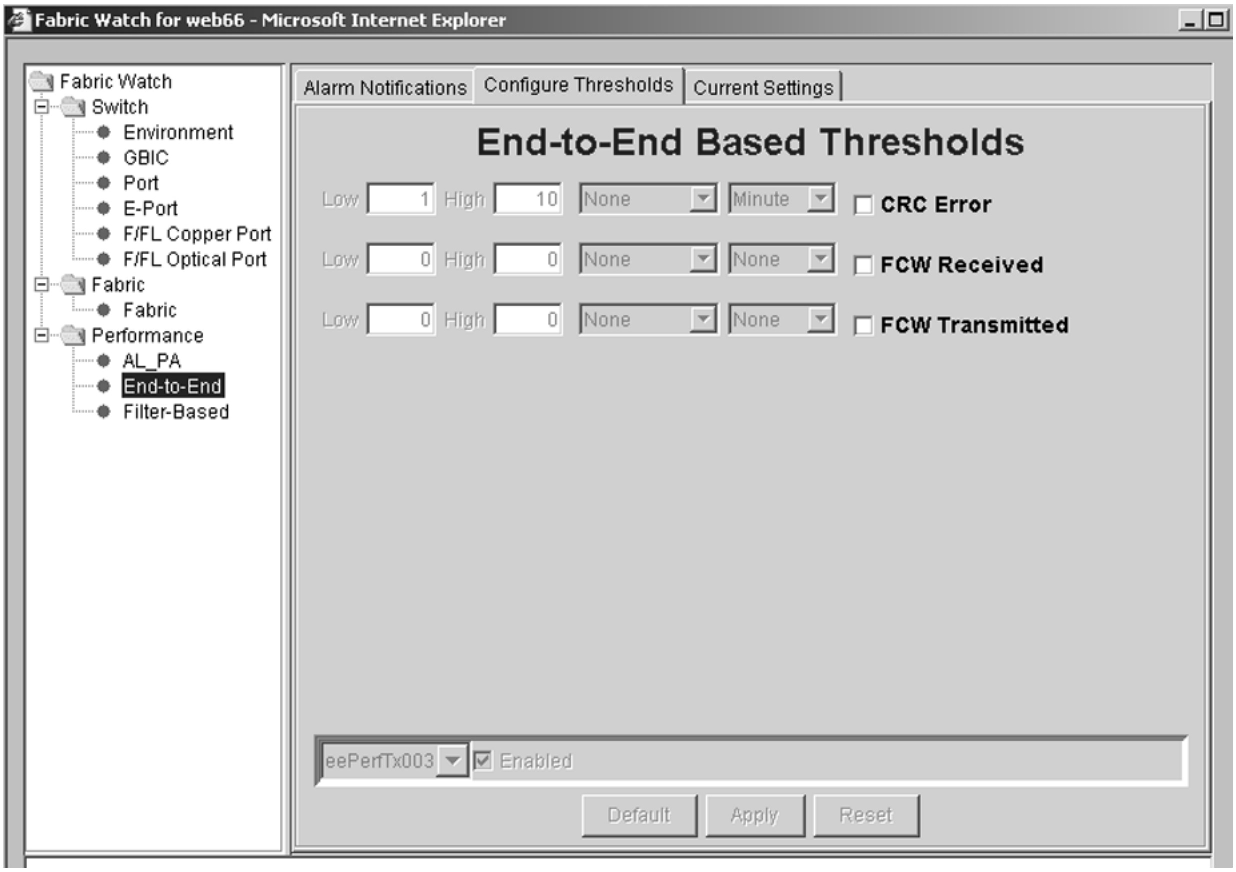


Figure 37. The Configure Thresholds tab with End-to-End class selected in the Fabric Watch view

You must define the SID/DID pair through the Performance Monitor before you can monitor the threshold in the End-to-End class. For more information about the Performance Monitor, see "Performance Monitor" on page 106 or Chapter 4, "Advanced Performance Monitoring" on page 153.

Use the **Configure Thresholds** tab to view and configure Filter-Based thresholds for the Performance class currently selected in the organizational tree on the left side of the window. The **Configure Thresholds** tab for Filter-Based thresholds is shown in Figure 38.

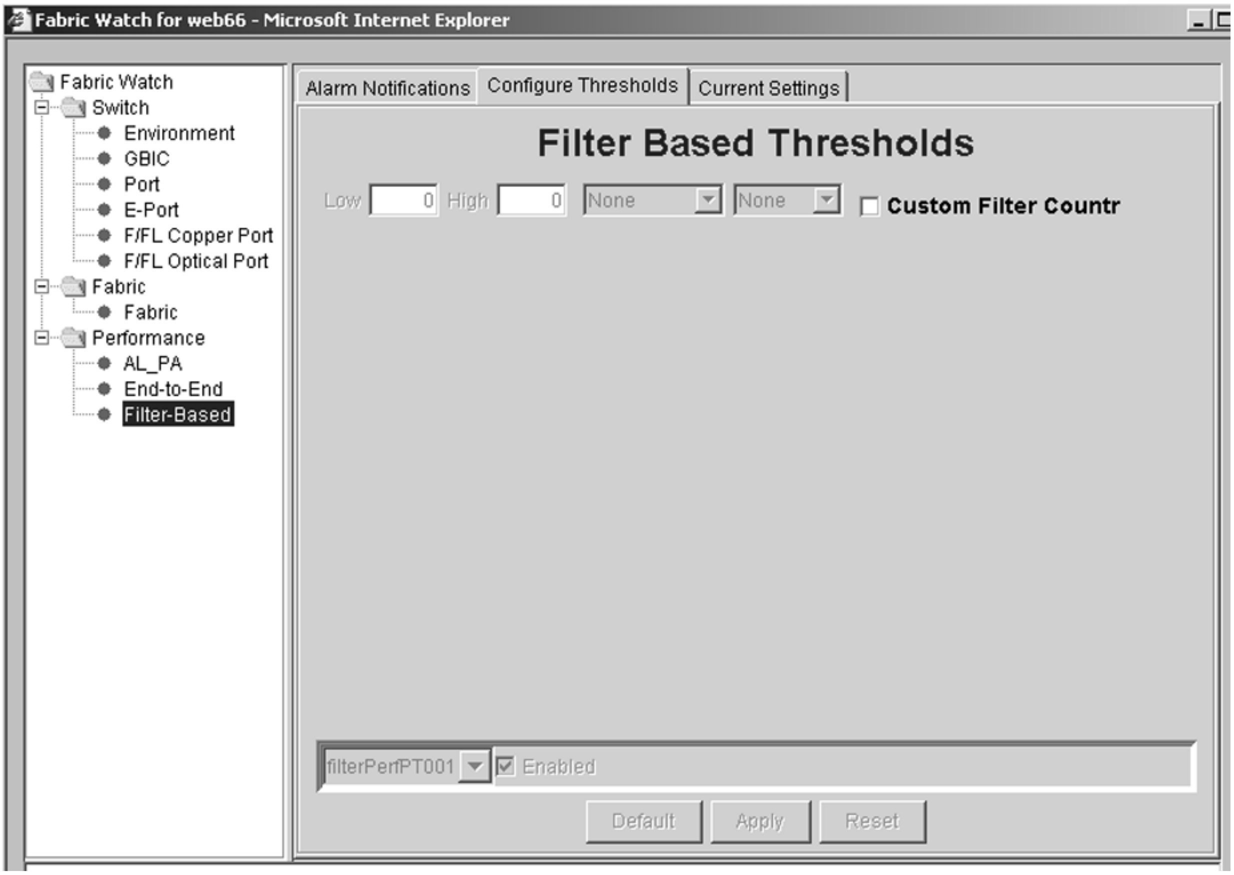


Figure 38. Configure Thresholds tab with Filter-Based class selected in the Fabric Watch view

The filter type must be predefined in the Performance Monitor before you can use the Filter-Based thresholds. For more information about the Performance Monitor, see “Performance Monitor” on page 106 or Chapter 4, “Advanced Performance Monitoring” on page 153.

Current Settings tab

Use the **Current Settings** tab to view the current Fabric Watch threshold parameters for the area selected in the Fabric Watch organizational tree. The **Current Settings** tab is shown in Figure 39.

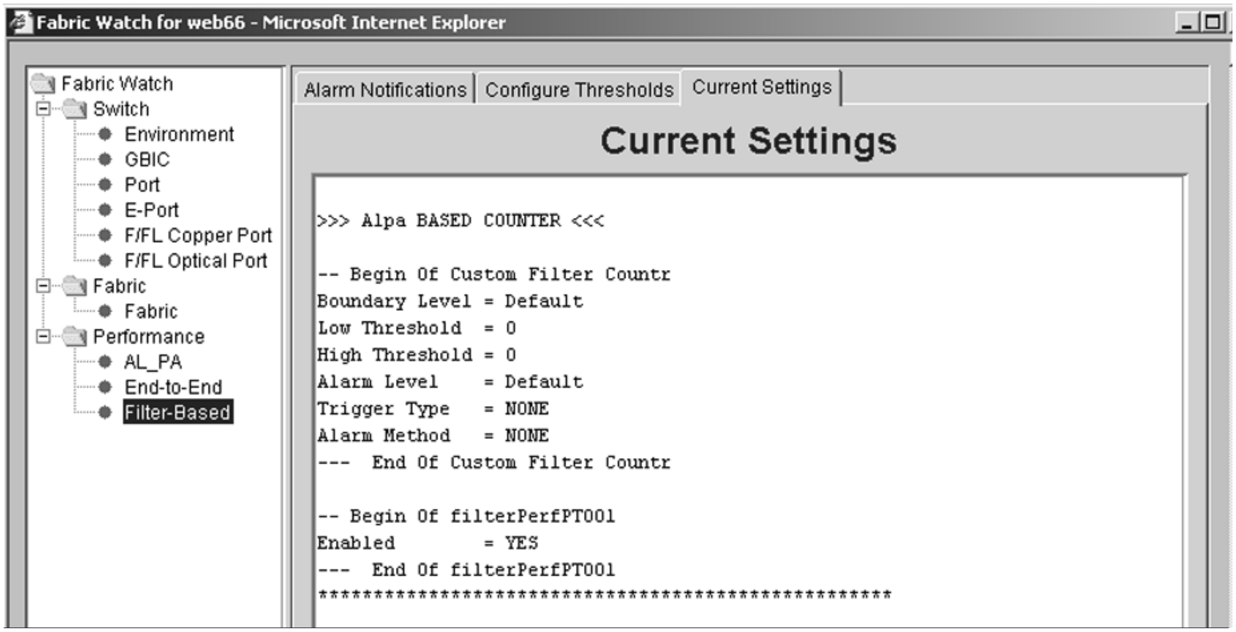


Figure 39. Current Settings tab in the Fabric Watch view

Port Information view

The Port Information view displays statistics about the selected port. This information is automatically updated when you open the view, and is also refreshed periodically while the view remains open.

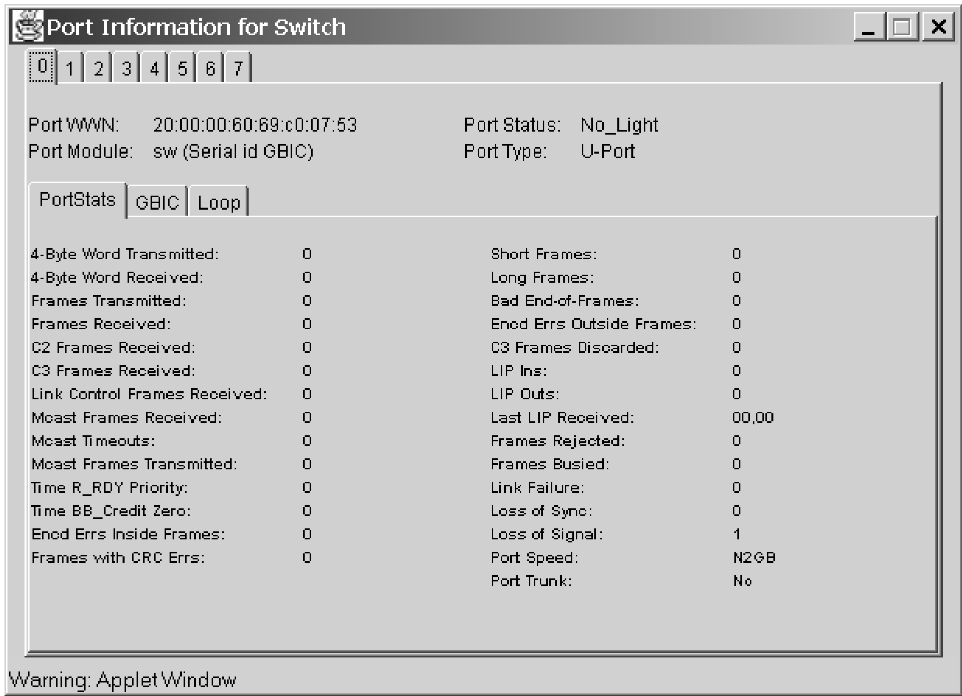
Perform the following steps to access the Port Information view:

1. Launch the Web browser.
2. Type the switch name or IP address in the **Location/Address** field and press Enter.

   TotalStorage Specialist launches, displaying the Fabric view.
3. Click the **Switch** icon in Fabric view.

   The Switch view displays.
4. Click a **Port** icon.

   The Port Information view displays, as shown in Figure 40 on page 98.



SJ000351

Figure 40. Port Information view

The following tabs are available in Port the Information view:

- PortStats
- GBIC
- Loop

Following is a description of the fields in the Port Information view regardless of which tab is selected.

Port WWN
The worldwide name (WWN) of this port.

Port Module
The GBIC type. Valid types are:

-- No GBIC present

SW Shortwave GBIC

LW Longwave GBIC

CU Copper GBIC

SWID Shortwave serial ID GBIC

LWID Longwave serial ID GBIC

CUID Copper serial ID GBIC

Port Status
The current status of the port. Valid statuses are:

No_Module
No GBIC module is in this port.

No_Light
The module is not receiving light.

No_Sync
The module is receiving light but is out of sync.

In_Sync
The module is receiving light and is in sync.

Laser_Flt
The module is signaling a laser fault (defective GBIC).

Port_Flt
The port is marked faulty (defective GBIC, cable, or device).

Diag_Flt
The port failed diagnostics.

Online
The port is up and running.

Lock_Ref
The port is locking to a reference signal.

Note: Removing a cable from an E_port temporarily generates errors, causing the status to show as faulty. The status returns to healthy when the sample interval has passed (the default interval is 1 minute).

Port Type
The type of port. Valid types are:

E_port
Switch-link port

G_port
Generic port

U_port
Universal port

F_port
Fabric port

FL_port
Fabric loop port

L_port
Loop port

PortStats tab

The **PortStats** tab provides information about transmission speed, reception speed, and the volume of traffic through the selected port. The **PortStats** tab is shown in Figure 41 on page 100.

SJ000351

Figure 41. PortStats tab of the Port Information view

Following is a description of the fields in the **PortStats** tab.

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

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

Frames Transmitted
The number of frames transmitted.

Frames Received
The number of frames received.

C2 Frames Received
The number of class 2 frames received.

C3 Frames Received
The number of class 3 frames received.

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

Mcast Frames Received
The number of multicast frames received.

Mcast Timeouts
The number of multicast timeouts.

Mcast Frames Transmitted
The number of multicast frames transmitted.

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

Time BB_Credit Zero
: The number of times BB_credit (buffer-to-buffer credit) went to zero.

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

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

Short Frames
: The number of frames shorter than minimum.

Long Frames
: The number of frames longer than maximum.

Bad End-of-Frames
: The number of frames with faulty end-of-frames.

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

C3 Frames Discarded
: The number of class 3 frames discarded.

LIP Ins
: The number of LIPs received.

LIP Outs
: The number of times loop initialized by FL_port.

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

Frames Rejected
: The number of F_RJTs sent.

Frames Busied
: The number of F_BSYs sent.

Link Failure
: The number of times NOS is received or sent.

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

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

Port Speed
: Displays the speed of the port.

Port Trunk
: Displays whether Trunking is enabled or disabled.

GBIC tab

The **GBIC** tab provides information about the GBIC that is installed in the selected port. The information displayed depends on the type of GBIC that is installed.

Standard GBIC
: Module type (for example shortwave, longwave, copper).

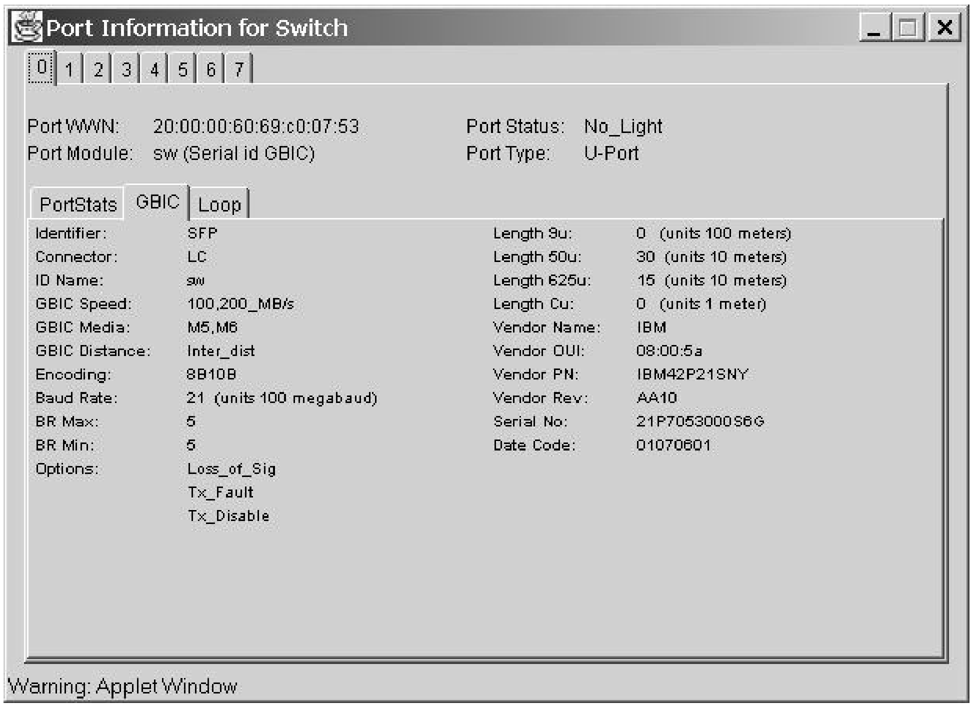
Serial ID GBIC
: Module type, plus extended information about capabilities, interfaces, and manufacturer.

Smart Finisar GBIC
All of the above information, plus GBIC active status.

If the port does not contain a GBIC, the following message displays:

```
Not a serial ID GBIC. No GBIC info available.
```

Figure 42 shows the **GBIC** tab in the Port Information view.



SJ000352

Figure 42. GBIC tab of the Port Information view

Following is a description of the fields in the **GBIC** tab.

Identifier
Indicates the type of serial transceiver; can be GBIC or on-board.

Connector
Indicates the external connector type. Valid types are:

- SC
- Style-1 copper
- Style-2 copper
- BNC/TNC
- Coaxial

ID Name
Indicates the GBIC module type. Valid types are:

-- No GBIC present

sw Shortwave GBIC

lw Longwave GBIC

cu Copper GBIC

swid Shortwave serial ID GBIC

lwid Longwave serial ID GBIC

cuid Copper serial ID GBIC

GBIC Speed
Indicates the GBIC speed; can be 100 MBps, 200 MBps, or 400 MBps.

GBIC Media
Indicates the transmission media. Valid media are:

SM Single mode

M5 Multimode, 50u

M6 Multimode, 62.5u

TV Video coax

MI Miniature coax

TP Shielded twisted pair

TW Twin axial pair

GBIC Distance
Indicates the length of the fibre-channel link; can be long distance, intermediate distance, or short distance.

Encoding
Indicates the serial encoding mechanism; can be 8B10B, 4B5B, NRZ, or Manchester.

Baud Rate
Nominal baud rate in units of 100 MB.

BR Max
Upper limit at which the GBIC meets its specifications (in units of 1 percent above nominal baud rate).

BR Min
Lower limit at which the GBIC meets its specifications (in units of 1 percent below nominal baud rate).

Options
Indicates any of the following:

- Loss of Signal
- Loss of Signal Inverted
- Transmission Fault
- Transmission Disable

Length 9u
The length of the link using single mode fibre.

Length 50u
The length of link using 50 um multimode fibre.

Length 625u
The length of the link using 62.5 um multimode fibre.

Length Cu
The minimum length of the link using copper cable.

Vendor Name
The vendor name.

Vendor OUI
: The unique identifier for vendor.

Vendor PN
: The vendor part number.

Vendor Rev
: The vendor revision number.

Serial No.
: The vendor serial number.

Date Code
: The vendor date code.

Smart GBIC Data (only displays if a smart GBIC is present):

Temperature
: The module temperature (in degrees Centigrade).

Rx Power
: Received optical power in micro Watts.

Tx Power
: Transmitted optical power in micro Watts (longwave only).

Current
: Laser diode drive current in Amps.

Loop tab

The **Loop** tab provides the following information about any loop on the port:

- Loop statistics
- Local AL_PA statistics
- QuickLoop looplet statistics (if a QuickLoop license is available and the port is a member of the QuickLoop)
- QuickLoop statistics (if a QuickLoop license is available and the port is a member of the QuickLoop)

If the port is not a loop-enabled port, the following message displays:

```
Not an L_port. No loop info available.
```

The **Loop** tab is shown in Figure 43 on page 105.

Figure 43. Loop tab of the Port Information view

Following is a description of the fields in the **Loop** tab.

FL Port Transfer
Displays the number of times that the FL_port used the transfer state.

FL Tenancies
Displays the number of times that the FL_port opens the loop tenancy.

NL Tenancies
Displays the number of times that the NL_port opens the loop tenancy.

QL/Zone Inits Caused
Displays the number of times that the looplet has caused QuickLoop to be initialized.

Successful QL/Zones Inits
Displays the number of times that a looplet has successfully initialized.

Number of Failed QL/Zone Inits
Displays the number of times that a looplet failed to successfully initialize.

Times Being Bypassed
Displays the number of times that a looplet was not included as part of QuickLoop.

Last Time bypassed
Displays the time that a looplet was last bypassed.

Local AL_PA List
Displays a list of AL_PAs that are associated with devices that are connected to the loop.

QL Init Attempts
Displays the number of times that a QuickLoop attempted initialization.

Successful QL Inits
Displays the number of times that a QuickLoop successfully initialized.

Times in Single Switch Mode
Displays the number of times that a switch reverted to single switch mode.

Times in Dual Switch Mode
Displays the number of times that a switch operated in dual switch mode.

Time of Last QL Init
Displays the time of the latest QuickLoop initialization.

Switch, Port Caused the Last Init
Displays the number of the switch and port that caused the latest initialization.

Performance Monitor

The Performance Monitor performs the following functions:

- Graphically displays throughput (megabytes per second) for each port and for the entire switch. Port throughput is the number of bytes that are received at a port plus the number of bytes that are transmitted. Switch throughput is the sum of the throughput for all the ports. The Performance Monitor also allows the graphing of traffic based on the Source ID and the Destination ID hardware-filtering mechanism.
- Provides the ability to change the configuration of a switch or port visually by using the graphics.

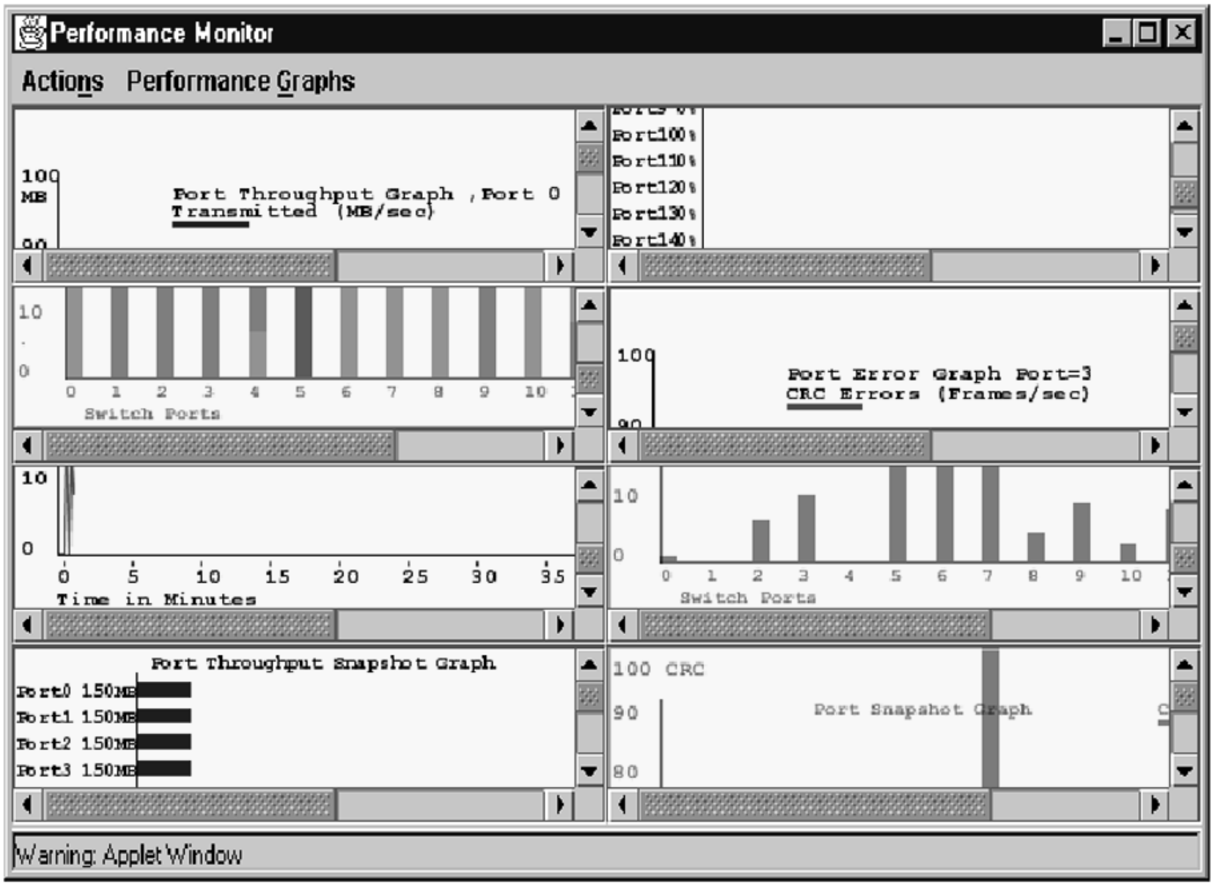
Perform the following steps to access the Performance Monitor:

1. Launch the Web browser.
2. Type the switch name or IP address in the **Location/Address** field and press Enter.

   TotalStorage Specialist launches, displaying the Fabric view.
3. Click the **Switch** icon.

   The Switch view displays.
4. Click the **Performance** icon.

   The Performance Monitor displays, as shown in Figure 44 on page 107.



SJ000222

Figure 44. Performance Monitor

Features

The Performance Monitor includes the following features:

- An existing report can be selected from a list of reports that are predefined. In some cases, you can supply the object to be monitored and graphed (such as port number, SID/DID pair, AL_PA, or switch domain number).
- Graphs are displayed on the display panel, or *canvas*, which can hold a maximum of eight graphs simultaneously. An individual graph can be maximized to occupy the entire canvas. The size of the graphs on the canvas is determined by the number of graphs being displayed. The window does not need to be scrolled to view all the selected graphs.
- The collection of graphs in the canvas can be stored for later retrieval on the switch. Up to 20 individual canvases can be saved. Each canvas is saved with its name, a brief description, and the graphs that comprise the canvas.
- Any graph can be magnified and detached from the main canvas or removed from the main canvas using a pop-up menu. You can display the pop-up menu by pointing the mouse at any graph on the main canvas and clicking the right mouse button. To reattach the detached (Zoomed Out) graph back to the main canvas, you can point the mouse to the detached graph, click the right button and select Zoom In.
- Each graph can be printed.

Graph types

There are three graph types used to display port and switch information:

- Vertical
- Horizontal
- Line chart

All graphs are real-time. Each graph is updated either every 5 seconds or every 15 seconds.

Performance Monitor menus

The Performance Monitor is made up of two main menus:

- The Performance Monitor Actions menu
- The Performance Graphs menu

Performance Monitor Actions menu

The Performance Monitor Actions menu is made up of the following sub-menus:

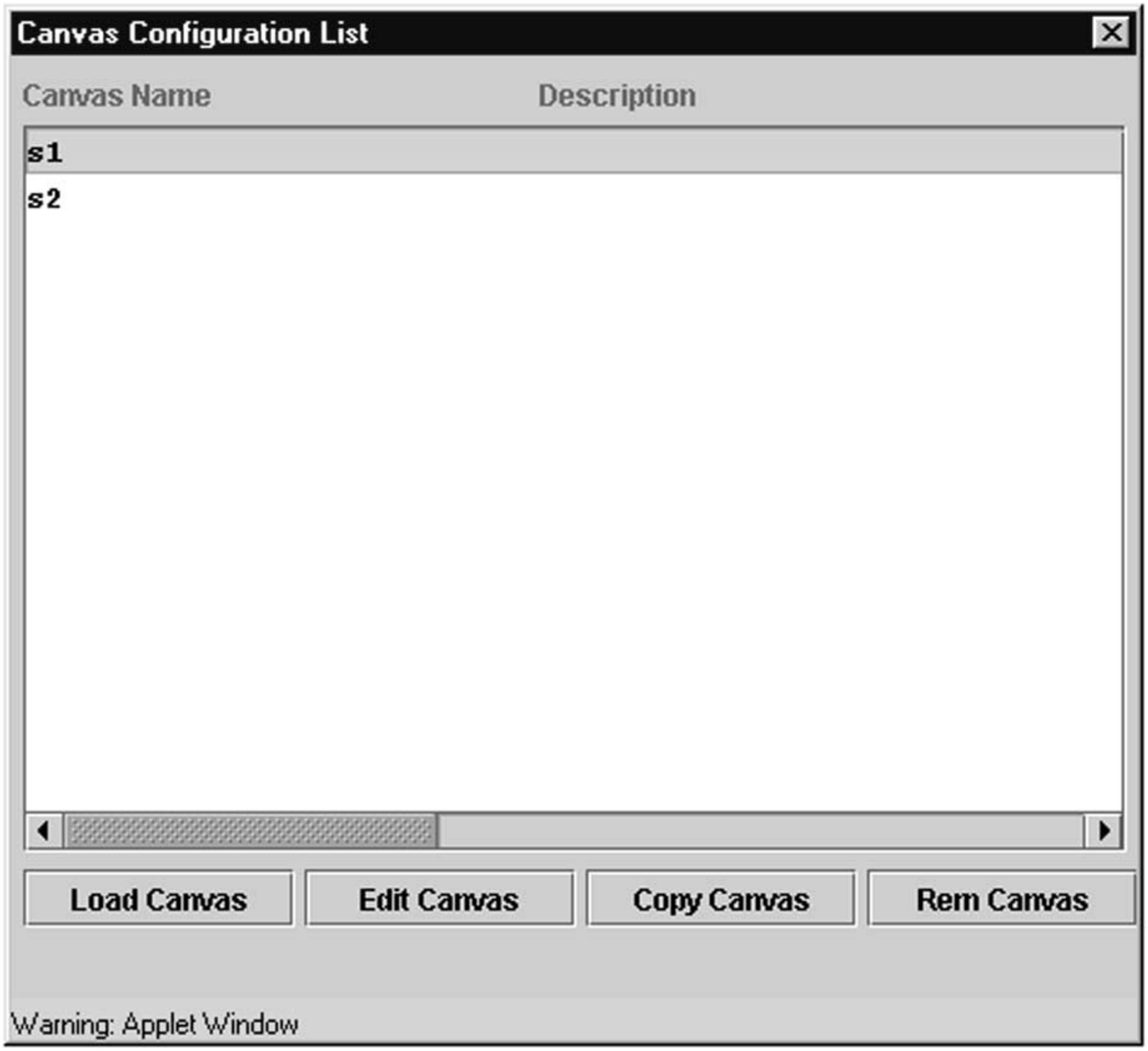
- Display Canvas Configurations
- Save Current Canvas Configuration
- Resource Usage Display
- Print All Graphs

Display Canvas Configurations menu: The Display Canvas Configurations menu allows you to view all the canvas configurations that have been saved on the switch.

Perform the following steps to access the Display Canvas Configuration menu:

1. Select the **Performance** icon from the Switch view.
2. Select the Actions menu.
3. Select the Display Canvas Configurations option.

   The Canvas Configuration List window displays, as shown in Figure 45 on page 109.



SJ000226

Figure 45. Display Canvas Configurations

The following are descriptions of the buttons that are available on the Display Canvas Configurations window.

Load Canvas
Select a graph name and click **Load Canvas** to load a canvas of up to eight graphs onto the Performance Monitor feature.

Figure 46 on page 110 shows an example of what you see when you select two graphs and click the **Load Canvas** button.

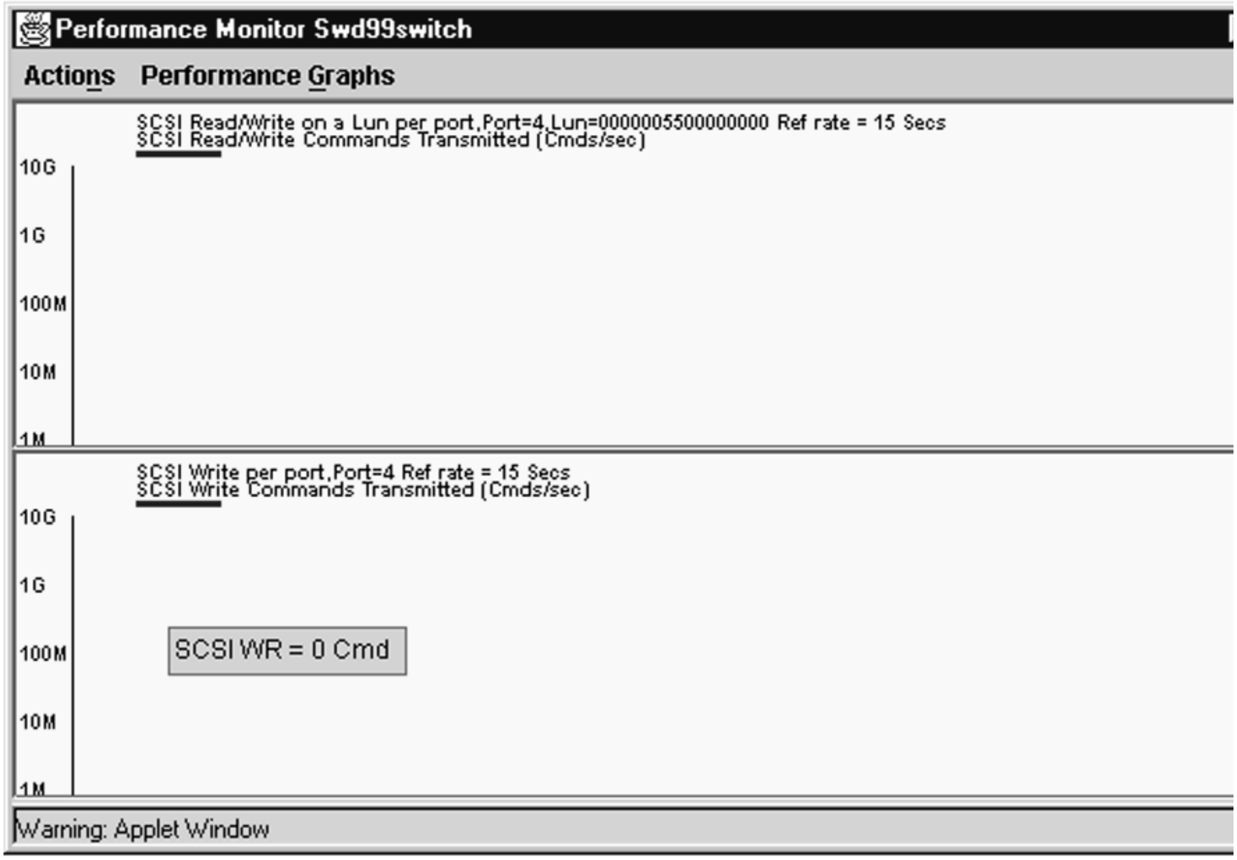


Figure 46. Load Canvas example

Edit Canvas

Click **Edit Canvas** to make changes to a canvas or to change configurations.

Figure 47 on page 111 shows an example of what you see when you click the **Edit Canvas** button.

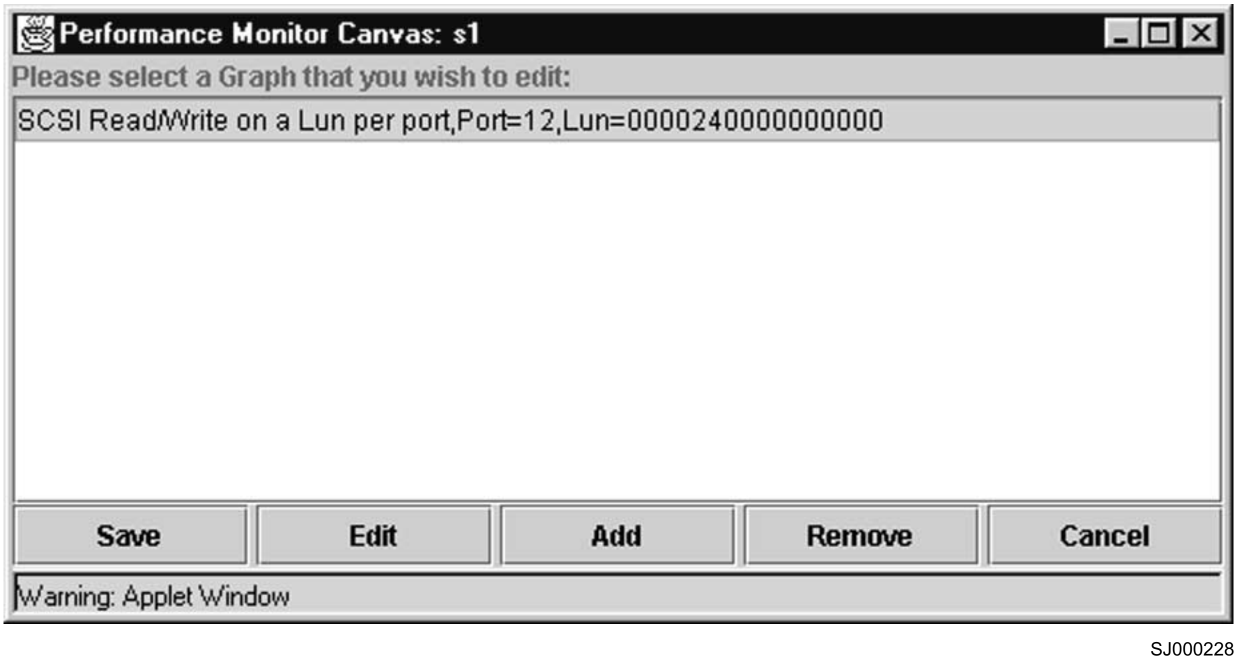


Figure 47. Edit Canvas example

Following is a description of the choices that are available from the Edit Canvas display.

Save Click to save an edited graph.

Edit Click to alter a graph.

Add Click to add a graph to a canvas. You are prompted to choose Basic or Advanced Monitoring. For more information, see "Basic Monitoring menu" on page 117 and "Advanced Monitoring menu" on page 117.

Remove
Click to delete a graph. You are prompted to choose the graph that you want to delete.

Cancel
Click to exit the window without making any changes.

Figure 48 on page 112 shows an example of the data entry window that you see when you click the **Edit Canvas** button.

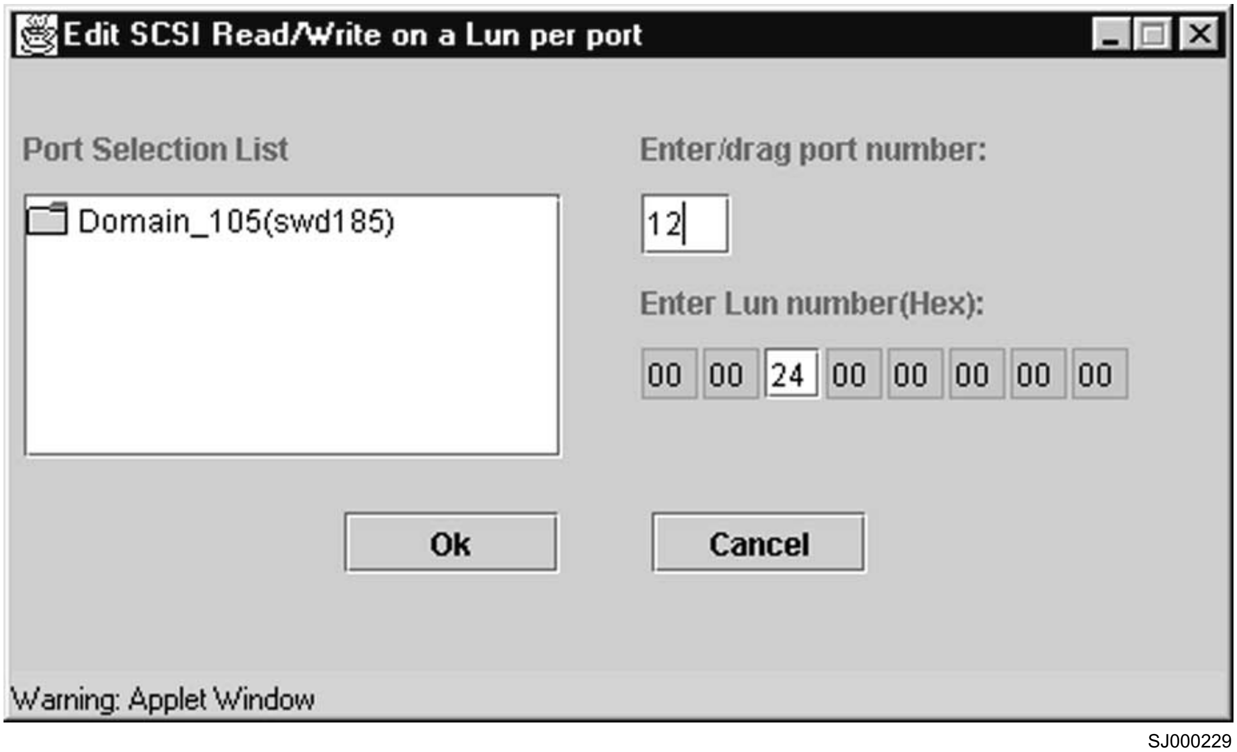


Figure 48. Edit Canvas data entry window

Perform the following steps to choose the port and LUN that you want to graph or configure:

1. Double-click on the folder in the **Port Selection List** field. A drop-down list of ports displays.
2. Select the port that you want to monitor or change by using one of the following methods:
   a. Type the port number in the **Enter/drag port number** field.
   b. Drag the port file from the **Port Selection List** field to the **Enter/drag port number** field.
3. Type a LUN number in the **Enter Lun Number (Hex)** field.

   You can only type four LUN numbers at a time.
4. Click **OK**.

Note: If you try to enter more than four LUN numbers, a warning window displays.

Copy Canvas

Click **Copy Canvas** to copy the highlighted canvas configuration from the list to the switch flash. You are prompted to type in the name and description of the canvas that you want to copy your chosen graph to.

Figure 49 on page 113 shows an example of what you see when you click the **Copy Canvas** button.

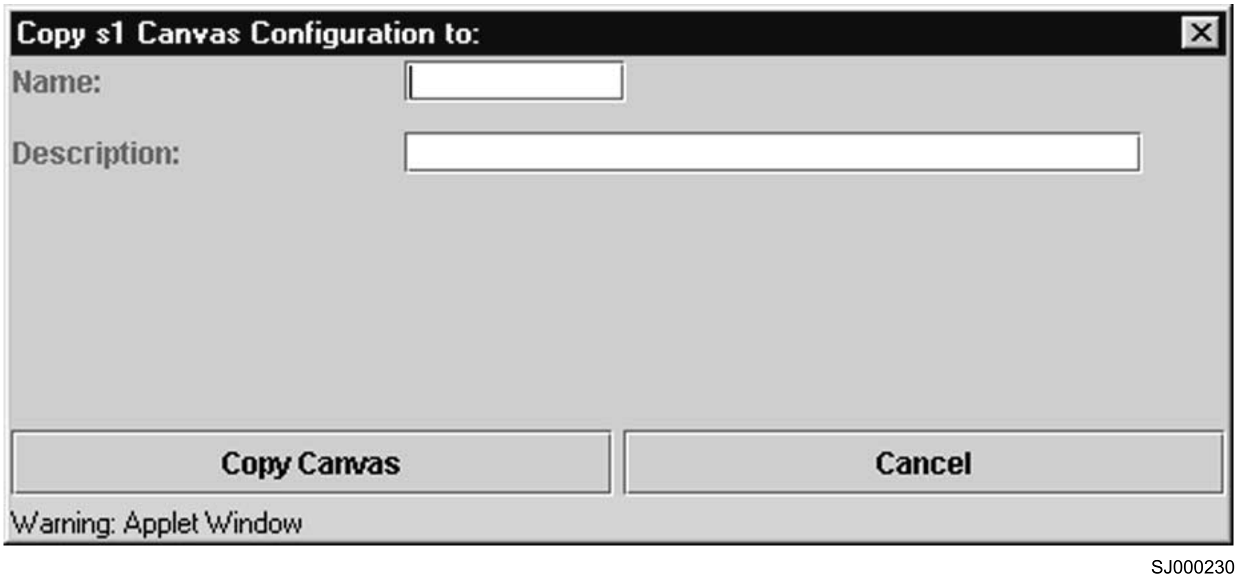


Figure 49. Copy Canvas example

Rem Canvas
Click **Rem Canvas** to remove a highlighted canvas from the list and the switch flash. You are prompted with a warning that you are about to delete the selected canvas.

Save Current Canvas Configuration menu: The Save Current Canvas Configuration menu allows you to save the currently configured canvas to the switch. It uses a canvas name and a brief description to save the canvas.

Perform the following steps to access the Save Current Canvas Configuration menu:

1. Select the **Performance** icon from the Switch view.
2. Select the Actions menu.
3. Select the Save Current Canvas Configurations option.

The Canvas Configuration Save menu displays, as shown in Figure 50 on page 114.

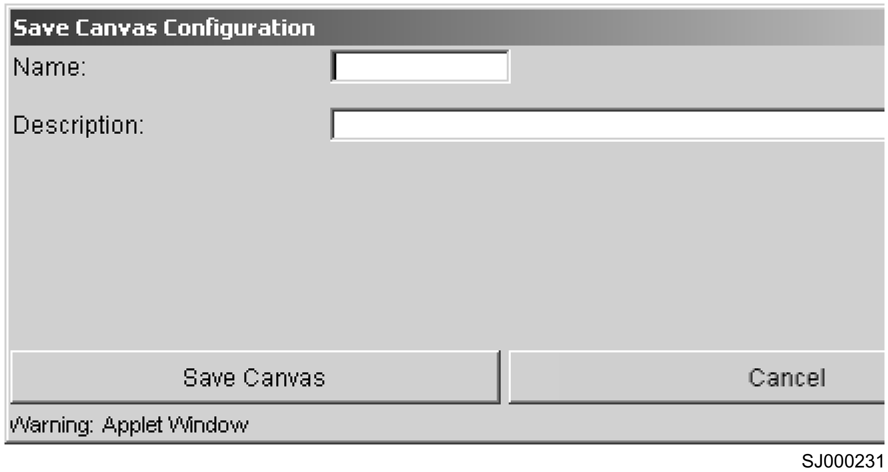


Figure 50. Canvas Configuration Save menu

Following is a description of the buttons that are available on the Save Current Canvas Configuration menu:

Save Canvas
Click to save the canvas to the switch flash.

Cancel
Click to close the window without any action.

If the canvas already exists, a confirmation screen displays, as shown in Figure 51.

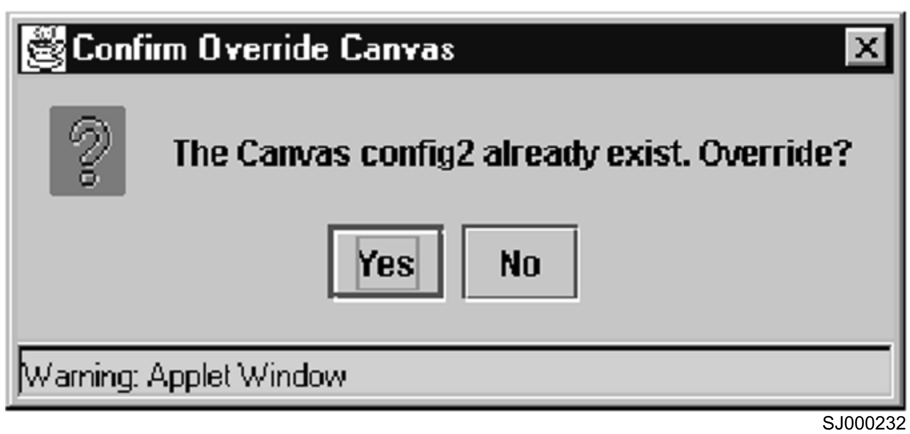


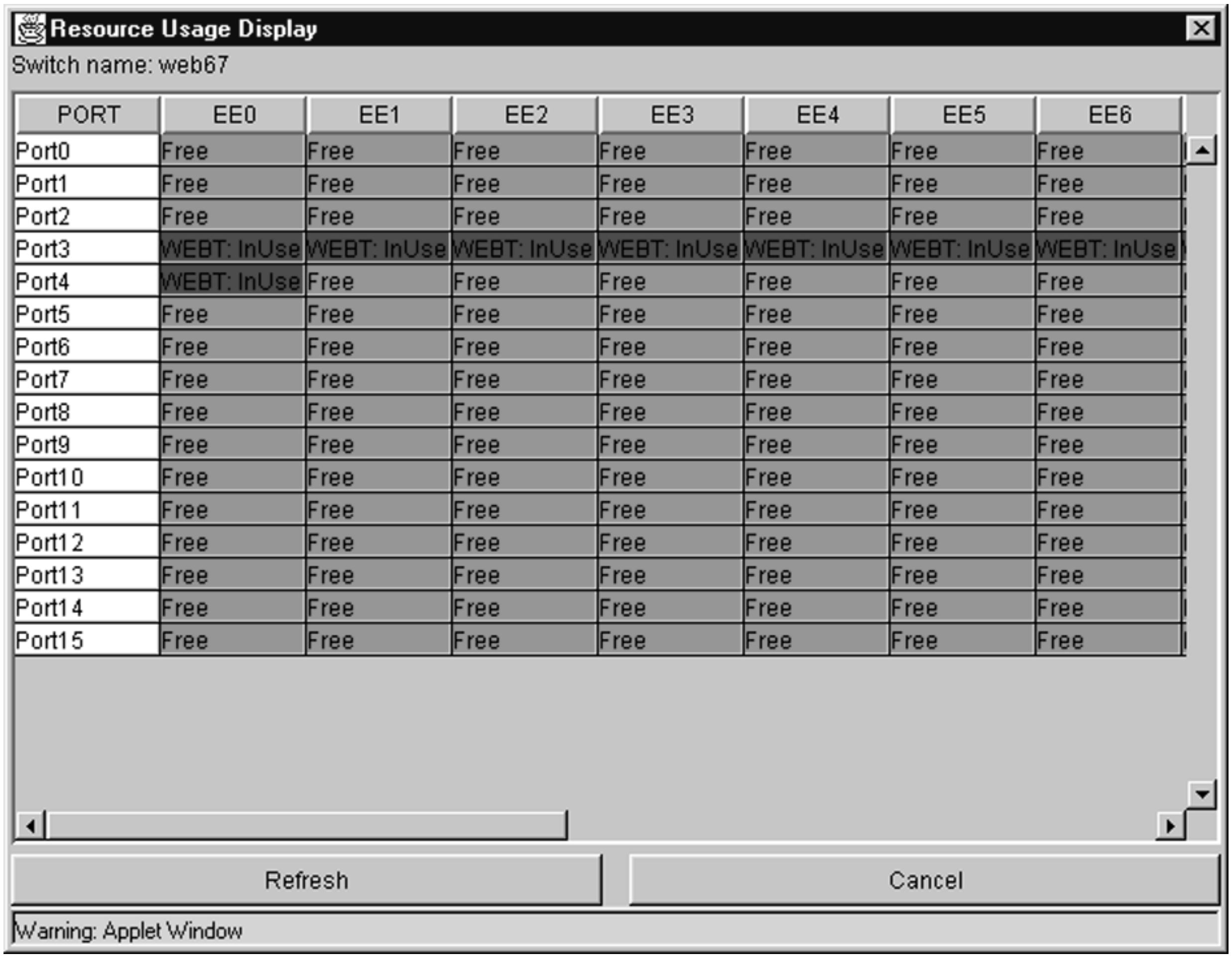
Figure 51. Confirm Override Canvas

Use the override option when you need to update an existing canvas.

Resource Usage Display menu: The Resource Usage Display menu allows you to view the resources that are allocated for end-to-end use as well as providing filter-based monitoring for each port.

Perform the following steps to access the Resource Usage Display menu:
1. Select the **Performance** icon from the Switch view.
2. Select the Actions menu.
3. Select the Resource Usage Display option.

The Resource Usage Display menu displays, as shown in Figure 52.



SJ000232

Figure 52. Resource Usage Display menu

Following is a description of the buttons that are available in the Resource Usage Display menu.

Refresh
Click to reload the window immediately. The window automatically reloads either every 5 seconds, or every 15 seconds. The exact amount of time between reloads is listed at the top of every graph.

Cancel
Click to close the window without any action.

Print All Graphs: The Print All Graphs menu allows you to print all the graphs on a selected canvas.

Perform the following steps to access the Print All Graphs menu:

1. Select the **Performance** icon from the Switch view.
2. Select the Actions menu.
3. Select the Print All Graphs option.

A dialog box displays, as shown in Figure 53.

Figure 53. Print All Graphs

4. Click **Yes** to accept.

   The Print dialog box displays, as shown in Figure 54. Select print options such as printer choice, print to a file, print properties, the number of pages to print, and the number of copies.

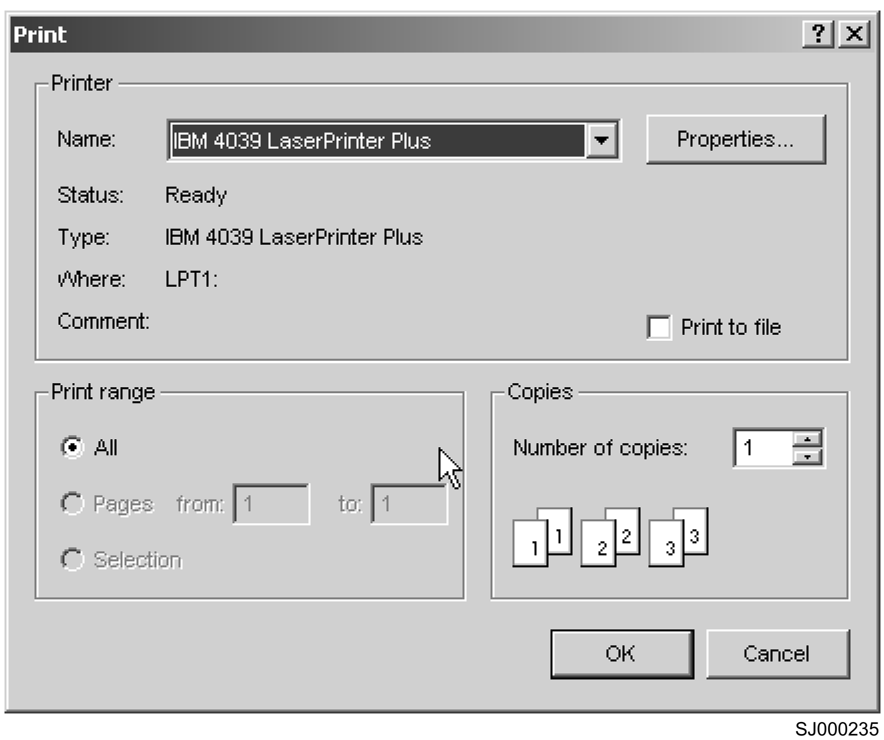


Figure 54. Print dialog box

5. Click **OK**.

   Each report prints two pages. The first is the banner page with the name of the graph, and the second is the actual graph.

Performance Graphs menu

The Performance Graphs menu is made up of the following sub-menus:

- The Basic Monitoring menu
- The Advanced Monitoring menu

Basic Monitoring menu: The Basic Monitoring menu allows you to create graphs that monitor the functions of switches and ports, such as performance and traffic. Unlike the Advanced Monitoring graphs, Basic Monitoring graphs do not display device-specific information.

Perform the following steps to access the Basic Monitoring menu:

1. Select the **Performance** icon from the Switch view.
2. Select the Performance Graphs menu.
3. Select the Basic Monitoring option.

Table 7 lists the types of graphs that are available from the Basic Monitoring menu.

Table 7. Graphs displayed on a Basic Monitoring canvas

Scope	Graph name	Graph type	Description
Port	Port Throughput	Line chart	Displays the performance of a port based on four-byte frames that are received and transmitted.
Switch	Switch Aggregate Throughput	Line chart	Displays the aggregate performance of all ports of a switch.
Switch	Switch Throughput Utilization	Horizontal chart	Displays the port throughput at the time the sample is taken.
Switch	Port Error	Line chart	Displays a line of CRC errors for a given port.
Switch	Switch Percent Utilization	Horizontal bar chart	Displays the percentage of usage of a chosen switch at the time the sample is taken.
Switch	Port SnapShot Error	Vertical bar chart	Displays the CRC error count between sampling periods for all the ports on a switch.

Advanced Monitoring menu: Advanced Monitoring is an optionally-licensed feature. The Advanced Monitoring menu allows you to create graphs that monitor switch and port functions such as traffic and performance that is device-specific.

Table 8 lists the types of graphs that are available from the Advanced Monitoring menu.

Table 8. Graphs displayed on an Advanced Monitoring canvas

Scope	Graph name	Graph type	Description
Switch	SID/DID Performance	Line chart	Charts the traffic between an SID (or WWN) and a DID (or WWN) pair on the switch being managed. See Figure 55 on page 119.

Table 8. Graphs displayed on an Advanced Monitoring canvas (continued)

Scope	Graph name	Graph type	Description
Switch	SCSI Commands	Line chart	Charts the total number of Read or Write commands on a given port to a specific LUN. Provides the following choices: • SCSI Read/Write on a LUN per port • SCSI Read on a LUN per port • SCSI Write on a LUN per port • SCSI Read/Write per port • SCSI Read per port • SCSI Write per port See Figure 57 on page 121.
Switch	SCSI vs IP	Vertical bar chart	Shows percentage of SCSI vs IP frame traffic on each individual port. See Figure 58 on page 122.
Switch	ALPA Error	Line chart	Displays CRC errors for a given port and a given AL_PA. See Figure 60 on page 124.

SID/DID Performance graph: When you select the SID/DID Performance graph, you are prompted with a data entry window where you choose the SID and DID to be charted. Figure 55 on page 119 shows the data entry window that you see when you choose to create an SID/DID Performance graph.

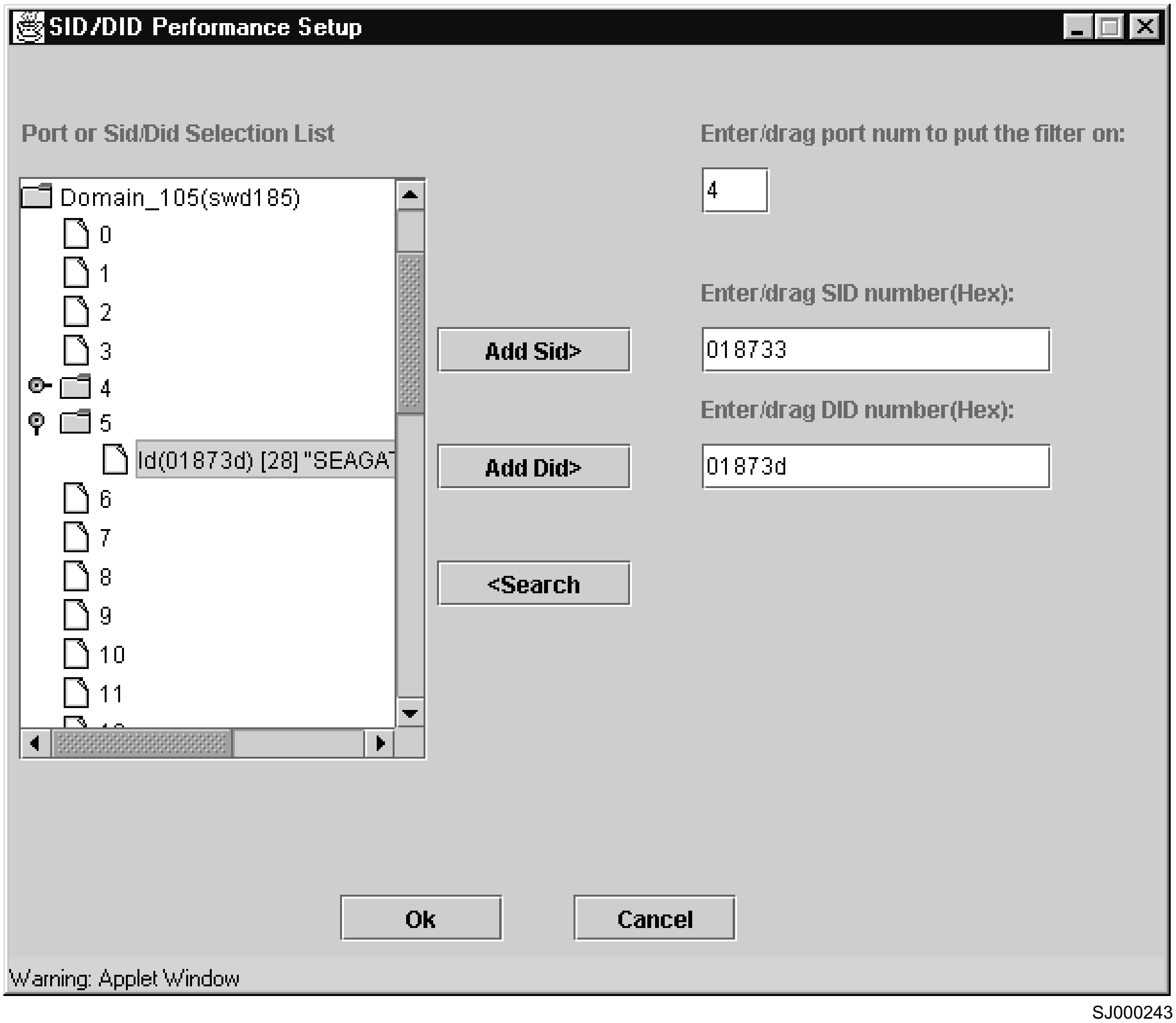


Figure 55. SID/DID Performance Setup data entry window

Perform the following steps to choose the port and SID/DID that you want to graph:

1. Double-click on a folder in the **Port or SID/DID Selection List** field. A drop-down list of ports displays.
2. Select the port that you want to monitor or change using one of the following methods:
   - Type the port number in the **Enter/drag port num to put the filter on** field.
   - Drag the port folder from the **Port or SID/DID Selection List** field to the **Enter/drag port num to put the filter on** field.
3. Select the port folder, or the small icon that is displayed next to it. A drop-down list of SID/DID files displays.
4. Select the SID/DID numbers that you want to graph using one of the following methods:
   - Type the SID number in the **Enter/drag SID number (Hex)** field. Repeat for the DID number.
   - Drag the SID file from the **Port or SID/DID Selection List** field to the **Enter/drag SID number (Hex)** field. Repeat for the DID number.
   - Click **OK**.

A graph for the chosen port displays.

Figure 56 shows an example of an SID/DID graph, which displays the traffic between an SID and a DID pair.

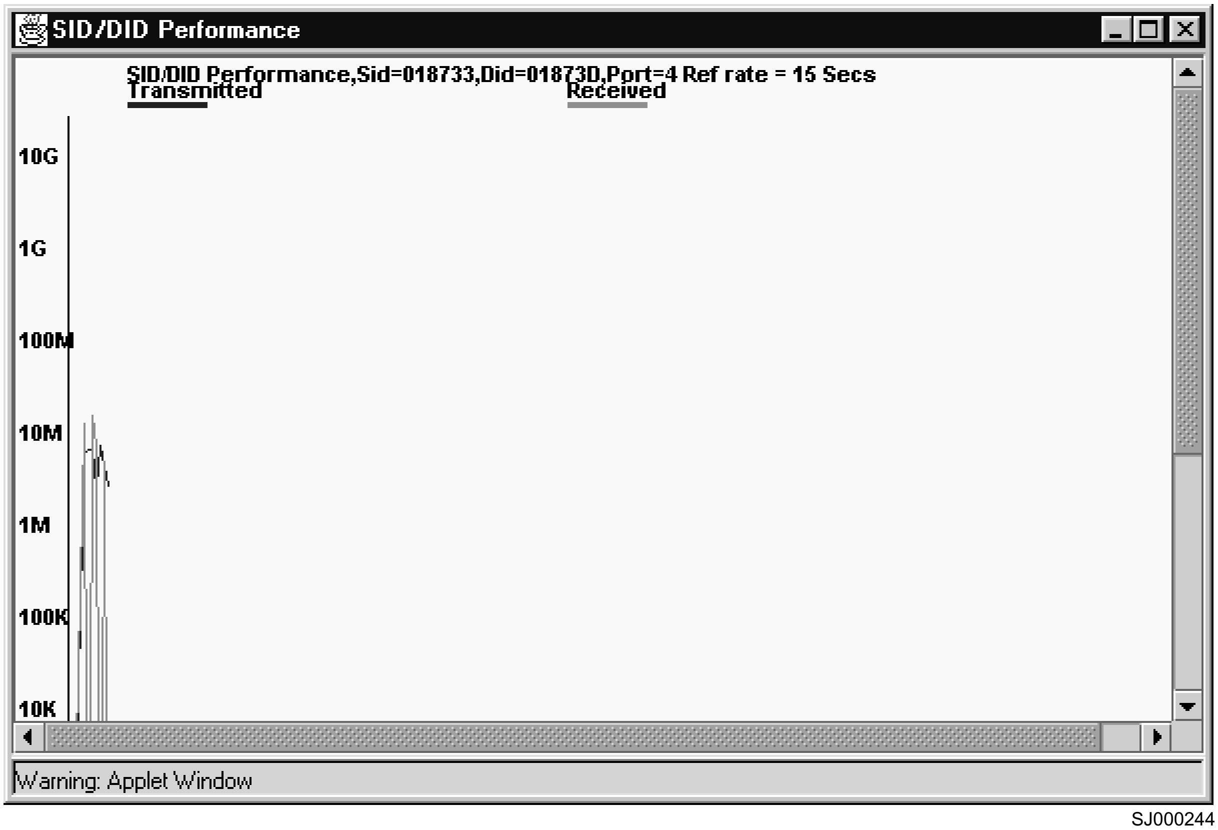


Figure 56. SID/DID Performance graph

SCSI Commands graph: When you select the SCSI Commands graph, the following options are displayed in a pull-down menu:

- SCSI Read/Write on a LUN per port
- SCSI Read on a LUN per port
- SCSI Write on a LUN per port
- SCSI Read/Write per port
- SCSI Read per port
- SCSI Write per port

Each graph prompts you with a data entry window to select the port and LUN to be monitored, as shown in Figure 57 on page 121.

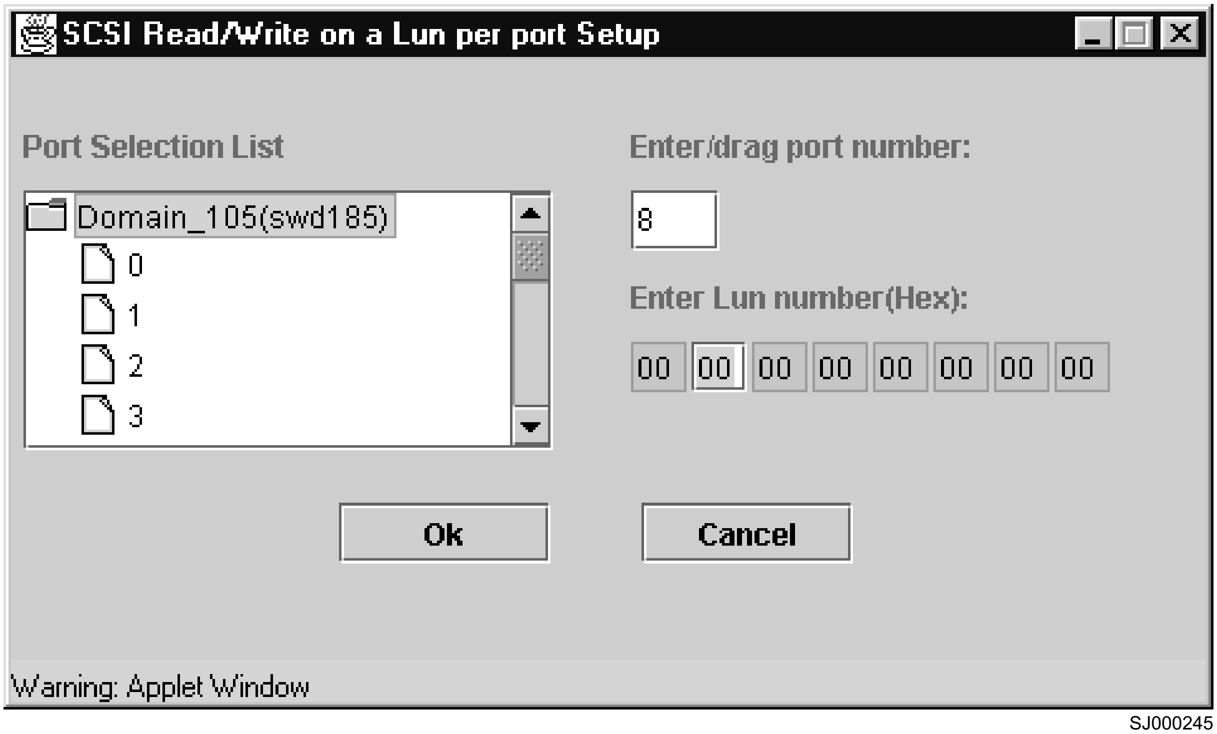


Figure 57. SCSI Commands Graph data entry window

Perform the following steps to choose the port and LUN to monitor:

1. Double-click on the folder in the **Port Selection List** field.

   A drop-down list of ports displays.
2. Select the port that you want to monitor or change using one of the following methods:
   - Type the port number in the **Enter/drag port number** field.
   - Drag the port file from the **Port Selection List** field to the **Enter/drag port number** field.
3. Type a LUN number in the **Enter LUN Number (Hex)** field.

   Note: You can enter only four LUN numbers at a time. If you try to enter more than four LUN numbers, a warning window displays.
4. Click **OK**.

   A graph displaying the total number of Read or Write commands on a given port to a specific LUN displays.

Figure 58 shows an example of a SCSI graph, which uses the Write on a LUN per port option.

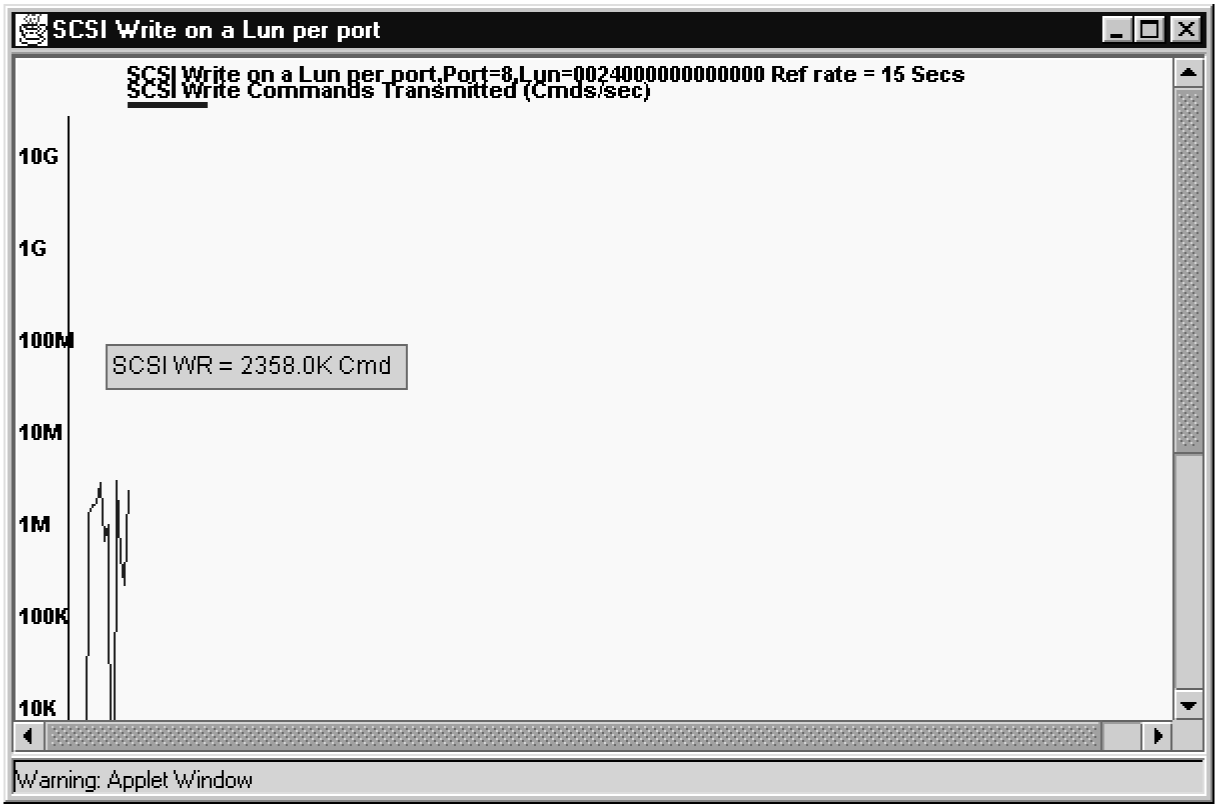


Figure 58. SCSI Write on a LUN per port graph

SCSI vs IP graph: Figure 59 shows an example of a SCSI vs IP graph, which displays the percentage of SCSI vs IP frame traffic.

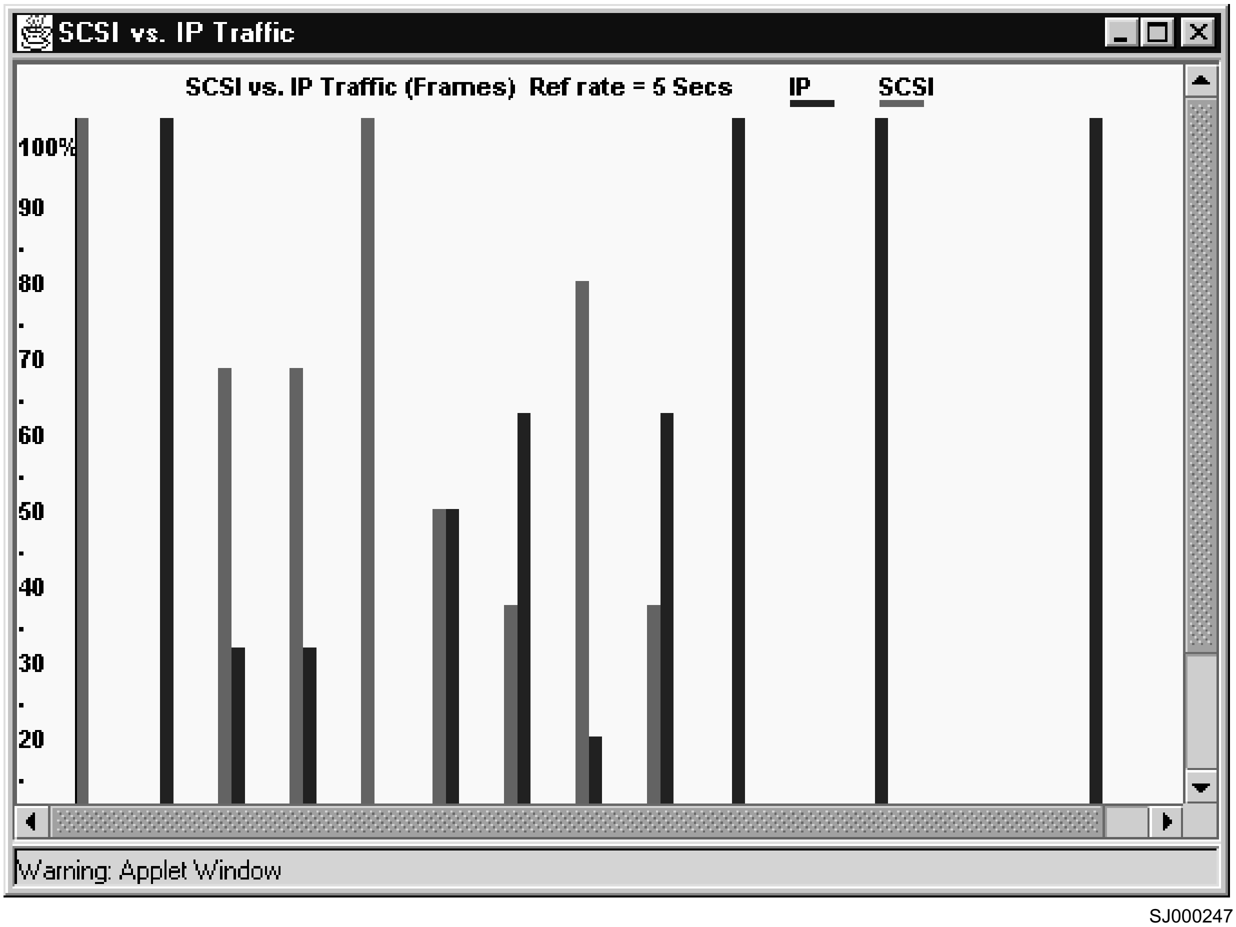


Figure 59. SCSI vs IP graph

ALPA Error graph: When you select an ALPA Error graph, you are prompted to chose the port that you want to monitor for various errors. Figure 60 is an example of the data entry window that you see when you choose to create a ALPA Error graph.

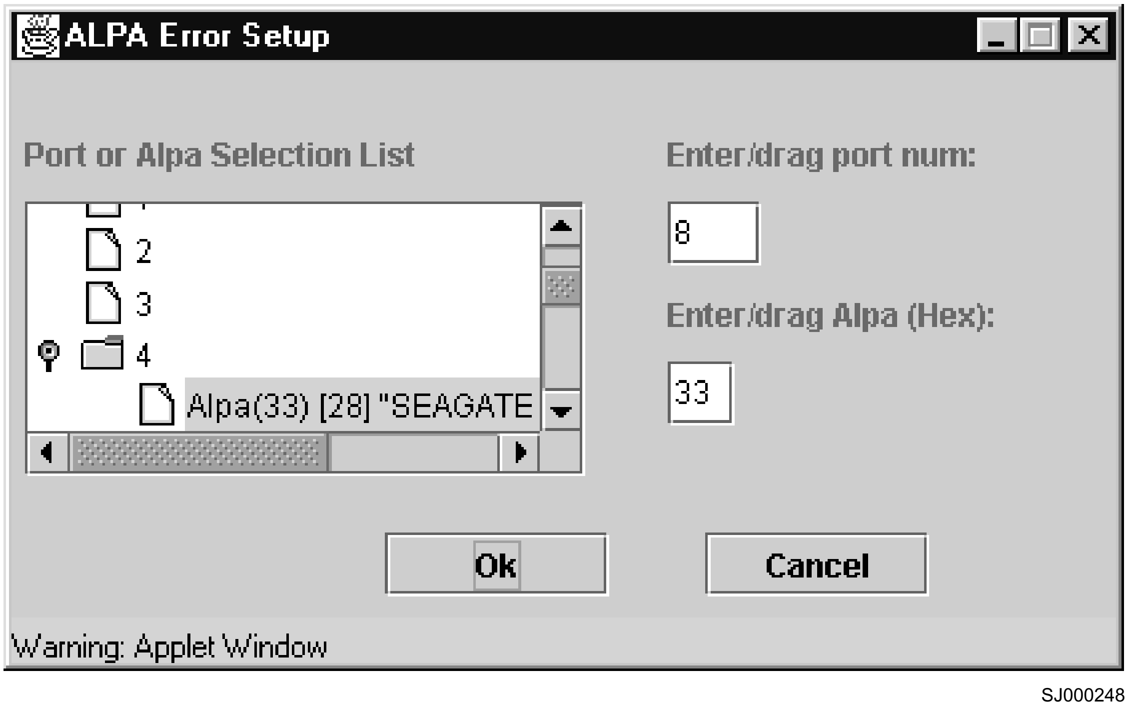


Figure 60. ALPA Error Setup data entry window

Perform the following steps to choose the port and AL_PA that you want to graph:

1. Double-click on the folder in the **Port or Alpa Selection List** field. A drop-down list of ports displays.
2. Select the port that you want to monitor or change using one of the following methods:
   - Type the port number in the **Enter/drag port num** field.
   - Drag the port folder from the **Port or Alpa Selection List** field to the **Enter/drag port num** field.
3. Select the port folder, or the small icon that is displayed next to it. A drop-down list of SID/DID files displays.
4. Select the AL_PA number that you want to graph using one of the following methods:
   - Type the AL_PA number in the **Enter/drag Alpa (Hex)** field.
   - Drag the AL_PA file from the **Port or Alpa Selection List** field to the **Enter/drag Alpa (Hex)** field.
5. Click **OK**.

   An ALPA Error graph displays.

Figure 61 on page 125 shows an example of an ALPA Error graph, which displays CRC errors for a given port and a given AL_PA.

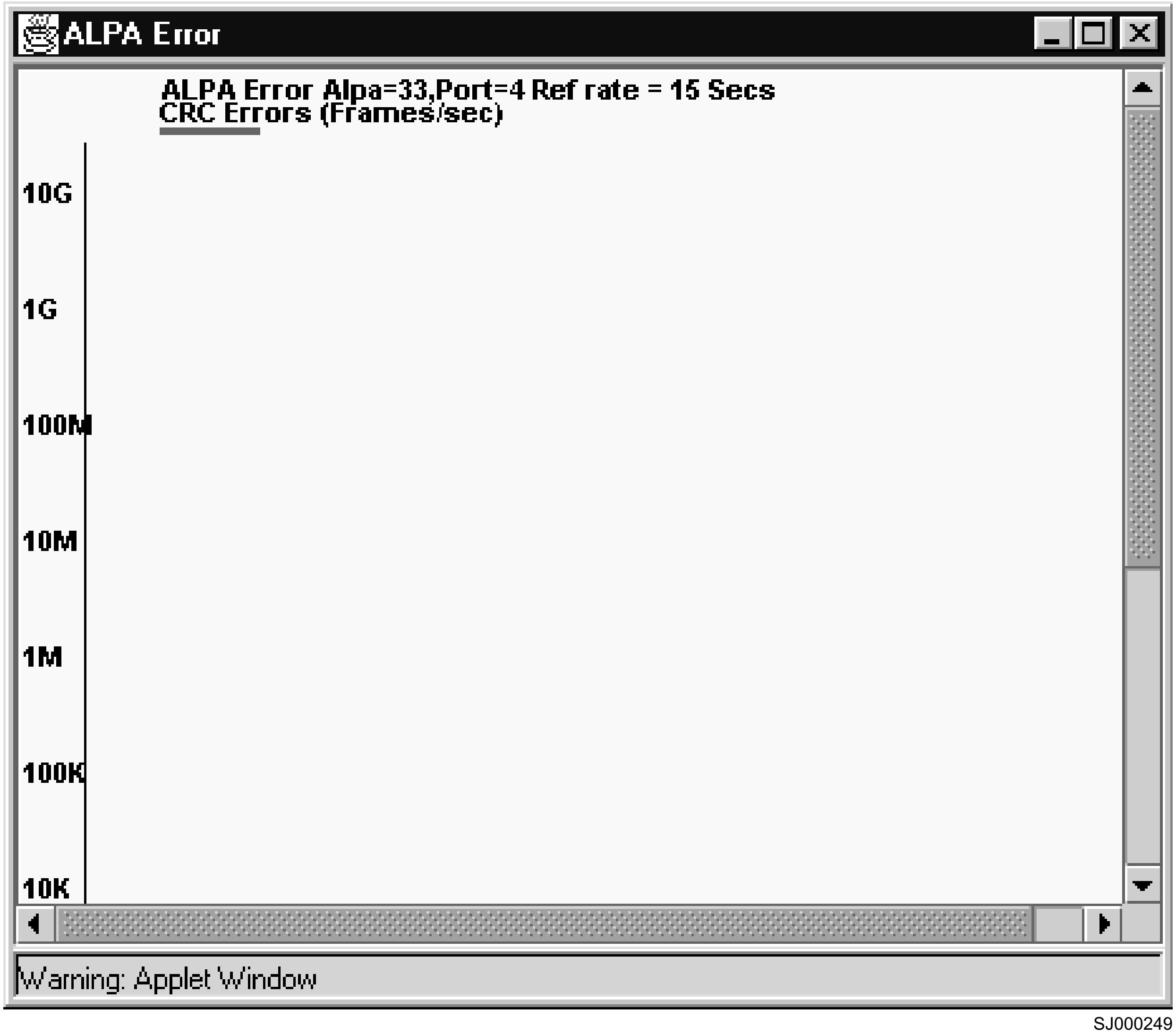


Figure 61. ALPA Error graph

Additional options

Additional options are available for some graphs in the Performance Monitor feature. You can access these options either by right-clicking on a graph or by using the Tools Tips.

These options are available by rolling over a graph with your mouse.

Right-click graph options

Each graph contains a variety of options that are available by pointing to a graph and click your right mouse button.

Note: Not all graphs have all options available, but every graph supports at least the first three options.

Following is a description of the possible options that are available by right-clicking your mouse in a particular graph.

Zoom In
Select to zoom in, or magnify, a single graph rather than viewing multiple graphs on one canvas.

Remove
Select to delete any graph from the canvas.

Print
Select to print any graph.

Show Tx/Rx
Displays the number of bytes being both transmitted and received.

Show Tx
Displays the number of bytes being transmitted.

Show Rx
Displays the number of bytes being received.

Show Crc
Displays the amount of CRC errors being transmitted.

Tools Tips

Each graph provides additional information when you roll your mouse over a graph.

Note: Not all graphs have all options available, but almost every graph supports at least one Tools Tip.

Following is a description of all the possible Tools Tips information that is available.

Top 5 busiest port(s)
Displays the five ports that are transmitting and receiving the most bytes.

Tx=0.0, Rx=0.0
Displays the number of bytes being transmitted and received.

CRC=0
Displays the number of CRC errors being transmitted on a port.

SCSI RW=0
Displays the number of SCSI commands being read or written on a port or on a given port to a specific LUN.

SCSI RD=0
Displays the number of SCSI commands being read on a port or on a given port to a specific LUN.

SCSI WR=0
Displays the number of SCSI commands being written on a port or on a given port to a specific LUN.

Administrative Interface

The Administrative Interface provides access to the administrative functions through the following tabs:

- Switch Settings
- Network Config
- Firmware/Upgrade
- SNMP
- License Admin
- Report
- Port Settings

- User Admin
- Configure
- Routing
- Trunk Information
- QuickLoop
- Remote Switch
- Extended Fabric

Note: The Administrative Interface requires administrative privileges. After you enter an administrative login, administrative privileges remain available until you close the Web browser.

Perform the following steps to access the Administrative Interface:

1. Launch the Web browser.
2. Type the switch name or IP address in the **Location/Address** field and press Enter.

   TotalStorage Specialist launches, displaying the Fabric view.
3. Click the **Admin** icon on the switch panel.

   The Enter Network Password dialog displays, as shown in Figure 62.

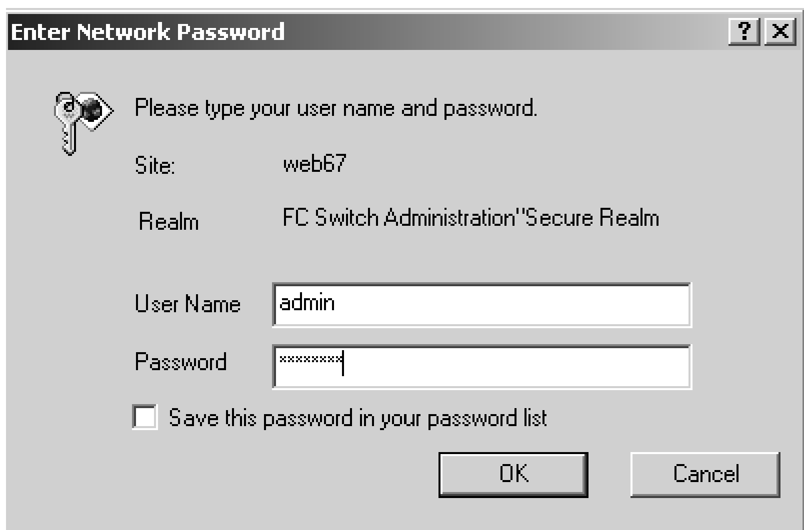


Figure 62. Enter Network Password dialog box

4. Type your user name and password. The logon account must have administrative privileges.
5. Click **OK**.

   The Administrative Interface displays, with the **Switch Settings** tab selected by default, as shown in Figure 63 on page 128.

For each tab at the top of the Administrative Interface, a message area at the bottom of the Administrative Interface reveals the status of the changes that were applied to the switch. Expand or compress the message area by clicking on the up or down arrows in the upper-left corner of the message area.

All tabs in the Administrative Interface are consistent with the tabs of the other interfaces with the exception of the Trunk Information tab and the Report tab, which is a read-only tab and has only the **Close** button function.

Switch Settings tab

You can use the **Switch Settings** tab to manage basic switch setup for items such as switch name, switch domain ID, and enabling and disabling the switch and compatibility modes. The **Switch Settings** tab is shown in Figure 63.

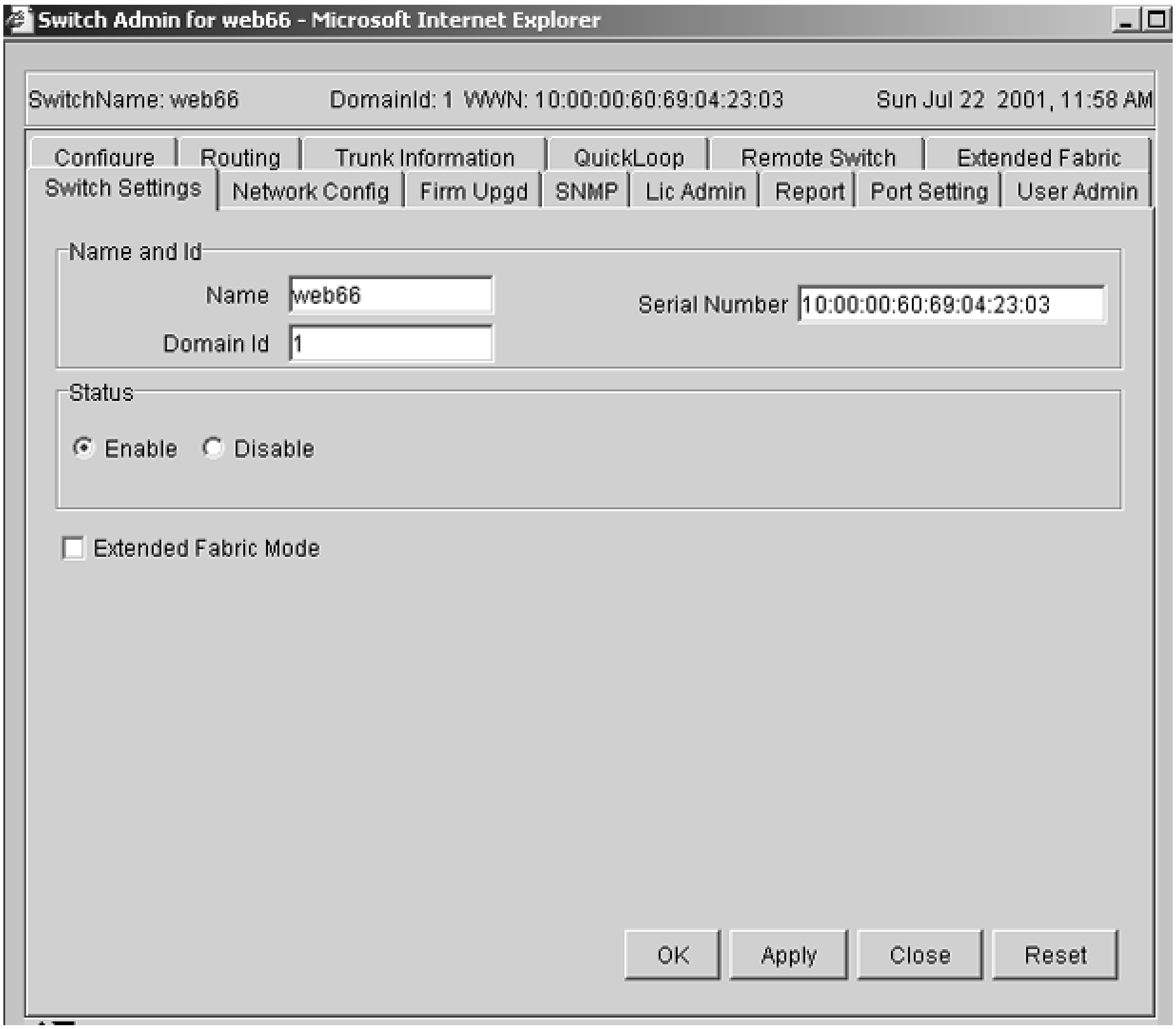


Figure 63. Switch Settings tab

Following is a description of the fields in the **Switch Settings** tab.

Name Type the switch name. Type a new name to change a name in this field.

Domain ID
Displays or sets the switch domain ID. Domain IDs must be unique within a fabric. To change the domain ID, type a new domain ID in this field. Use a number from 1 - 239 for normal operating mode (FCSW compatible) and a number from 0 - 31 for VC-encoded address format mode (backward compatible to 3534 switch).

Serial Number
: Displays the serial number of the switch.

Status
: Click **Enabled** to enable the switch, or click **Disabled** to disable the switch.

Extended Fabric Mode
: Select the box to allow ports to be configured for long distance, or clear to turn the option off.

OK Click to exit the Administrative Interface and save any changes.

Apply Click to save any changes made to this tab and remain in the current tab. Click **Apply** when making changes incrementally.

Close Click to exit the Switch Admin view. If changes have been made and not applied by clicking **Apply**, a dialog box is presented. It allows the changes to be applied or deleted.

Reset Click to reset the tab to the last set of saved changes.

Network Config tab

You can use the **Network Config** tab to manage the IP networking functions of the switch. Fill in the Ethernet, FC IP, and SYSLOG fields. The **Network Configuration** tab is shown in Figure 64 on page 130.

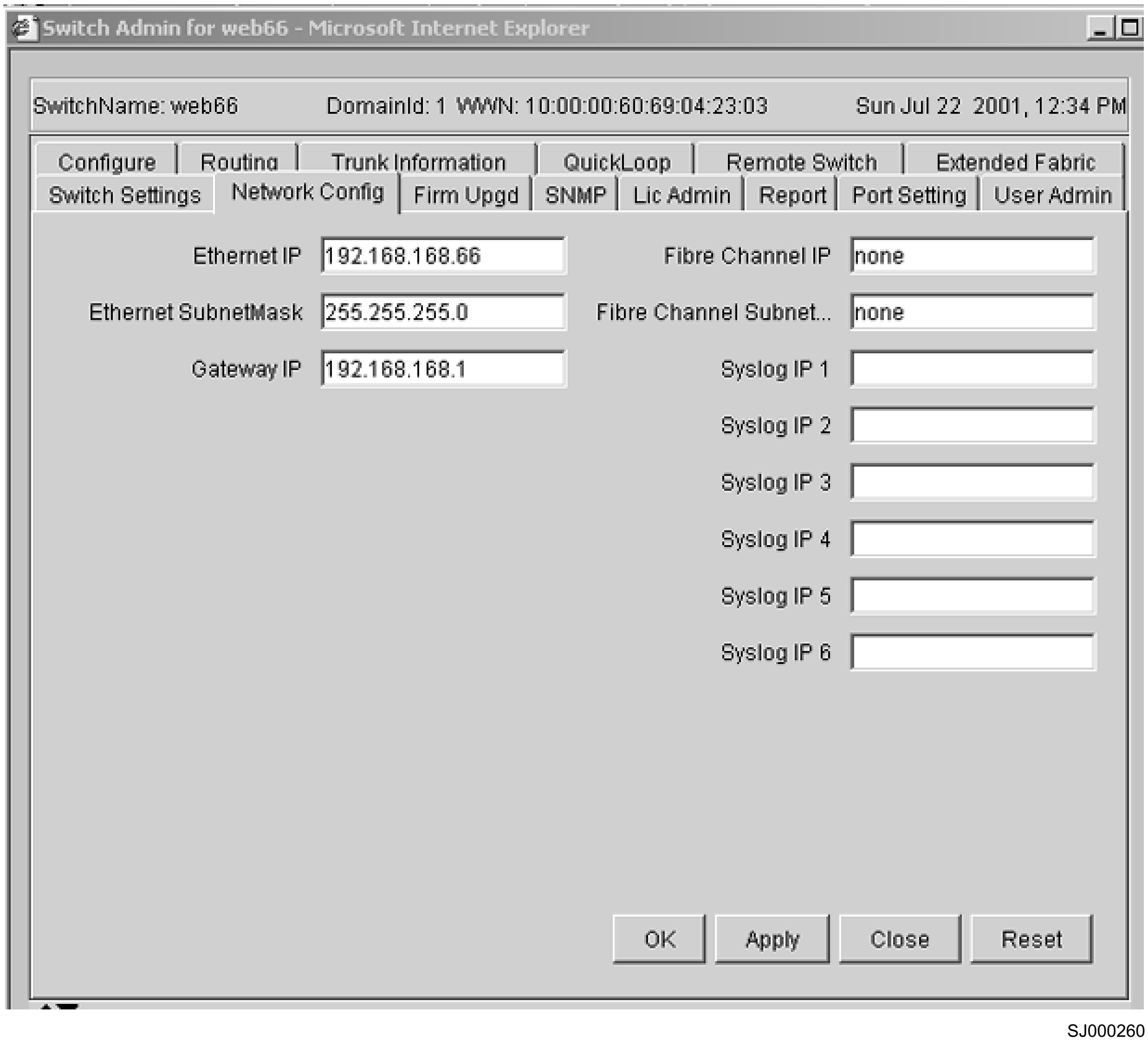


Figure 64. Network Config tab

Following is a description of the fields in the **Network Config** tab.

Ethernet IP
Displays the Ethernet IP address.

Ethernet SubnetMask
Displays the Ethernet SubnetMask address.

Gateway IP
Displays the gateway IP address.

Fibre Channel IP
Displays the fibre-channel IP address.

Fibre Channel SubnetMask
Displays the fibre-channel SubnetMask address.

Syslog IP 1 - 6
Displays the six Syslog IP addresses that you can configure.

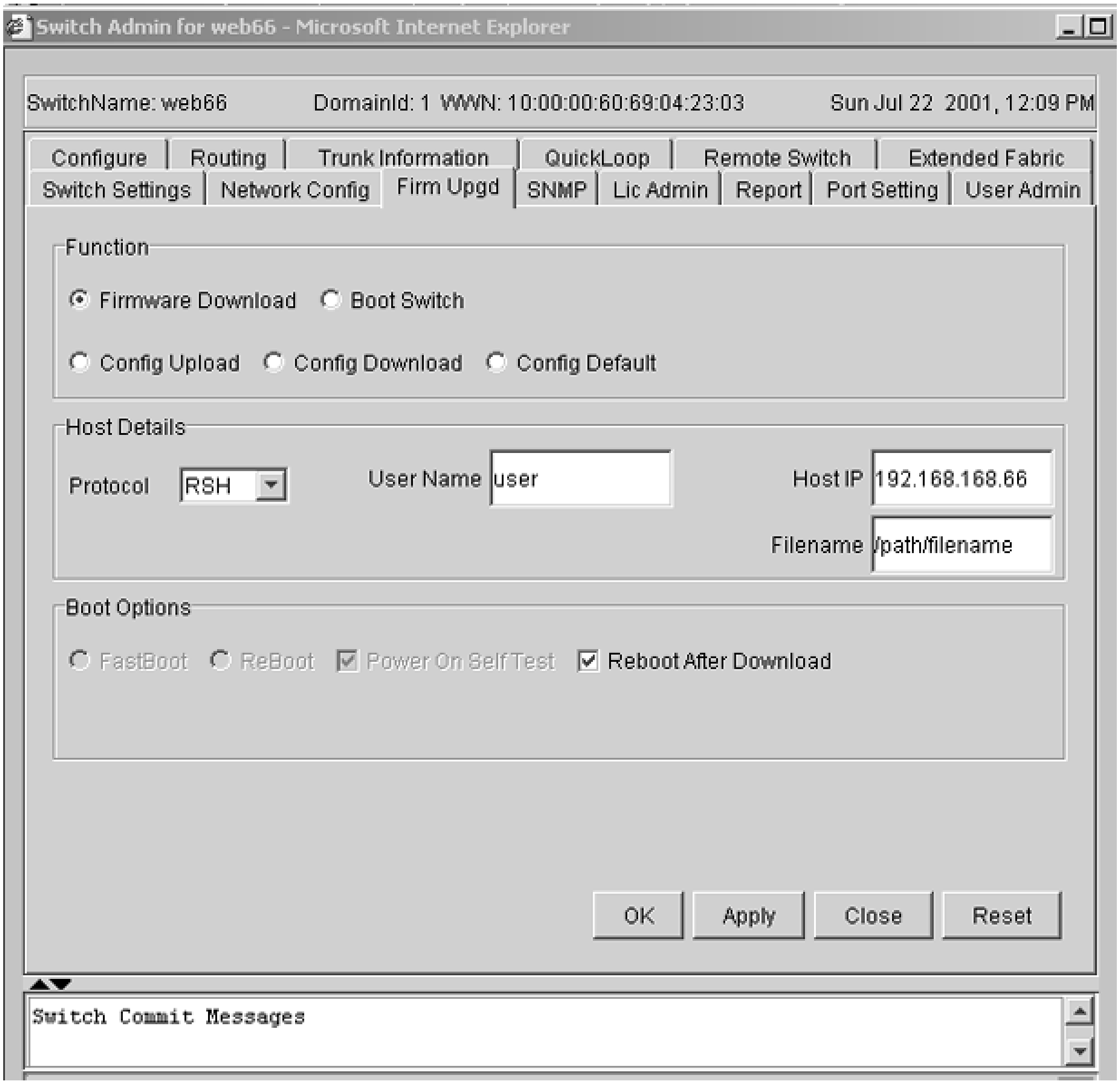
For a description of the **OK, Apply, Close** and **Reset** buttons, see “Switch Settings tab” on page 128.

Firmware/Upgrade tab

You can use the **Firmware/Upgrade** tab to complete the following tasks:

- Download firmware
- Start the switch
- Upload a configuration file to the host
- Download the configuration from a file to the switch
- Reset the configuration to the default value
- Select the download protocol (FTP or RSH)
- Select the location and authorization information and switch restart directions

The **Firmware/Upgrade** tab is shown in Figure 65 on page 132.



SJ000253

Figure 65. Firmware/Upgrade tab

Following is a description of the fields in the **Firmware/Upgrade** tab.

Function section

Firmware Download
: Select to download firmware.

Boot Switch
: Select to start the switch.

Config Upload
: Select to upload the configuration file to the specified host. This saves the configuration file to the switch using the specified filename (full path). The user name and password must be valid for the specified host, and the file path must be read-write capable.

Config Download
Select to download the firmware.

Config Default
Select to reset the configuration to the default value.

Host Details section

Protocol
Select a download protocol from the pull-down menu.

User name
Type the user name.

Host IP
Type the IP address of the host.

Filename
Type the filename to be downloaded.

Boot Options section

FastBoot
Select to do a fast start on the switch. This causes the switch to skip the POST.

ReBoot
Select to restart the switch.

Power On Self-Test
Select to have the switch do a POST when it restarts.

Reboot After Download
Select to have the switch restart automatically after the firmware downloads.

For a description of the **OK, Apply, Close** and **Reset** buttons, see “Switch Settings tab” on page 128.

SNMP tab

You can use the **SNMP** tab for administering the SNMP subsystem. From the **SNMP** tab you can specify the switch community string, location, trap level, and trap recipients. The **SNMP** tab is shown in Figure 66.

Note: In order for the switches to send SNMP traps, you must first use the Telnet **snmpMibCapSet** command. This enables the MIBs on all switches to be monitored.

For information about the **snmpMibCapSet** command, see the *IBM TotalStorage SAN Fibre Channel Switch 3534 Model F08 Command Reference*.

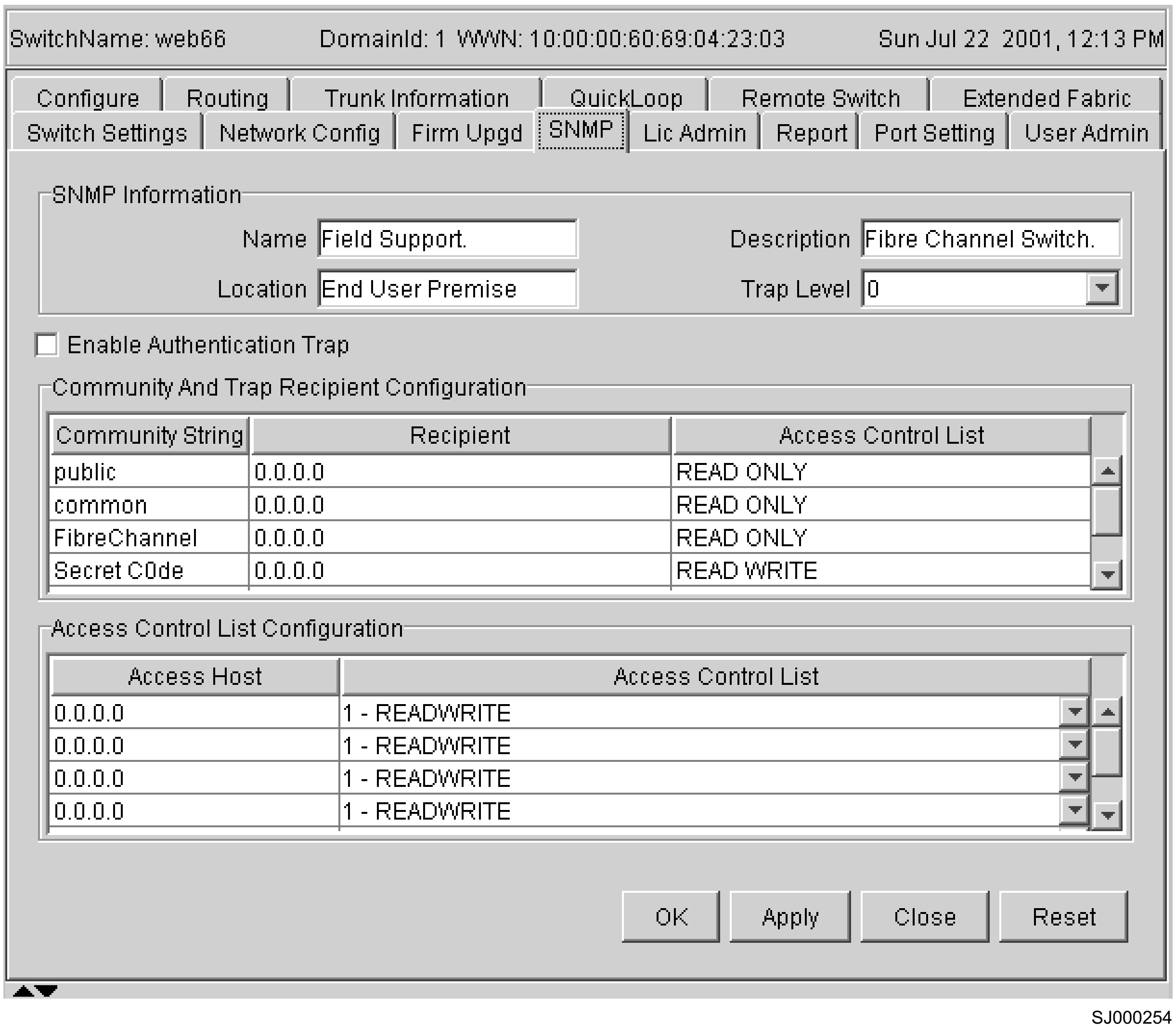


Figure 66. SNMP tab

Following is a description of the fields in the **SNMP** tab.

SNMP Information section

Name Displays or sets the contact information for the switch. The default is `Field Support`.

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

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

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

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

Community And Trap Recipient Configuration section

Community String
: Displays the community strings that are available to use. A community refers to a relationship between a group of SNMP managers and an SNMP agent, in which authentication, access control, and proxy characteristics are defined. A maximum of six community strings can be saved to the switch.

Recipient
: Displays the IP address of the trap recipient. A trap recipient receives the message that is sent by an SNMP agent to inform the SNMP management station of a critical error.

Access Control List
: Displays the read or write access of a particular community string. `READ ONLY` access means that a member of a community string has the right to view, but cannot make changes. `READ WRITE` access means that a member of a community string can view and make changes.

Access Control List Configuration section

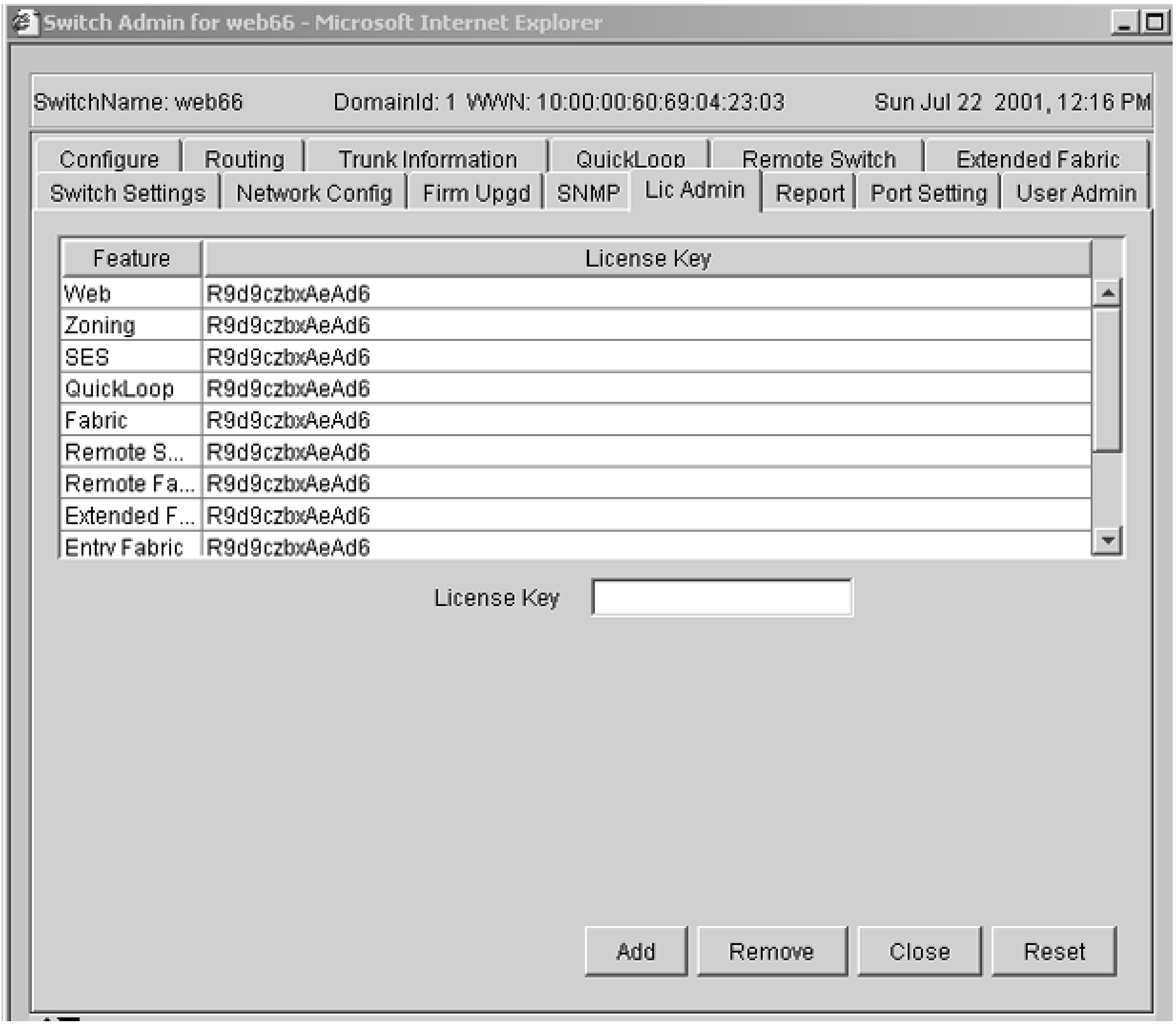
Access Host
: Displays the IP address of the host of the access list.

Access Control List
: Displays the read or write access of a particular access list. `READ ONLY` access means that a member of an access list has the right to view, but cannot make changes. `READ WRITE` access means that a member of an access list can both view and make changes.

For a description of the **OK, Apply, Close** and **Reset** buttons, see “Switch Settings tab” on page 128.

License Admin tab

You can use the **License Admin** tab to install license keys that are provided. You can use the table within the **Licence Admin** tab to remove an installed license from the switch. The **License Admin** tab is shown in Figure 67.



SJ000255

Figure 67. License Admin tab

Following is a description of the fields in the **License Admin** tab.

Feature
A list of the licenses that are installed on the switch and their associated license keys.

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

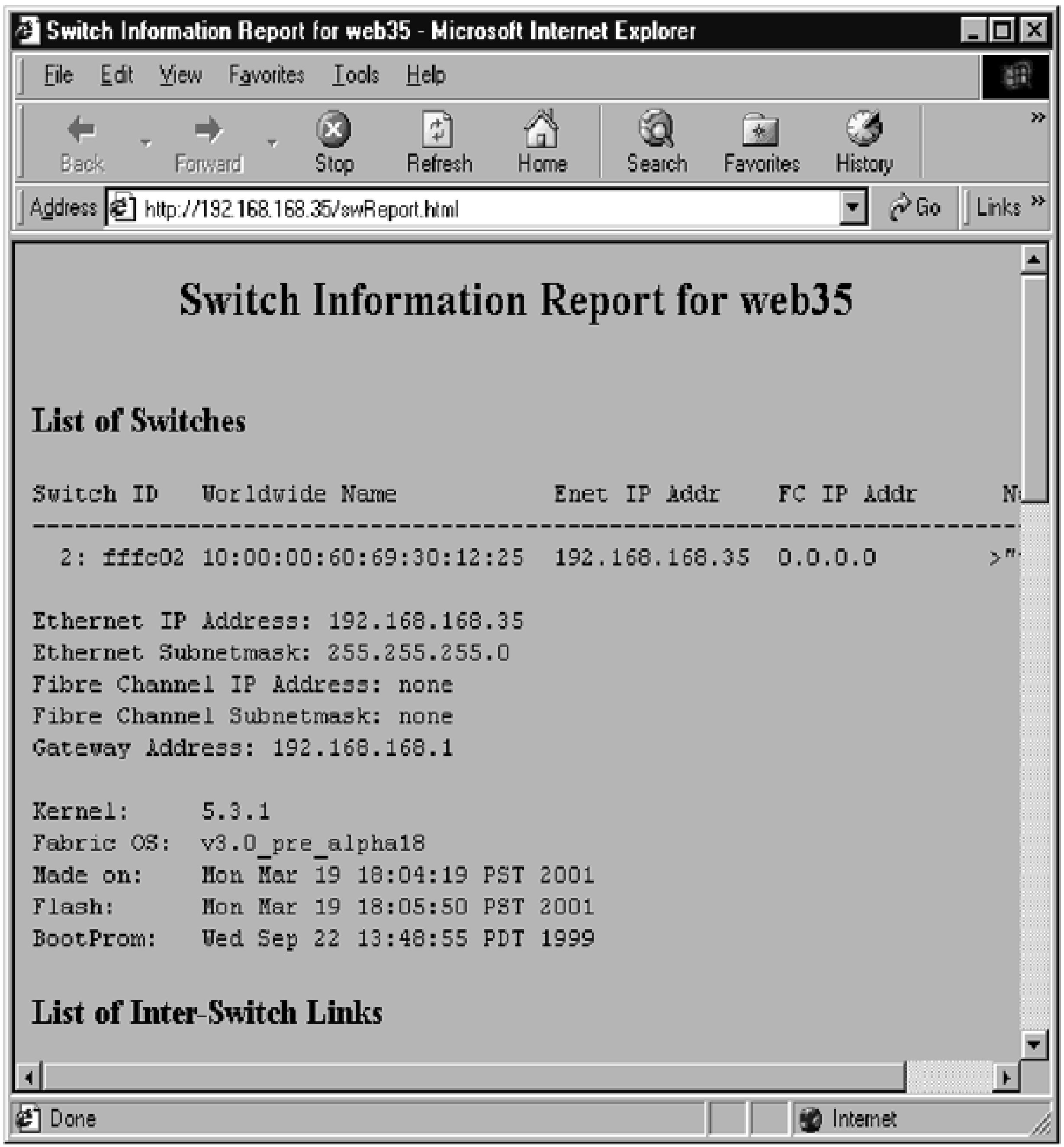
Add Click to add the specified license.

Remove
Click to remove the specified license.

For a description of the **Close** and **Reset** buttons, see “Switch Settings tab” on page 128.

Report tab

You can use the **Report** tab to display a report from the switch configuration. The Switch Information report can be generated by clicking on the corresponding link on the **Configure** tab in the Administrative Interface. This report provides information about all the switches, inter-switch links, and ports in the fabric. The **Report** tab is shown in Figure 68.

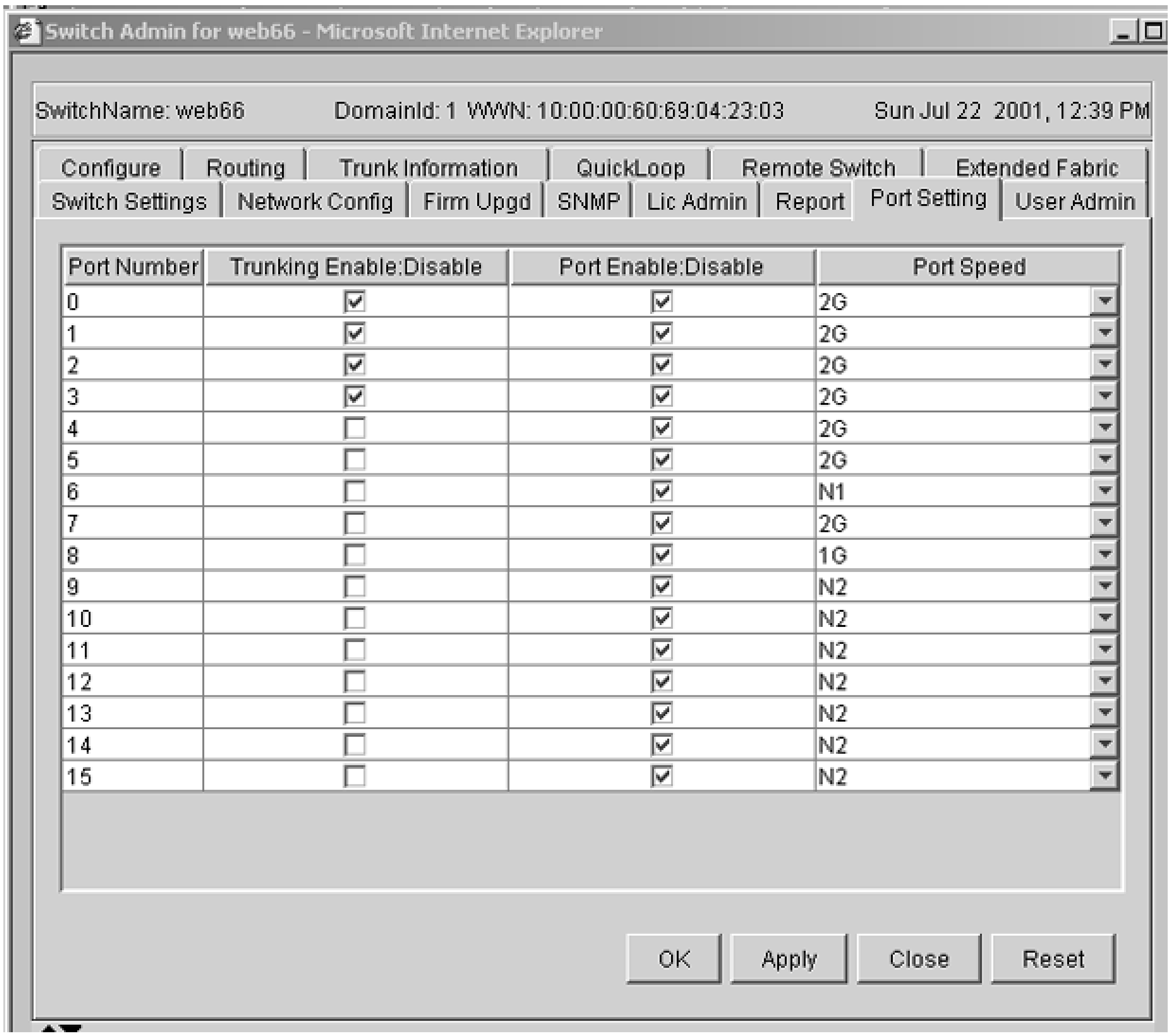


SJ000264

Figure 68. Report tab

Port Settings tab

You can use the **Port Settings** tab to enable or disable ports on the switch. From this tab you can also set port speed to 1 GB or 2 GB Autosense, as well as enable or disable Trunking. The **Port Settings** tab is shown in Figure 69.



SJ000261

Figure 69. Port Settings tab

Following is a description of the fields in the **Port Settings** tab.

Port Number
The port number.

Trunking Enable:Disable
Select to enable or clear to disable Trunking. Four trunk ports form a group, with one of them in the role of master port. The group can have member ports.

Port Enable:Disable
Select to enable or clear to disable ports on the switch.

Port Speed

Click to display the port speed. Port speed can be fixed to 1G, 2G, or Negotiate. If the speed is set to Negotiate, the speed depends on the negotiated result.

For a description of the **OK, Apply, Close** and **Reset** buttons, see “Switch Settings tab” on page 128.

User Admin tab

You can use the **User Admin** tab to change the switch User and Admin account names and passwords. The **User Admin** tab is shown in Figure 70.

Note: A user can only log into the **User Admin** tab if they have administrative privileges.

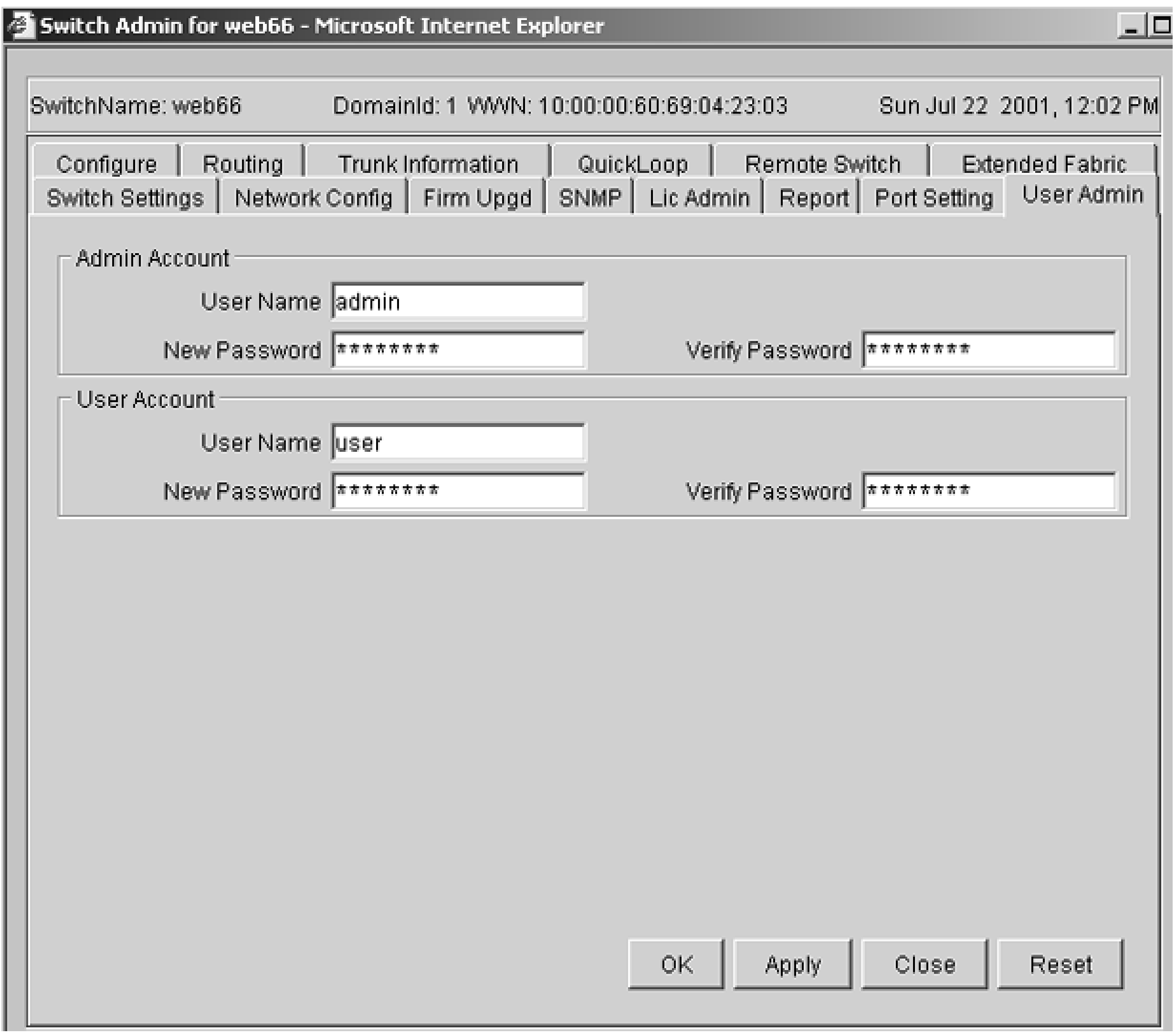


Figure 70. User Admin tab

Following is a description of the fields in the **User Admin** tab.

User Name
Type a new user name or modify the existing user name.

New Password
Type a new password or modify the existing password.

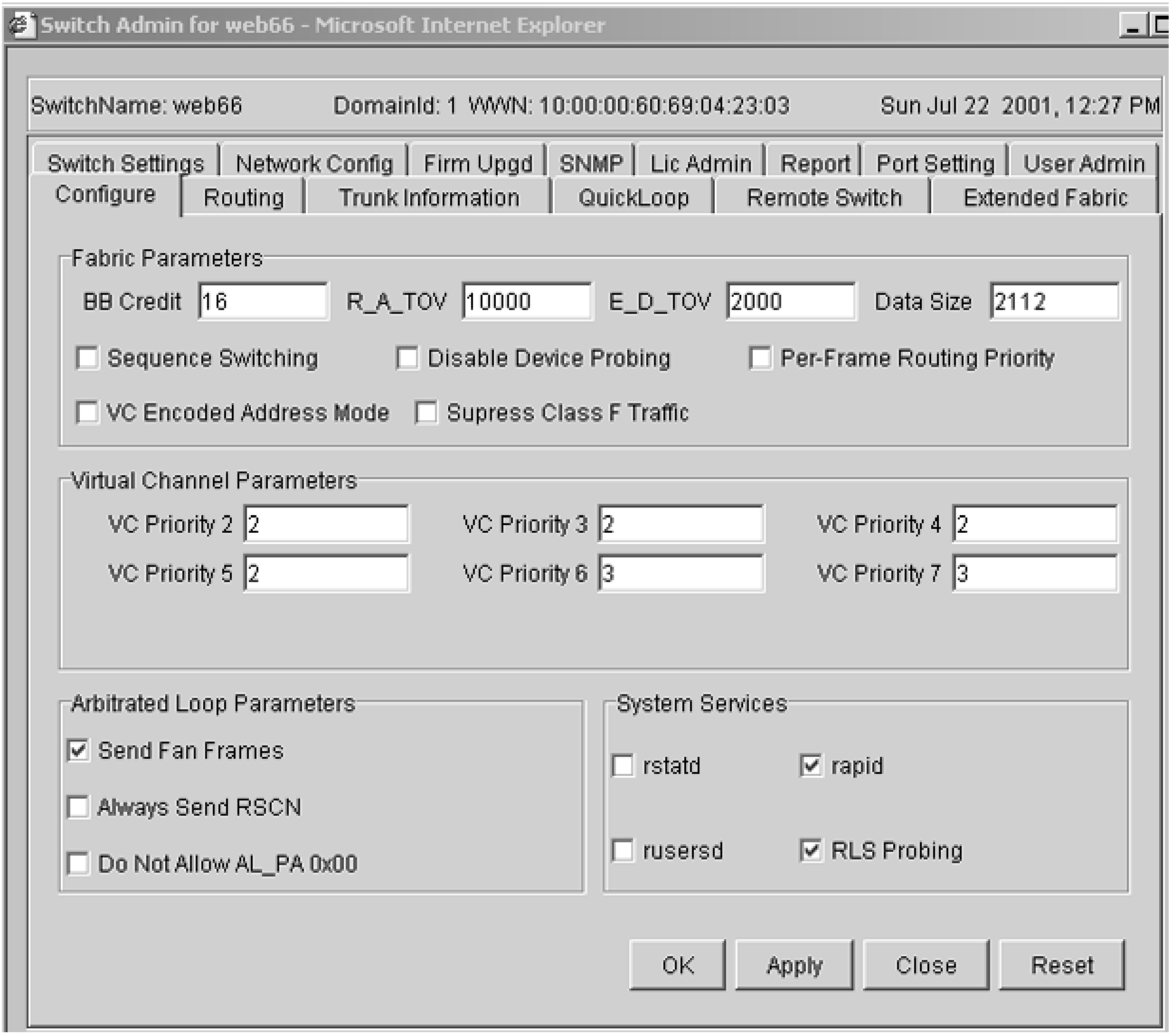
Verify Password
Reenter the password to verify.

For a description of the **OK, Apply, Close** and **Reset** buttons, see "Switch Settings tab" on page 128.

Note: A user does not gain access to the user interface with the user ID and password created in this tab.

Configure tab

The **Configure** tab provides the same function as the Telnet **configure** command. The following actions are controlled from the **Configure** tab: Fabric Parameters, Virtual Channel Parameters, Arbitrated Loop Parameters, and Systems Services. See *IBM TotalStorage SAN Fibre Channel Switch 3534 Model F08 Command Reference* for valid values for each editable field of the **configure** command. The **Configure** tab is shown in Figure 71 on page 141.



SJ000258

Figure 71. Configure tab

Following is a description of the fields in the **Configure** tab.

Fabric Parameters section

BB Credit
: Displays the number of buffers that are available to attached devices for frame receipt.

R_A_TOV
: Displays the resource allocation timeout value in milliseconds. This variable works with the E_D_TOV to determine switch actions when presented with an error condition.

E_D_TOV
: Displays the error detect timeout value in milliseconds. This timer is used to flag a potential error condition when an expected response is not received within the set time.

Data Size
: Specifies the largest possible data field size in bytes.

Sequence Switching

Sequence Level Switching is set to 1
Frames of the same sequence from a particular source are transmitted together as a group.

Sequence Level Switching is set to 0
Frames are transmitted interleaved among multiple sequences.

Under normal conditions, Sequence Level Switching should be disabled for better performance. However, some host adapters have performance issues when receiving interleaved frames from multiple sequences. When there are such devices attached to the fabric, Sequence Level Switching should be enabled.

Disable Device Probing
When selected, devices that do not register with the name server are not present in the name server database. Set this mode only if the switch N_port discovery process (PLOGI, PRLI, INQUIRY) causes an attached device to fail.

Per-Frame Routing Priority
When selected, the virtual channel ID is used in conjunction with a frame header to form the final virtual channel ID.

VC Encoded Address Mode
When selected, the frame source and destination address use an address format that is compatible with the 3534 switch. Set this mode only if the fabric includes this type of switch.

Suppress Class F Traffic
Only applies if VC Encoded Address Mode is also set. When selected, translative addressing is disabled.

Virtual Channel Parameters section

VC Priority
Enables fine tuning for a specific application by configuring the parameters for eight virtual channels.

Arbitrated Loop Parameters section

Send Fan Frames
Select to specify that fabric access notification (FAN) frames be sent to public loop devices to notify them of their node ID and address.

Always Send RSCN
Select to issue a registered state change (RSCN) notification, following the completion of loop initialization, when FL_ports detect the presence of new devices or the absence of preexisting devices.

Do Not Allow AL_PA 0x00
Select to specify that AL_PA is not allowed.

System Services section

rstatd Dynamically enables or disables a server that returns information about system operation information through remote procedure calls.

rapid Select to enable rapid system service.

rusersd
Dynamically enables or disables a server that returns information about the user who is logged into the system through remote procedure calls.

RLS Probing
Select to enable RLS Probing services.

For a description of the **OK, Apply, Close** and **Reset** buttons, see “Switch Settings tab” on page 128.

Routing tab

You can use the **Routing** tab to set the link cost for the selected ports and static route. The **Routing** tab is shown in Figure 72.

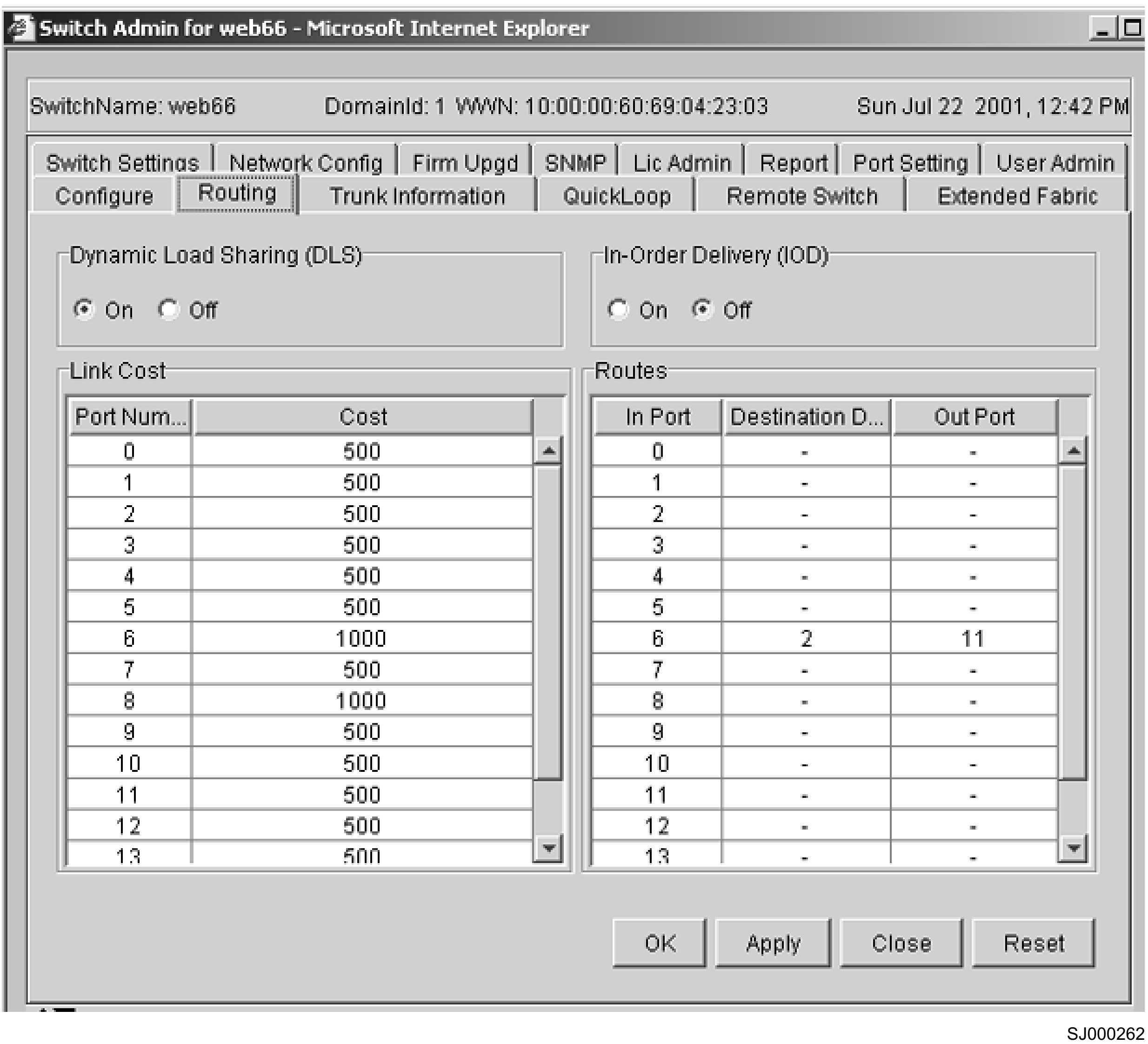


Figure 72. Routing tab

Following is a description of the fields in the **Routing** tab.

Dynamic Load Sharing (DLS)
Select to turn Dynamic Load Sharing on or off.

In-Order Delivery (IOD)
Select to turn In-Order Delivery on or off.

Link Cost section

Port Number
Displays the port number.

Cost Used to change the link cost for a particular tab.

Routes section

In Port
Displays the in port.

Destination
Displays the destination domain ID for the comma-separated participating static routes for a particular in port. The destination domain IDs match the out ports in the cell.

Out Port
The out port should be within the range of ports that are available for static route in the destination domain. More than one out port can be used for any in port with a different domain ID.

For a description of the **OK, Apply, Close** and **Reset** buttons, see "Switch Settings tab" on page 128.

Trunk Information tab

The **Trunk Information** tab is a read-only tab, and is shown in Figure 73 on page 145

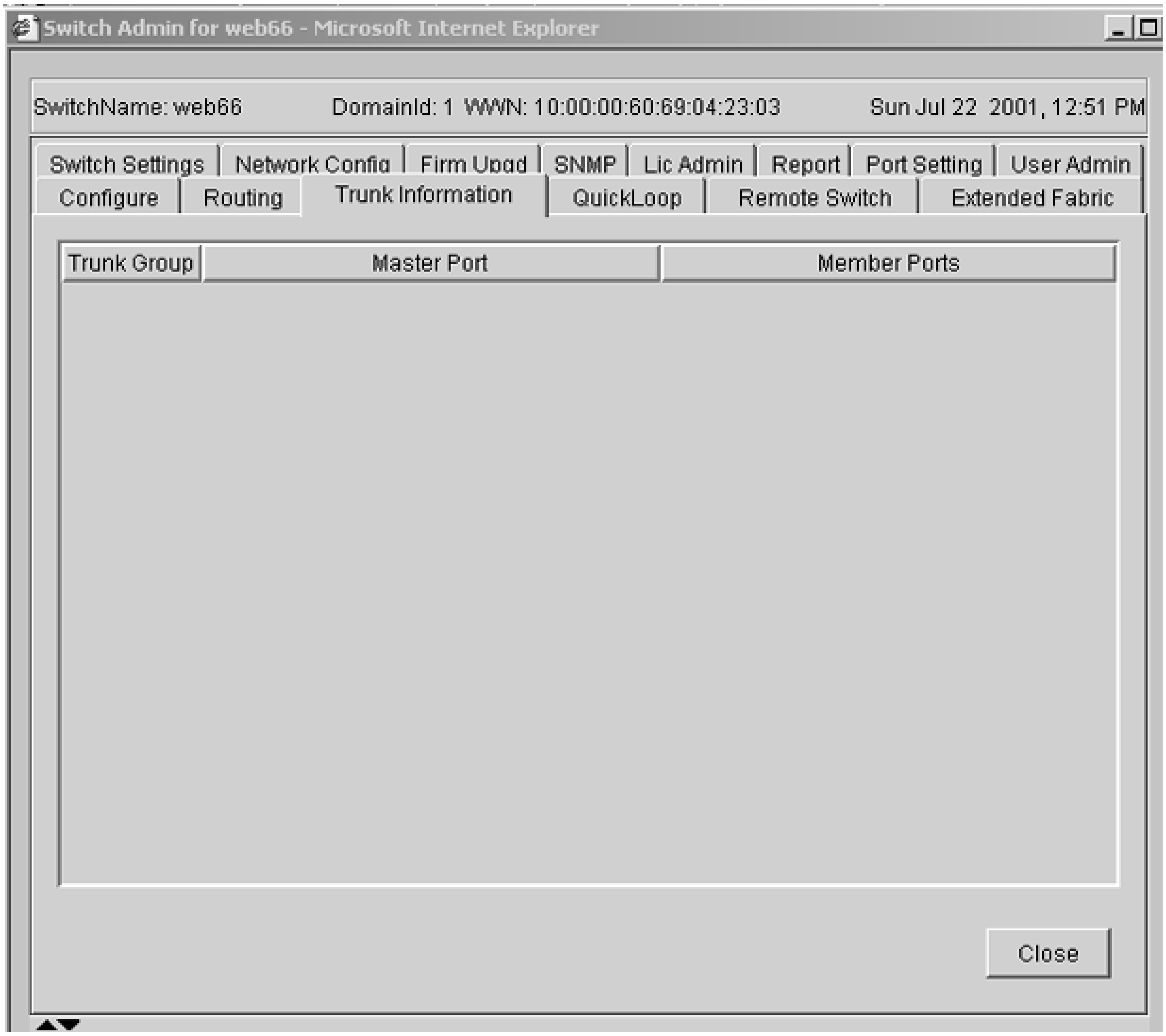


Figure 73. Trunk Information tab

The following fields are in the **Trunk Information** tab:

- Trunk Group
- Master Port
- Member Ports

QuickLoop tab

You can use the **QuickLoop** tab to manage a QuickLoop configuration. For information about managing the features available when QuickLoop and zoning are used together, see "Zone Administration view (optional software required)" on page 57. For detailed information about the QuickLoop feature, see Chapter 7, "QuickLoop" on page 197.

The **QuickLoop** tab is displayed only when the QuickLoop license is installed. The **QuickLoop** tab is shown in Figure 74.

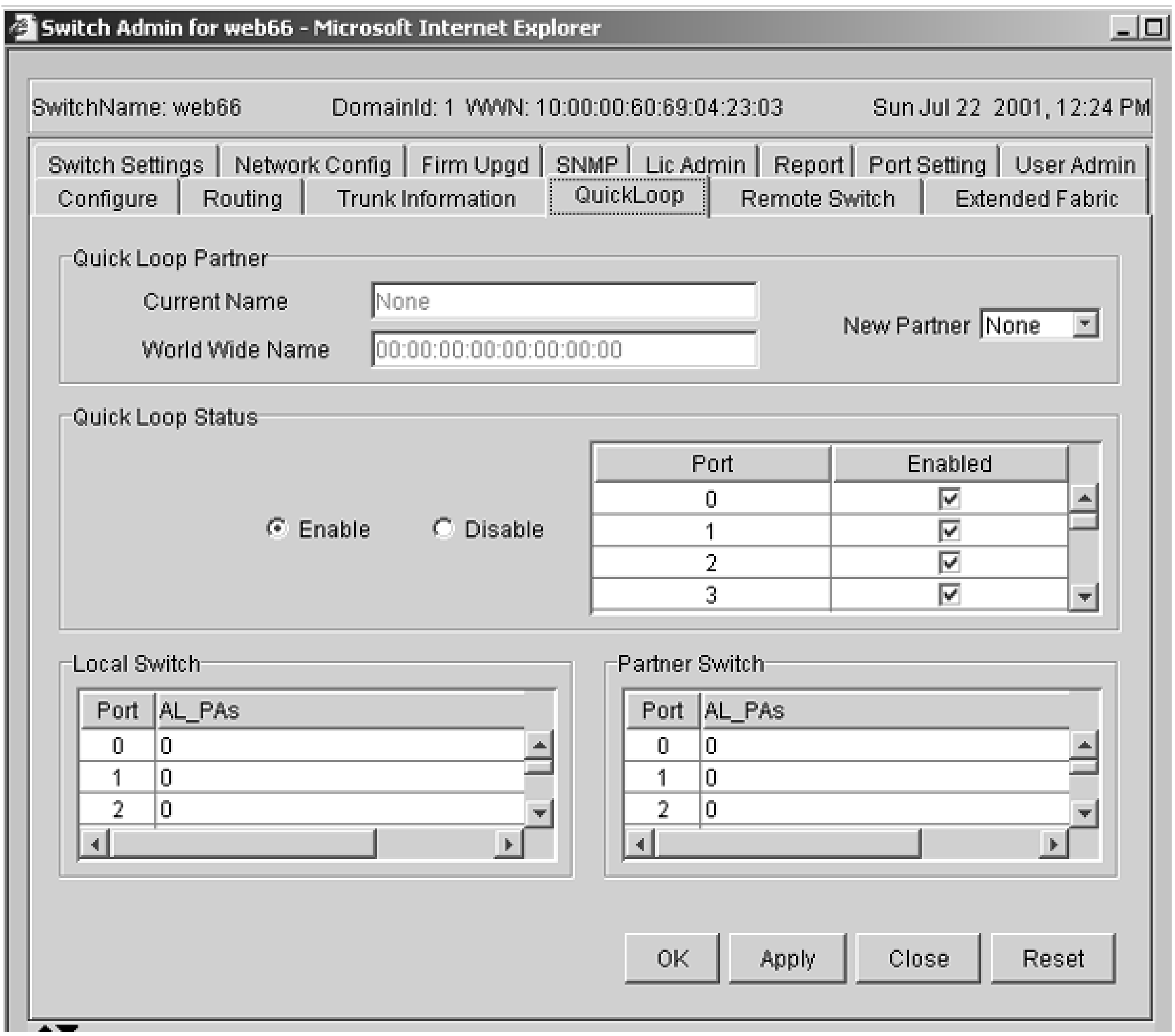


Figure 74. QuickLoop tab

Following is a description of the fields in the **QuickLoop** tab.

QuickLoop Partner section

Current Name
Displays the current name of the remote switch.

World Wide Name
Displays the WWN of the remote switch.

New Partner
Displays the current partner switch name of a dual-switch QuickLoop.

QuickLoop Status section

Enable
Select to enable the switch for QuickLoop, or clear to disable the switch for QuickLoop.

Disable
Select to disable the switch for QuickLoop.

Port Displays the port numbers.

Enabled
Select to enable a port for QuickLoop, or clear to disable the port for QuickLoop.

Local Switch Port
Lists the ports that are connected to the local switch.

Local Switch AL_PAs
Lists the AL_PAs of devices that are connected to the local switch.

Partner Switch Port
Lists the ports that are connected to a remote switch.

Partner Switch AL_PAs
Lists the AL_PAs of devices that are connected to a remote switch. This information displays if a partner is configured.

For a description of the **OK, Apply, Close** and **Reset** buttons, see “Switch Settings tab” on page 128.

Remote Switch tab

The Remote Switch feature configures a pair of switches to operate over an extended wide area network (WAN) interface, so that they can communicate across an asynchronous transfer mode (ATM) network by using a compatible fibre-channel to ATM gateway. This feature requires an active Remote Switch license in both switches.

Use the **Remote Switch** tab to manage the Remote Switch feature. This tab is displayed only when the Remote Switch is installed. The **Remote Switch** tab is shown in Figure 75.

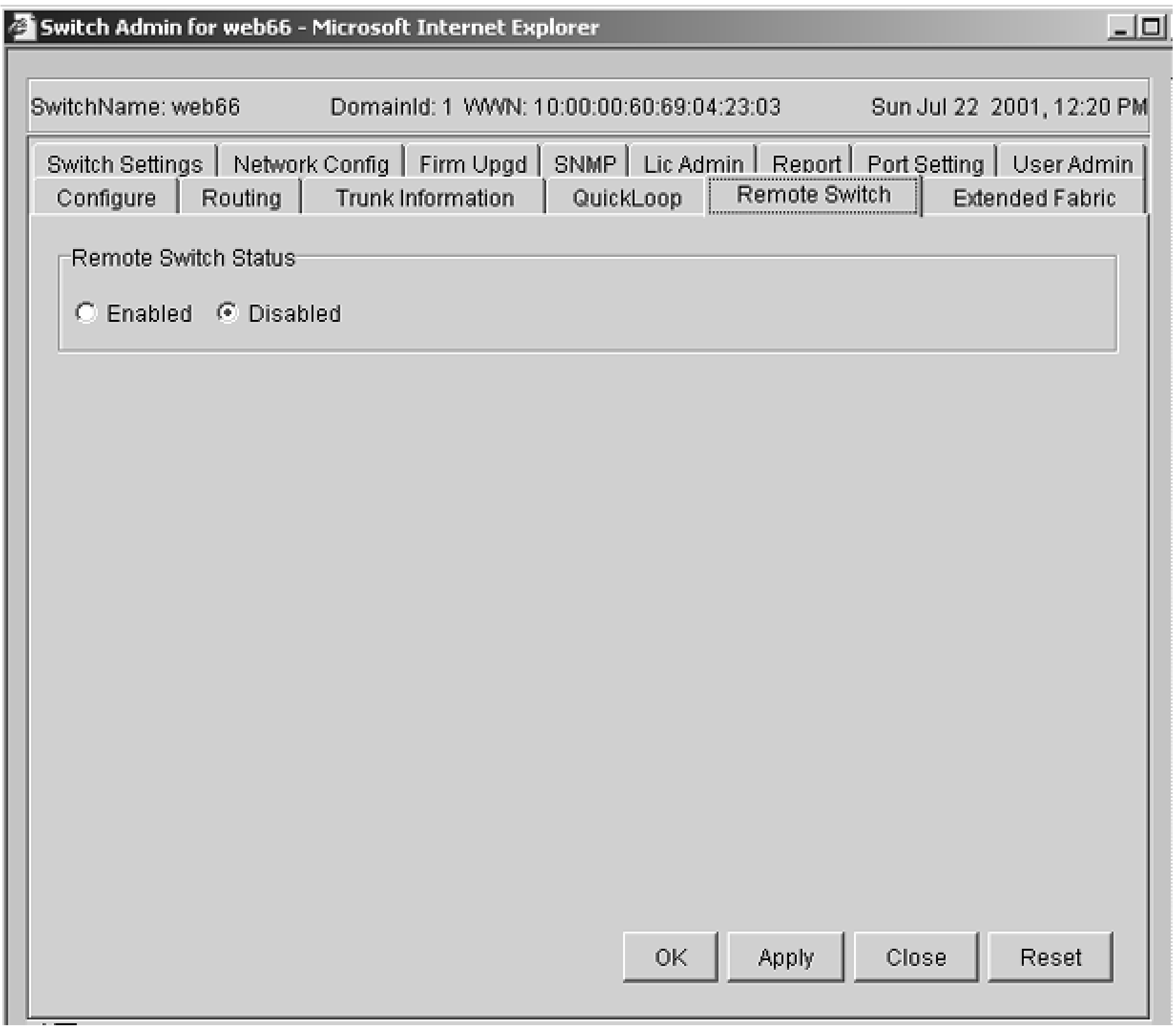


Figure 75. Remote Switch tab

Following is a description of the fields in the **Remote Switch** tab.

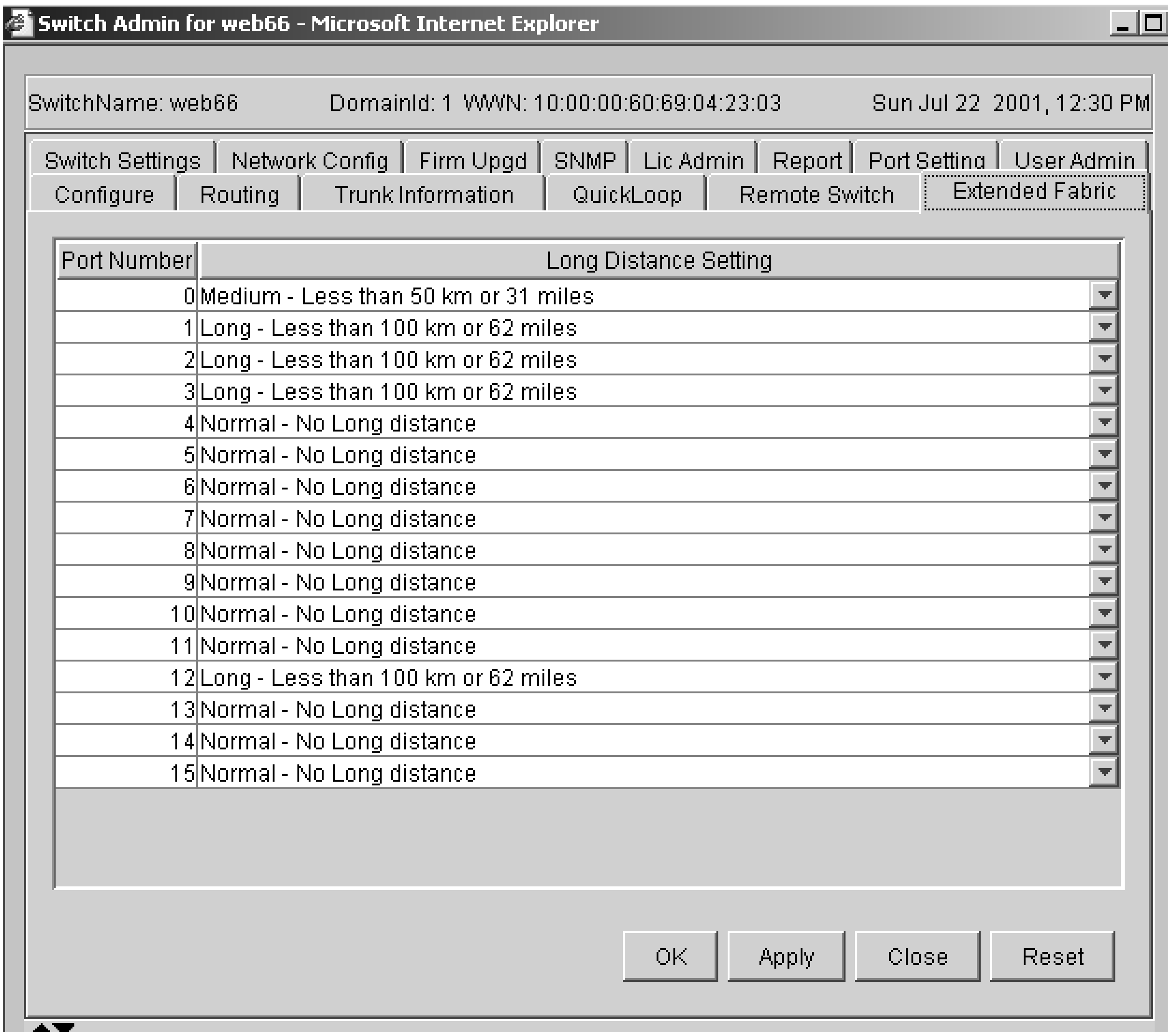
Enabled
Select to enable the Remote Switch feature, or clear to disable it.

Disabled
Select to disable the Remote Switch feature, or clear to disable it.

For a description of the **OK, Apply, Close** and **Reset** buttons, see “Switch Settings tab” on page 128.

Extended Fabric tab

You can use the **Extended Fabric** tab to manage the Extended Fabric feature. From the **Extended Fabric** tab you can specify which ports are to be configured for distance and at what level. The **Extended Fabric** tab displays only when the Extended Fabric license is installed on the switch. For ports that are disabled, the rows are grayed-out in the table within the tab. The **Extended Fabric** tab is shown in Figure 76.



SJ000259

Figure 76. Extended Fabric tab

Following is a description of the fields in the **Extended Fabric** tab.

Port Number
: The port number that is being used for the Extended Fabric.

Long Distance Setting
: Select to view long distance settings.

For a description of the **OK, Apply, Close** and **Reset** buttons, see "Switch Settings tab" on page 128.

Telnet interface

The Telnet interface requires administrative privileges. After you enter an administrative login, administrative privileges remain available until you close the Web browser. Only one Telnet session can be active at a time.

Perform the following steps to access the Telnet Interface:

1. Launch the Web browser.
2. Type the switch name or IP address in the **Location/Address** field and press Enter.

   TotalStorage Specialist launches, displaying the Fabric view.
3. Click the **Telnet** icon on the switch panel.

   If a Telnet session is already active, the following message displays as shown in Figure 77.

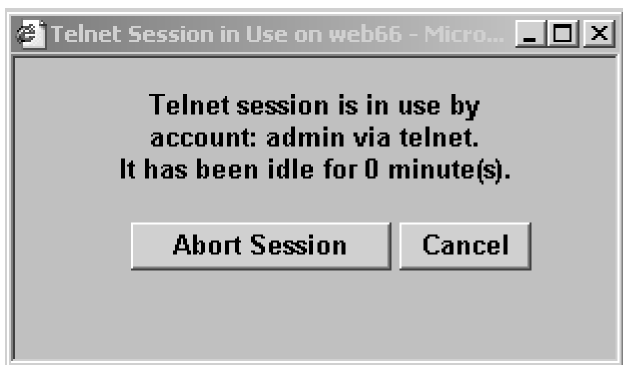


Figure 77. Telnet Session in Use message

4. If this message displays and you want to end the active session, click **Abort Session**. Otherwise, click **Cancel**. If there is no active session or it has been ended, the following dialog displays as shown in Figure 78 on page 151.

Figure 78. Enter Network Password dialog box

5. Type your user name and password (the account must have administrative privileges).
6. Select **Save the password in your password list** if you want the password saved.
7. Click **OK**.

   The Telnet interface displays, as shown in Figure 79.

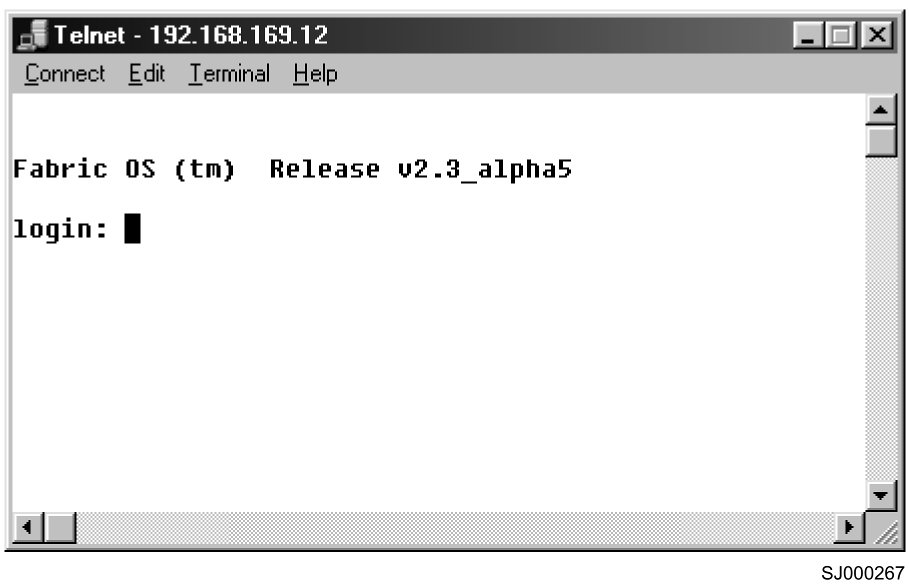


Figure 79. Telnet interface

Chapter 4. Advanced Performance Monitoring

This chapter provides the following information about Performance Monitoring:

Overview of Performance Monitoring

Performance Monitoring is an optionally licensed product that runs on 3534 Model F08 series switches. It provides SAN performance management through an end-to-end monitoring system that enables you to:

- Increase end-to-end visibility into the fabric
- Enable more accurate reporting for service level agreements and charged access applications
- Improve performance tuning and resource optimization
- Shorten troubleshooting time
- Promote better capacity planning
- Simplify administration and setup
- Increase productivity with preformatted and customizable screens and reports

Features

The Performance Monitoring product:

- Monitors transaction performance from its source to its destination
- Provides device performance measurements by port, AL_PA, and LUN
- Reports CRC error measurement statistics
- Measures trunking performance
- Compares IP versus SCSI traffic on each port
- Includes a wide range of predefined reports
- Allows you to create customized user-defined reports

Administration

You can administer Performance Monitoring through either Telnet commands or TotalStorage Specialist. If you use TotalStorage Specialist, a TotalStorage Specialist license must also be installed on the switch.

Performance Monitoring with Telnet commands

Three different types of Performance Monitoring can be done using Telnet commands:

- AL_PA monitoring
- End-to-end monitoring
- Filter-based monitoring

See “Using Performance Monitoring” on page 161 for detailed information about how to use the Telnet commands to monitor performance.

AL_PA monitoring

AL_PA monitoring provides information about the number of CRC errors occurring in fibre-channel frames in a loop configuration. AL_PA monitoring collects CRC error counts for each AL_PA that is attached to a specific port.

End-to-end monitoring

End-to-end monitoring provides information about transaction performance between the transactions source (SID) and destination (DID) on a fabric or a loop. Up to 16 SID-DID pairs per port can be specified. For each of the SID-DID pairs, the following information is available:

- CRC error count on the frames for the SID-DID pair
- Fibre-channel words that have been transmitted from the port for the SID-DID pair
- Fibre-channel words that have been received by the port for the SID-DID pair

Filter-based monitoring

Filter-based monitoring provides information about the hit count of a filter. Any parameter in the first 64 bytes of the fibre-channel frame can be measured. The counter increases each time a frame is filtered through the corresponding port. Examples of port filter statistics that can be measured are:

- SCSI read, write, or read/write commands
- CRC error statistics (port and AL_PA)
- IP versus SCSI traffic comparison

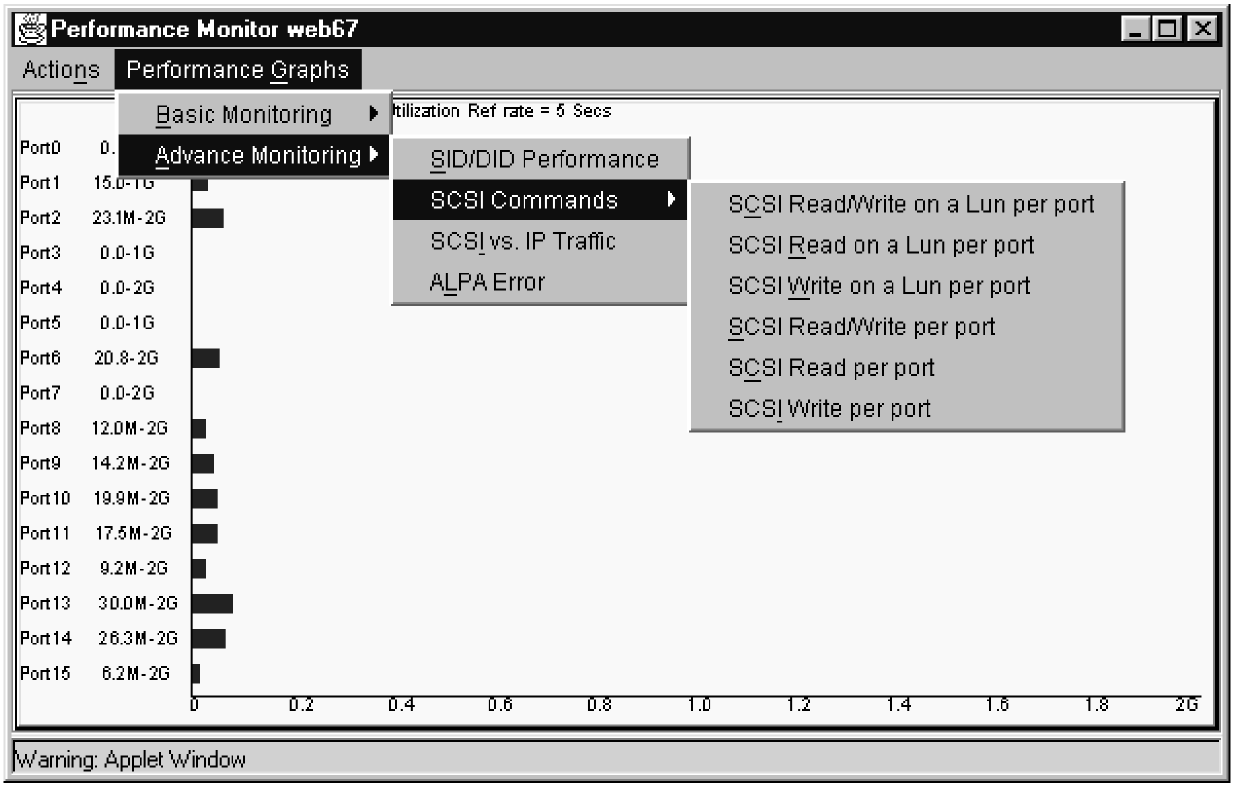
Performance Monitoring with TotalStorage Specialist

You can monitor performance using TotalStorage Specialist if a TotalStorage Specialist license is also installed. The enhanced Performance Monitoring features in TotalStorage Specialist provide:

- Predefined performance graphs for AL_PA, end-to-end, and filter-based monitoring
- User-defined graphs
- Performance canvas for application-level or fabric-level views
- Configuration editor (save, copy, edit, and remove multiple configurations)
- Persistent graphs across restarts (saves parameter data across restarts)
- Print capabilities

Predefined performance graphs

Predefined graphs are provided to simplify performance monitoring. Figure 80 on page 155 shows the list of predefined performance graphs. A wide range of end-to-end fabric, LUN, device, and port metrics are included.

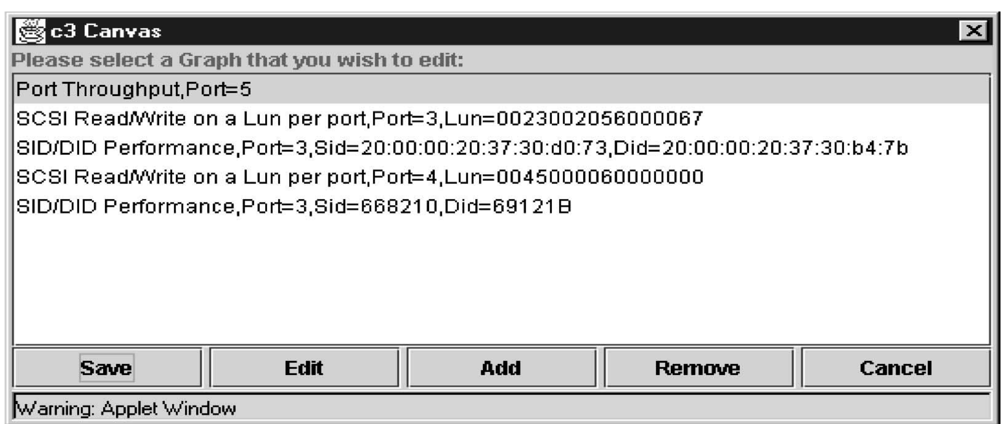


SJ000301

Figure 80. Predefined performance graphs

User-defined graphs

The predefined graphs can be modified based on parameter fields such as SID/DID, LUN, AL_PA, and port. These new user-defined graphs can be added and saved to canvas configurations. Figure 81 shows a list of user-defined graphs defined in a canvas.

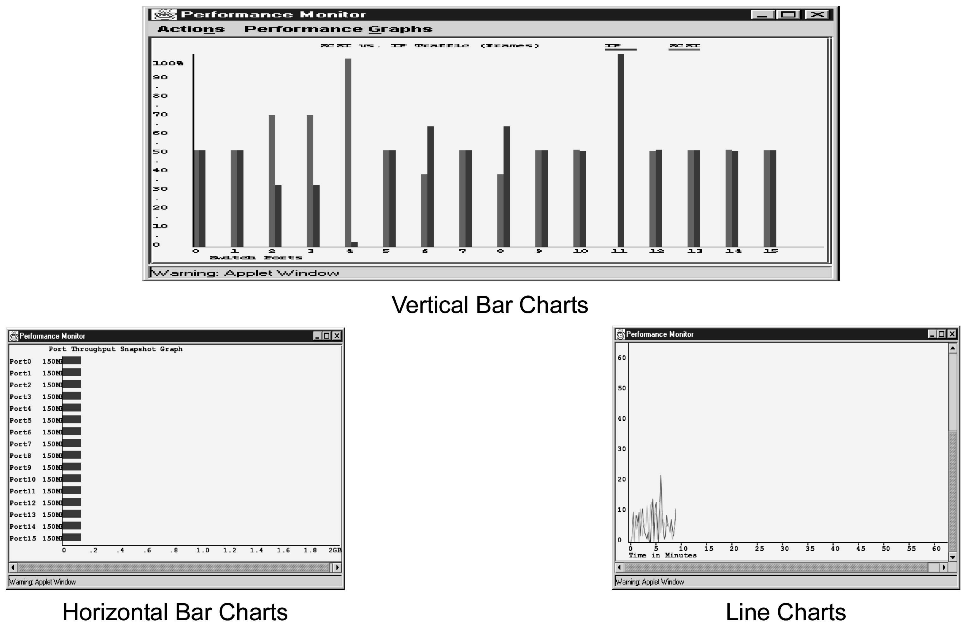


SJ000302

Figure 81. User-defined graphs

Performance graph formats

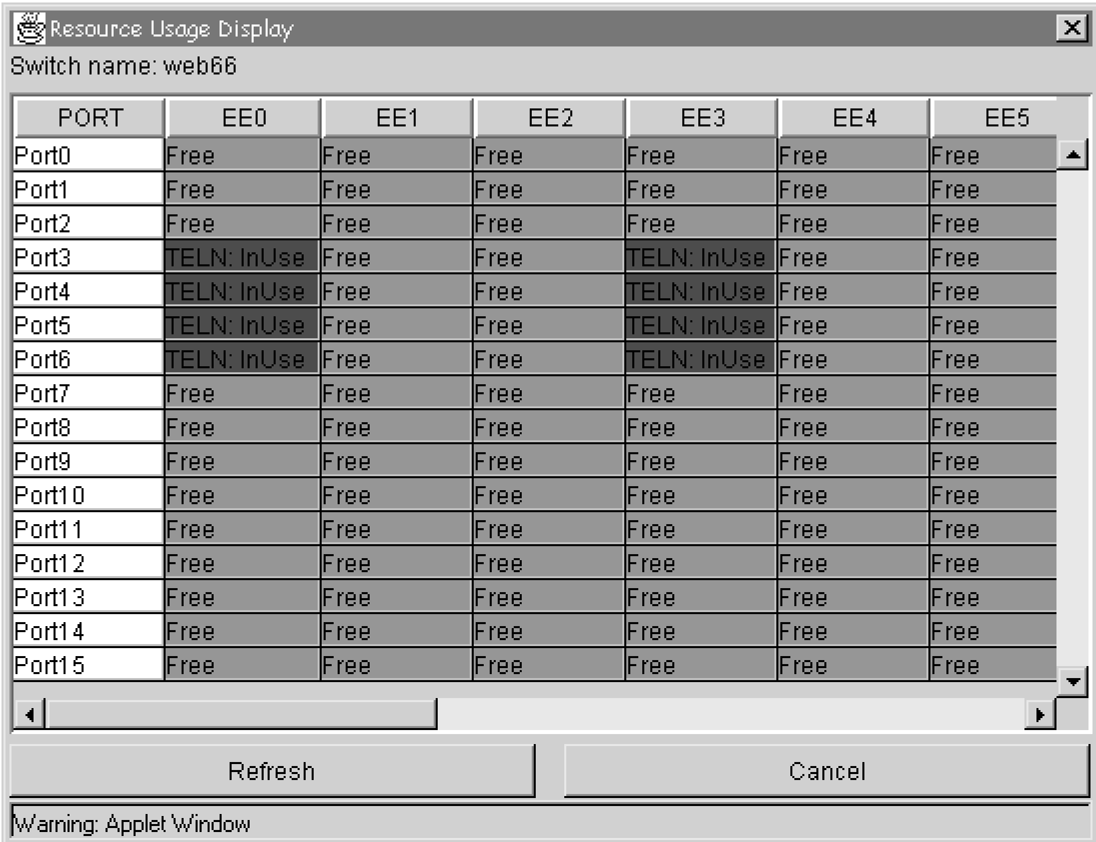
Performance graphs can be displayed as vertical bar charts, horizontal bar charts, and line charts, as shown in Figure 82.



SJ000305

Figure 82. Types of performance graphs

In addition, the resource usage display as shown in Figure 83 on page 157 provides selected switch status in a single graph. The color-coded interface makes troubleshooting easier.



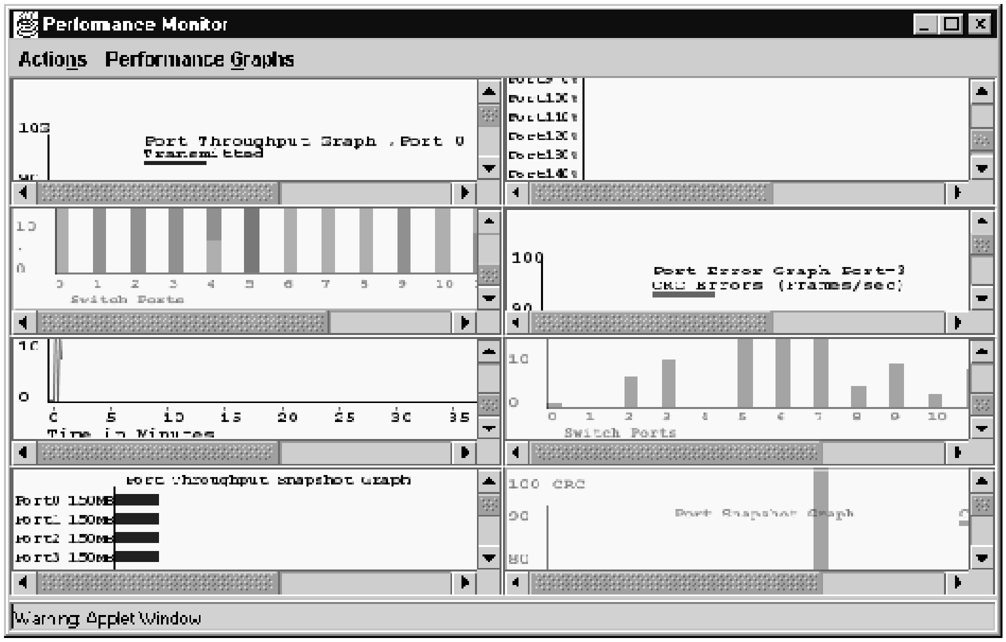
PORT	EE0	EE1	EE2	EE3	EE4	EE5
Port0	Free	Free	Free	Free	Free	Free
Port1	Free	Free	Free	Free	Free	Free
Port2	Free	Free	Free	Free	Free	Free
Port3	TELN: InUse	Free	Free	TELN: InUse	Free	Free
Port4	TELN: InUse	Free	Free	TELN: InUse	Free	Free
Port5	TELN: InUse	Free	Free	TELN: InUse	Free	Free
Port6	TELN: InUse	Free	Free	TELN: InUse	Free	Free
Port7	Free	Free	Free	Free	Free	Free
Port8	Free	Free	Free	Free	Free	Free
Port9	Free	Free	Free	Free	Free	Free
Port10	Free	Free	Free	Free	Free	Free
Port11	Free	Free	Free	Free	Free	Free
Port12	Free	Free	Free	Free	Free	Free
Port13	Free	Free	Free	Free	Free	Free
Port14	Free	Free	Free	Free	Free	Free
Port15	Free	Free	Free	Free	Free	Free

SJ000306

Figure 83. Resource usage display

Performance graph canvas

The enhanced Performance Monitoring in TotalStorage Specialist enables you to set up a canvas of performance graphs. The canvas can hold up to eight graphs per window, as shown in Figure 84.



SJ000303

Figure 84. Canvas of eight performance monitoring graphs

Multiple canvasses can be created for different users or different scenarios. You can then save the multiple canvasses, edit them, and recall them. Figure 85 on page 159 shows a list of the different canvas configurations that you can choose to display.

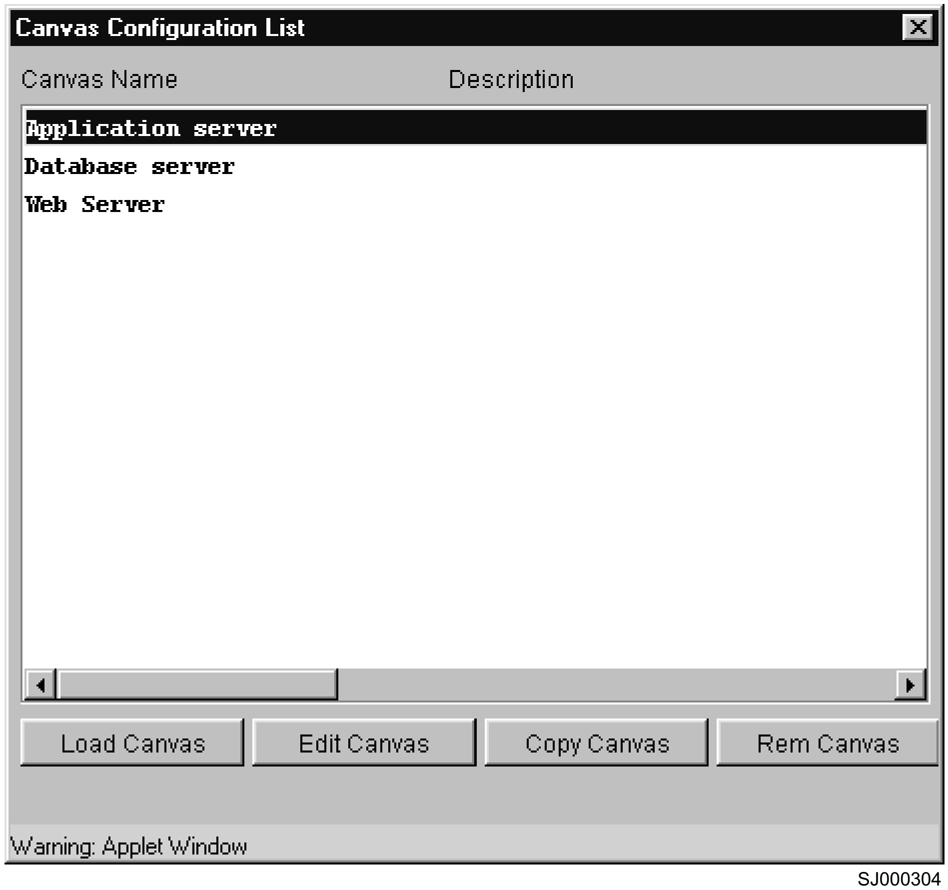


Figure 85. Canvas management

Installing Performance Monitoring

To enable Performance Monitoring, you must install a license on each switch that will use this feature. Contact your switch supplier to obtain a license key.

Note: A license might have already been installed on the switch at the factory.

You can install a Performance Monitoring license using Telnet commands or using TotalStorage Specialist.

Note: Version 3.0 of Performance Monitoring requires a 3534 Model F08 series switch with Fabric OS version 3.0 or later installed.

Installing Performance Monitoring using Telnet

Perform the following steps to install Performance Monitoring using Telnet:

1. Log into the switch through Telnet (see "Logging into a switch" on page 19 for details), using an account that has administrative privileges.
2. To determine whether a Performance Monitoring license is already installed on the switch, type `licenseShow` on the Telnet command line.

   A list of all the licenses that are currently installed on the switch displays. For example:

```
admin> licenseShow
 1A1AaAaaaAAA1a:
 Release v3.0
 Zoning license
 SES license
 QuickLoop license
```

If the Performance Monitoring license is not included in the list, continue with step 3.

3. Type the following on the command line:

   `licenseAdd "key"`

   where `key` is the license key exactly as provided by your switch supplier, surrounded by double quotation marks. The license key is case-sensitive and must be entered exactly as given.

4. Verify that the license key was successfully added by typing `licenseShow` on the command line.

   A list of all the licenses displays. For example:

```
admin> licenseShow
 1A1AaAaaaAAA1a:
 Release v3.0
 Zoning license
 SES license
 QuickLoop license
 Performance Monitor license
```

The Performance Monitoring Telnet commands are available as soon as the license key is added.

Installing Performance Monitoring using TotalStorage Specialist

You can install a license key using TotalStorage Specialist if a TotalStorage Specialist license is already installed.

1. Launch a Web browser, type the switch name or IP address in the **Location/Address** field of the browser, and press Enter.

   TotalStorage Specialist launches, displaying the Fabric view.

2. Click the **Admin** button on the relevant switch panel.

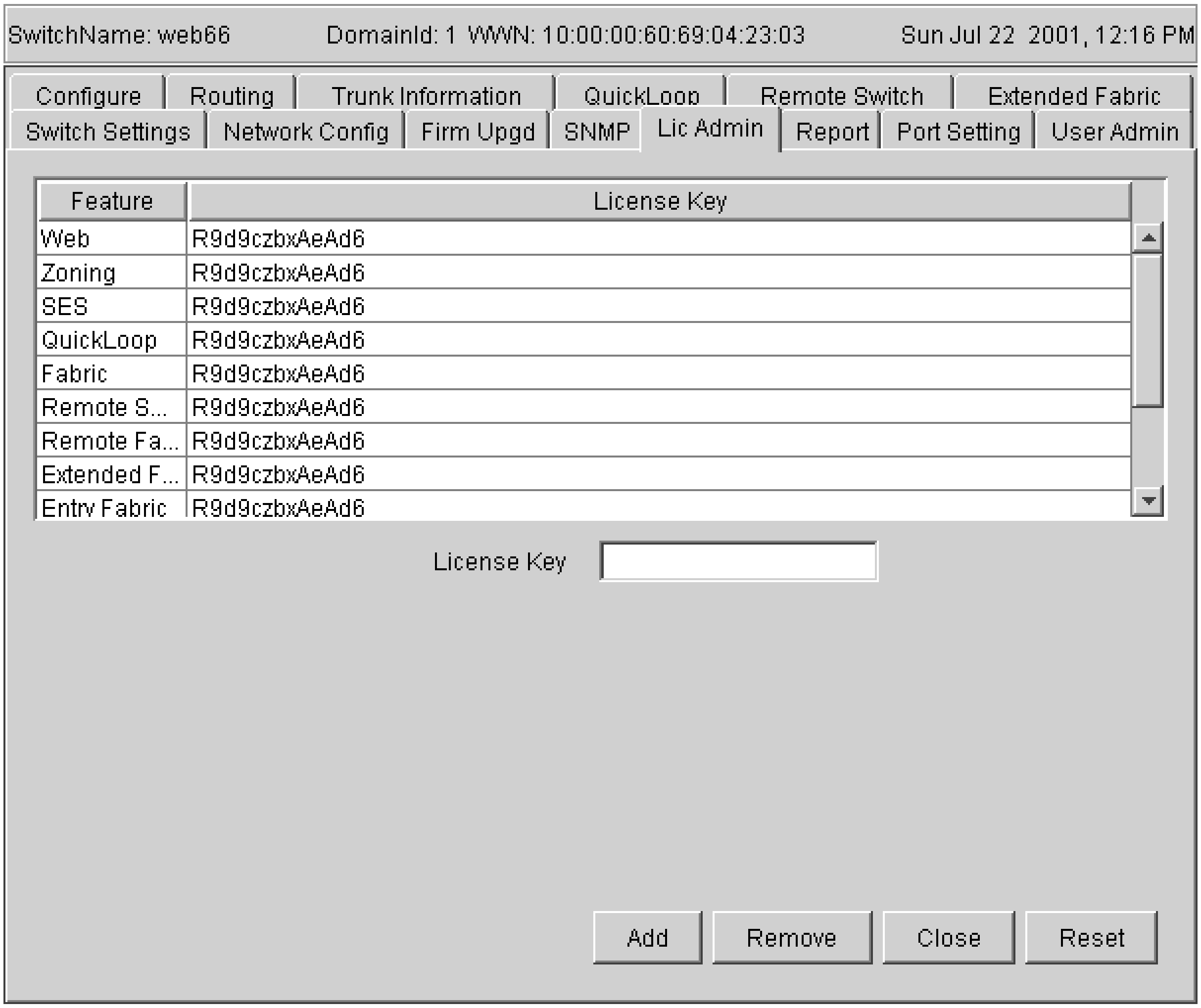
   The logon window displays.

3. Type a logon name and password with administrative privileges and press Enter. The administrator account name is `admin` and the default password is `password`.

   The Administration view displays.

4. Select the **License Admin** tab.
5. Type the license key in the **License Key** field exactly as provided by your switch supplier and click **Add**, as shown in Figure 86 on page 161.

The Performance Monitoring Telnet commands are available as soon as the license key is added.



SJ000308

Figure 86. License Admin tab

For more information about TotalStorage Specialist, see Chapter 3, “TotalStorage Specialist” on page 37.

Using Performance Monitoring

You can administer Performance Monitoring through Telnet commands or through TotalStorage Specialist. This section describes Performance Monitoring using Telnet commands. For a description of Performance Monitoring using TotalStorage Specialist, see “Performance Monitoring with TotalStorage Specialist” on page 154.

Telnet commands

The Telnet commands for Performance Monitoring become available through the shell “admin” account when the Performance Monitoring license key is installed. To use a Telnet command, log into the relevant switch with administrative privileges. Type the command, along with any required arguments, and press Enter.

Using Telnet commands, you can track the following:

- The number of CRC errors for AL_PA devices
- The number of words in fibre-channel frames going from an SID to a DID
- The number of times a particular command or frame type is received by a port

For a description of all the Telnet commands that are used for Performance Monitoring, see *IBM TotalStorage SAN Fibre Channel Switch 3534 Model F08 Command Reference*.

AL_PA Performance Monitoring

AL_PA Performance Monitoring allows you to track and display the number of CRC errors that have occurred on frames that are sent to each AL_PA on a specific port. No monitor configuration is necessary for AL_PA Performance Monitoring.

Displaying the CRC error count

You use the **perfShowAlpaCrc** command to display the CRC error count for all AL_PA devices or for a single AL_PA on a specific port. The port must be an active L_port. In the following example, the CRC error count for all AL_PA devices on port 3 displays:

```
sw1:admin> perfShowAlpaCrc 3
AL_PA            CRC COUNT
---------------------------
0x01                2
0x03                0
0x04                1
```

In the following example, the CRC error count for AL_PA 1 on port 3 displays:

```
sw1:admin> perfShowAlpaCrc 3, 1
The CRC count at ALPA 0x1 on port 3 is 0x000000002.
```

Clearing the CRC error count

You use the **perfClrAlpaCrc** command to clear the CRC error count for AL_PA devices on a specific port. You can clear the error counts for all the AL_PA devices or for a specific AL_PA.

In the following example, the CRC error count for all AL_PA devices on port 3 is cleared:

```
sw1:admin> perfClrAlpaCrc 3
No ALPA value is specified. This will clear all ALPA CRC counts on port 3.
Do you want to continue?
[y|n]y
Please wait ...
All alpa CRC counts are cleared on port 3.
```

In the following example, the CRC error count for AL_PA 1 on port 3 is cleared:

```
admin> perfClrAlpaCrc 3, 1

CRC error count at ALPA 0x1 on port 3 is cleared.
```

End-to-end Performance Monitoring

End-to-end Performance Monitoring counts the number of words in all fibre-channel frames that originate from a specified source ID (SID) and go to a specified destination ID (DID).

To enable end-to-end Performance Monitoring, you must configure an end-to-end monitor on a port, specifying the SID-DID pair. Each SID or DID has three fields, listed in the following order:

- Domain ID
- Area ID
- AL_PA

For example, the SID 0x118a0f has domain ID 0x11, area ID 0x8a, and AL_PA 0x0f. The prefix “0x” denotes a hexadecimal number.

You can set up a mask to selectively choose the kind of fibre-channel frames in which the number of words are to be counted. With no mask set, the frame must match the entire SID or DID to trigger the monitor counter. By setting a mask, you can choose to have the frame match only one or two of the three fields to trigger the monitor.

Note: You can set only one mask per port. The mask is applied to all of the end-to-end monitors on a port. If you subsequently create new monitors on the port, the mask is applied to these new monitors as well.

Adding end-to-end monitors

You use the **perfAddEEMonitor** command to add an end-to-end monitor to a port. With this command you specify the port, the SID, and the DID that you want to monitor. The port must be the port of either the SID or the DID, and not one of the ports in between. If the SID and DID are on different switches, the port must be the SID, the DID, or one of the E_ports.

In the following example, several end-to-end monitors are added on port 2 to count the number of words in fibre-channel frames that are going to DID 0x1182ef, and that originate from one of the following SIDs: 0x058e0f, 0x058ee0, 0x058ee1, 0x058ee2, and 0x058edc.

```
sw1:admin> perfAddEEMonitor 2, "0x058e0f", "0x1182ef"
End-to-End monitor number 0 added.

sw1:admin> perfAddEEMonitor 2, "0x058ee0", "0x1182ef"
End-to-End monitor number 1 added.

sw1:admin> perfAddEEMonitor 2, "0x058ee1", "0x1182ef"
End-to-End monitor number 2 added.

sw1:admin> perfAddEEMonitor 2, "0x058ee2", "0x1182ef"
End-to-End monitor number 3 added.

sw1:admin> perfAddEEMonitor 2, "0x058edc", "0x1182ef"
End-to-End monitor number 4 added.
```

By default, the monitor counts the number of words in all frames that are transmitted and received from port 2 that match one of the specified SID-DID pairs. To selectively choose the kind of fibre-channel frames in which the number of words are to be counted, set up an end-to-end mask on the port, as described in “Setting a mask for end-to-end monitors”.

Setting a mask for end-to-end monitors

You use the **perfSetPortEEMask** command to set a mask for end-to-end monitors. The command sets the mask for all end-to-end monitors of a port, so that you can selectively choose the kind of fibre-channel frames in which the number of words are to be counted.

The **perfSetPortEEMask** command sets a mask for the domain ID, area ID, and AL_PA of the SIDs and DIDs for frames that are transmitted from and received by the port. Figure 87 shows the mask positions in the command.

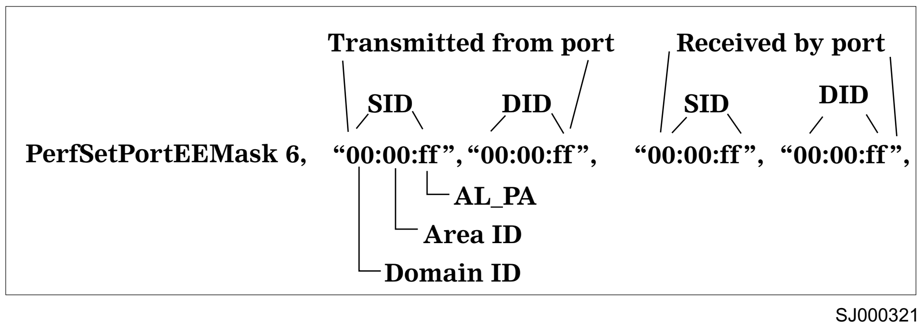


Figure 87. Mask positions for end-to-end monitors

In Figure 87, a mask (“ff”) is set on port 6 to compare the AL_PA fields on the SID and DID in all frames (transmitted and received) on port 6. The domain ID and area ID fields in all frames are ignored as no mask is set on these fields.

Each port can have only one EE mask. The mask is applied to all the end-to-end monitors on the port. You cannot specify individual masks for each monitor on the port. If you define a new end-to-end monitor on a port after you have created a mask for that port, the mask is automatically applied to the new monitor.

When the system is started, the default EE mask value is `"ff:ff:ff"` for the SID and DID on all transmitted and received frames.

In the following example, an end-to-end monitor is added to port 6, and then a mask is set on the SID and DID domain ID of frames transmitted from port 6.

```
sw1:admin> perfAddEEMonitor 6, "0x058e0f", "0x1182ef"
End-to-End monitor number 0 added.

sw1:admin> perfSetPortEEMask 6, "ff:00:00", "ff:00:00", "00:00:00", "00:00:00"
The EE mask on port 6 is set and EE counters are reset.
```

All frames that are transmitted from port 6 are compared to the SID-DID pairs defined by the **perfAddEEMonitor** command to determine whether there is a monitor that matches the SID domain ID and DID domain ID field of a frame.

If the domain ID field of the frame matches either 0x05 or 0x11, then monitor 0 is triggered, and the number of fibre-channel words in this transmitting frame is added to the monitor.

Displaying the end-to-end mask of a port

You use the **perfShowPortEEMask** command to display the current end-to-end mask of a port.

The end-to-end mask has 12 bits (from 11 down to 0). Bit 11 is the leftmost bit, and bit 0 is the rightmost bit. Frames that are transmitted by the port use the mask in bits 11 - 6; frames that are received by the port use the mask in bits 5 - 0.

In the following example, the end-to-end mask of port 11 is set and displayed:

```
sw1:admin> perfSetPortEEMask 11, "00:00:ff", "00:00:ff", "00:00:ff", "00:00:ff"
The EE mask on port 11 is set.

sw1:admin> perfShowPortEEMask 11
The EE mask on port 11 is set by application TELNET

TxSID Domain:     off
TxSID Area:       off
TxSID ALPA:       on
TxDID Domain:     off
TxDID Area:       off
TxDID ALPA:       on
RxSID Domain:     off
RxSID Area:       off
RxSID ALPA:       on
RxDID Domain:     off
RxDID Area:       off
RxDID ALPA:       on
```

Displaying end-to-end monitors

You use the **perfShowEEMonitor** command to display the end-to-end monitors that are defined on a port. This command displays the following information on all end-to-end monitors:

- The monitor number (KEY)
- The SID
- The DID
- The CRC error count (CRC_COUNT)
- The number of fibre-channel words transmitted (TX_COUNT)
- The number of fibre-channel words received (RX_COUNT)
- The creator application (OWNER)
- The IP address of the creator, if known (OWNER_IP)

If you specify a monitor number in the **perfShowEEMonitor** command, the command displays the information about that specific monitor. If you omit the monitor number, the command displays the information about all of the end-to-end monitors that are defined on that port.

In the following example, information about all end-to-end monitors that are defined on port 3 is displayed. The `KEY` column contains the monitor number.

```
sw1:admin> perfShowEEMonitor 3
There are 2 end-to-end monitor(s) defined on port 3.

KEY  SID      DID       OWNER_APP OWNER_IP_ADDR TX_COUNT           RX_COUNT           CRC_COUNT
-------------------------------------------------------------------------------------------------
0    0x58E0F  0x1182ef  TELNET    N/A           0x0000000000000000  0x000000000025ad4f 0x0000000000000000
```

In the following example, continuous information for end-to-end monitor 0 on port 3 is displayed:

```
sw1:admin> perfShowEEMonitor 3, 0
perfShowEEMonitor 3, 1: Tx/Rx are # of bytes and crc is # of crc errors
             0
----------------------------------
crc         Tx           Rx
----------------------------------
0            0           1.2k
0            0           272
0            0           136
0            0           272
0            0           272
0            0           204
0            0           204
0            0           136
0            0           272
0            0           272
```

Deleting end-to-end monitors

You use the **perfDelEEMonitor** command to delete an end-to-end monitor on a port. You indicate which monitor to delete by specifying the monitor number that was returned by a previous **perfAddEEMonitor** command.

In the following example, the end-to-end monitor 0 on port number 2 is deleted:

```
sw1:admin> perfDelEEMonitor 2, 0
End-to-End monitor number 0 deleted
```

Filter-based Performance Monitoring

Filter-based Performance Monitoring counts the number of times that a particular command or frame type is received by a port. Filter-based monitoring is achieved by configuring a filter for a particular purpose. The filter can be a standard filter (for example, a read command filter that counts the number of read commands that have been received by the port) or a user-defined filter that you customize for your particular use.

The maximum number of filters is eight per port, in any combination of standard filters and user-defined filters.

Adding standard filter-based monitors

Use the Telnet commands listed in Table 9 on page 167 to define filter-based monitors on a port.

Table 9. Telnet commands to add filter-based monitors

Telnet command	Description
perfAddReadMonitor	Count the number of SCSI read commands
perfAddWriteMonitor	Count the number of SCSI write commands
perfAddRWMonitor	Count the number of SCSI read/write commands
perfAddSCSIMonitor	Count the number of SCSI frames
perfAddIPMonitor	Count the number of IP frames

In the following example, several filter-based monitors are added to port 2 and the results are displayed:

```
sw1:admin> perfAddReadMonitor 2, "SCSI READ"
SCSI Read filter monitor #0 added

sw1:admin> perfAddWriteMonitor 2, "SCSI WR"
SCSI Write monitor #1 added

sw1:admin> perfAddRWMonitor 2, "SCSI R/W"
SCSI Read/Write monitor #2 is added

sw1:admin> perfAddSCSIMonitor 2, "SCSI CT"
SCSI traffic frame monitor #3 added

sw1:admin> perfAddIPMonitor 2, "IP Count"
IP traffic frame monitor #4 added

sw1:admin> perfShowFilterMonitor 2
There are 5 filter-based monitors defined on port 2.

KEY   COUNT                ALIAS       OWNER_APP   OWNER_IP_ADDR
0     0x0000000000000000   SCSI READ   TELNET          0
1     0x0000000000000000   SCSI WR     TELNET          0
2     0x0000000000000000   SCSI R/W    TELNET          0
3     0x0000000000000000   SCSI CT     TELNET          0
4     0x0000000000000000   IP COUNT    TELNET          0
```

Adding user-defined filter-based monitors

In addition to the standard filters (read, write, read/write, and frame count), you can create custom filters to qualify frames for statistics gathering to fit your own special needs.

To define a custom filter, use the **perfAddUserMonitor** command. With this command, you must specify a series of offsets, masks, and values. The following actions are performed for all incoming frames:

1. The switch locates the byte that is found in the frame at the specified offset.
2. The switch applies the mask to the byte that is found in the frame.
3. The switch compares the value with the given values in the **perfAddUserMonitor** command.
4. The switch increments the filter counter if a match is found.

You can specify up to six different offsets for each port, and up to four values to compare against each offset.

If more than one offset is required to properly define a filter, the bytes that are found at each offset must match one of the given values for the filter to increment its counter. If one or more of the given offsets does not match any of the given values, the counter does not increment.

The value of the offset must be between 0 - 63. Byte 0 indicates the first byte of the start-of-frame (SOF), byte 4 is the first byte of the frame header, and byte 28 is the first byte of the payload. Thus only the SOF, frame header, and the first 36 bytes of payload can be selected as part of a filter definition.

The hardware can manage only a limited number of unique offsets and values. If the switch does not have enough resources to create a given filter, then other filters might have to be deleted to free up resources.

In the following example, a filter-based monitor is added to count all FCP and IP frames that are received from domain 0x02 for port 2.

```
sw1:admin> perfAddUserMonitor 2, "12, 0xff, 0x05, 0x08; 9, 0xff, 0x02", "FCP/IP"
User monitor #5 added
```

The FCP and IP protocols are selected by monitoring offset 12, mask 0xff and matching values of 0x05 or 0x08. Domain 2 is selected by monitoring offset 9, mask 0xff, and matching a value of 0x02.

Displaying filter-based monitors

You use the **perfShowFilterMonitor** command to display the filter-based monitors of a port.

This command displays all the filter-based monitors that are defined on the specified port. It displays all the valid monitor numbers and user-defined aliases on the specified port.

In the following example, all filter-based monitors that are defined on port 2 are displayed. The KEY column lists the monitor numbers.

```
sw1:admin> perfShowFilterMonitor 2
There are 6 filter-based monitors defined on port 2.

KEY   ALIAS       OWNER_APP   OWNER_IP_ADDR   FRAME_COUNT
0     SCSI READ   TELNET      N/A             0x0000000000000132
1     SCSI WR     TELNET      N/A             0x0000000000000054
2     SCSI R/W    TELNET      N/A             0x0000000000000006
3     IP COUNT    TELNET      N/A             0x0000000000000012
4     SCSI CT     TELNET      N/A             0x0000000000000492
5     FCP/IPT     TELNET      N/A             0x0000000000000009
```

Removing filter-based monitors

To remove a filter-based monitor, you first list the valid monitor numbers using the **perfShowFilterMonitor** command. You then use the **perfRemoveFilterMonitor** command to delete a specific monitor.

In the following example, the monitors on port 2 are displayed in the KEY column, and then the deleted monitor number 1 on port 2 is displayed:

```
sw1:admin> perfShowFilterMonitor 2
There are 6 filter-based monitors defined on port 2.

KEY   COUNT               ALIAS       OWNER_APP   OWNER_IP_ADDR
-----------------------------------------------------------------
0     0x0000000000000132   SCSI READ   TELNET          0
1     0x0000000000000054   SCSI WR     TELNET          0
2     0x0000000000000006   SCSI R/W    TELNET          0
3     0x0000000000000012   IP Count    TELNET          0
4     0x0000000000000492   SCSI CT     TELNET          0
5     0x0000000000000009   FCP/IP      TELNET          0

sw1:admin> perfDelFilterMonitor 2, 1
The specified filter-based monitor is deleted
```

Saving and restoring monitor configuration

You use the **perfCfgSave** command to save the current end-to-end and filter-based monitor configuration into flash memory. This enables the Performance Monitoring configuration to be saved over power cycles. You can use the **perfCfgRestore** command to restore the saved monitor configuration from flash memory, for example, after you restart the switch. For example:

```
sw1:admin> perfCfgSave
This will overwrite previously saved Performance Monitoring
settings in FLASH ROM. Do you want to continue? [y|n]y
Please wait ...
Committing configuration...done.
Performance monitoring configuration saved in FLASH ROM.
sw1:admin> perfCfgRestore
This will overwrite current Performance Monitoring
settings in RAM. Do you want to continue? [y|n]y
Please wait ...
Performance monitoring configuration restored from FLASH ROM.
```

You use the **perfCfgClear** command to clear the previously-saved Performance Monitoring configuration settings from flash memory.

For example:

```
sw1:admin> perfCfgClear
This will clear Performance Monitoring settings in FLASH ROM.
The RAM settings wont change. Do you want to continue? [y|n]y
Please wait ...
Committing configuration...done.
Performance Monitoring configuration cleared from FLASH.
```

Chapter 5. Distributed fabrics

This chapter discusses the following two features that are available on the 3534 Model F08:

- “Remote Switch”
- “Extended Fabrics” on page 175

Remote Switch

This section describes the Remote Switch feature.

Remote Switch overview

Remote Switch is an optionally licensed product that runs on the 3534 F08 and 2109 F series with Fabric OS version 3.0 or later. Remote Switch runs on the 3534 1RU and 2109 S series with Fabric OS version 2.2 or later.

The Remote Switch feature, in conjunction with a compatible fibre channel to asynchronous transfer mode (ATM) gateway, enables two 3534 or 2109 series fabric switches to be connected over an ATM connection, with a distance of up to 10 km (32 808.4 ft) between each switch and the respective ATM gateway. The two switches are cascaded together to form a fabric that, from the viewpoint of the connected hosts and storage devices, interact the same as locally-connected switches. The performance limitations depend only on the type of ATM connection that is used. Remote Switch supports a maximum of two switches in a fabric.

The Remote Switch feature provides:

Any-to-any connectivity
A host that is connected on the local or remote switch can communicate with storage devices at either location.

Coordinated fabric services
The Remote Switch fabric configuration fully supports all fabric services, the same as a centralized fabric configuration. These services include Distributed Name Services, Registered State Change Notifications, and Alias Services.

Distributed management
Access to the management facilities (TotalStorage Specialist, Telnet, SNMP, and SES) is available from either the local or the remote switch. Interconnect for switch management is routed through the fibre-channel connection; no additional network connection is required between sites.

Ability to support multiple interswitch links (ISLs)
Sites that require redundant configurations can connect multiple E_ports to remote sites by using multiple gateways. Standard Fabric OS routing facilities automatically maximize throughput by using the E_ports to load share traffic during normal operation, with automatic failover and failback during interruption on the wide area network (WAN) connection.

Installing Remote Switch

A Remote Switch fabric requires two switches that are 3534 or 2109 series switches with Fabric OS version 3.0 installed, with the switches configured the same.

When you install a Remote Switch, you must also install a separate license on each of the two switches. Licenses might have been installed on the switches at the factory. If not, contact your switch supplier to obtain a license key.

You can install a Remote Switch license two ways:

- Using Telnet
- Using TotalStorage Specialist

Installing the Remote Switch feature using Telnet

Perform the following steps to install Remote Switch using Telnet:

1. Login to the switch through Telnet using an account that has administrative privileges. See “Logging into a switch” on page 19.
2. To determine whether a Remote Switch license is already installed on the switch, type `licenseShow` on the Telnet command line.

   A list of all the licenses that are currently installed on the switch displays. For example:

```
admin> licenseShow

 cQebzbRdScRfcOiK:
     Web license
     Zoning license
AybbzQQ9edTzccOX:
Fabric license
```

   If the Remote Switch license is listed, the feature is installed and is immediately available. If the Remote Switch license is not included in the list or is incorrect, continue with steps 3 and 4.
3. Type the following on the command line:

   `licenseAdd "key"`

   where `"key"` is the license key that was provided to you, surrounded by double quotation marks. 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 Remote Switch license is listed, the feature is installed and is immediately available. If the license is not listed, repeat step 3.

Installing the Remote Switch feature using TotalStorage Specialist

Perform the following steps to install Remote Switch using TotalStorage Specialist:

1. Launch the Web browser.
2. Type the switch name or IP address in the **Location/Address** field and press Enter.

   TotalStorage Specialist launches, displaying the Fabric view.
3. Click **Admin** on the relevant switch panel.

   The logon window displays.
4. Type a logon name and password with administrative privileges and press Enter.

   The Administration view displays.
5. Select the **License Admin** tab.
6. Type the license key in the **License Key:** field and click **Add License**.

The Remote Switch feature is available as soon as the license key is added.

Using Remote Switch

You can configure switches for use with Remote Switch through Telnet or through TotalStorage Specialist. For information about using TotalStorage Specialist and how to configure a switch, see “Administrative Interface” on page 126.

The Remote Switch feature operates in conjunction with a fibre-channel-to-ATM gateway. The gateway provides both a fibre-channel physical interface functioning as an E_port and an ATM physical interface.

The gateway accepts fibre-channel frames from one side of a Remote Switch fabric, transfers them across a WAN using ATM protocol, and passes them to the other side of the Remote Switch fabric.

To transfer frames across a WAN using ATM protocol, the fibre-channel frames (from 256 to 2112 bytes) must be broken into smaller pieces (53 byte ATM cells) at the local end of the ATM network. After the frames are broken into smaller pieces, they are tunnelled inside ATM cells to be transmitted across the ATM network. At the remote end of the ATM network these pieces are reassembled back into complete fibre-channel frames and are transmitted through the remote fibre-channel interface.

To accomplish this, the gateway provides an E_port interface that links to the 3534 Model F08 E_port. After the link between the two E_ports is negotiated, the gateway E_port moves to pass-through mode and passes fibre-channel traffic from the 3534 Model F08 E_port to the ATM network.

Configuring a Remote Switch fabric

A Remote Switch fabric requires two 3534 or 2109 series switches with identical configurations. A separate Extended Fabric license is not required to operate the switch at distances greater than 100 km (328 084 ft). This can be achieved when the switch operates over ATM. Performance is limited to the ATM link, which is capable of 1.55 Mbps to 155 Mbps.

In addition to normal switch configuration options, the following parameters must be configured:

Timeout values
: The resource allocation timeout value (R_A_TOV) and error detect timeout value (E_D_TOV) must be increased, as appropriate, for all switches participating in the Remote Switch fabric. This provides for the possible increase in transit time caused by the introduction of WAN links into the fabric.

Data field size
: All switches participating in the Remote Switch fabric must have the data field size configured to the maximum of 2048 bytes to accommodate the maximum field size that is supported by the ATM gateway. Data field sizes smaller than 2048 bytes can be set, but they might cause significant performance degradation.

Class F frame suppression
: All switches participating in the Remote Switch fabric must have the Class F frame suppression flag set. Class F frames are automatically converted to Class 2 frames.

BB credit
: The setting for BB credit must be the same on both switches. Switches with a different value will segment.

You use the Telnet **configure** command to set the parameter values.

Perform the following steps to set a parameter value.

Note: The switch must be disabled before running the **configure** command.

1. Type `configure` on the command line.
2. Type `Y` at the Fabric parameters prompt.
3. A prompt for each parameter is displayed. You can then set any parameter to any allowed value.

   Note: The allowable BB credit parameter values are 1 - 16. This value is the BB credit that is offered to all F_ports that are using the Remote Switch feature. E_ports that are not Remote Switch E_ports are not affected.

In the following example, the default values were accepted for BB credit and R_A_TOV. The parameter values were changed for E_D_TOV, Data field size, and Suppress Class F traffic.

```
switch:admin> configure

Configure. . .

    Fabric parameters (yes, y, no, n): [no] yes

         Domain:  (1. .239)   [2]
         BB credit:  (1. .16)   [16]
         R_A_TOV:  (4000. .120000)   [10000]
         E_D_TOV:  (1000. .5000)   [2000]5000
         Data field size:  (256. .2112)   [2112]   2048
         Non-SCSI Tachyon Mode:  (0. .1)   [0]
         Disable Device Probing:  (0. .1)   [0]
         Suppress Class F Traffic:  (0. .1)   [0]   1
```

Extended Fabrics

This section describes the Extended Fabrics feature.

Extended Fabrics overview

Extended Fabrics is an optionally licensed product that runs on 3534 or 2109 series switches with Fabric OS version 3.0.

The Extended Fabrics feature uses fibre-channel technology to create a fabric that is interconnected at a distance of up to 100 km (328 084 ft). Extended Fabrics can increase the allowable distance between two switches or between a switch and an ATM gateway used in a Remote Switch configuration.

Extended Fabrics optimizes the internal buffering algorithm for 3534 or 2109 series switches. It provides maximum buffering between E_ports that are connected over an extended distance through buffer reconfiguration. This results in line speed performance of close to full fibre-channel speed for switches that are interconnected at 100 km (328 084 ft), thus providing the highest possible performance for transfers between switches. The fibre-channel connection extensions can be provided by extended distance GBICs, fibre-channel repeaters, or wave division multiplexing (WDM) devices.

Note: Performance can vary depending on the condition of the fiber optic connections between the switches. Losses due to splicing, connectors, tight bends, and other degradation can affect the performance over the link and the maximum distance possible.

To enable Extended Fabrics, an Extended Fabrics license must be installed. If a fabric is created with a 3534 Model F08 switch, the long distance extended fabric configuration has to be set only once for each fabric at the edge port connector switch. The edge port connector switch automatically works with the rest of the switches in the fabric.

Note: To enable Extended Fabrics in a fabric created with 3534 switches, each switch in the fabric must be configured individually.

Installing Extended Fabrics

When you install Extended Fabrics, you must also install a license on each switch in the fabric. If a license was not installed in the switch at the factory, contact your switch supplier to obtain a license key.

You can install Extended Fabrics licenses two ways:

- Using Telnet
- Using TotalStorage Specialist

Installing the Extended Fabrics feature using Telnet

Perform the following steps to install Extended Fabrics using Telnet:

1. Login to the switch through Telnet using an account that has administrative privileges. See “Logging into a switch” on page 19.
2. To determine whether an Extended Fabrics license is already installed on the switch, type `licenseShow` on the Telnet command line.

   A list of all the licenses that are currently installed on the switch displays. For example:

```
admin> licenseShow

 1A1AaAaaaAAAA1a:
 Release v2.2
 Web license
 Zoning license
 SES license
 QuickLoop license
```

If an Extended Fabrics license is correctly listed, the feature is installed and immediately available. If an Extended Fabrics license is not included in the list, or is incorrect, continue with steps 3 and 4.

3. Type the following on the command line:

   `licenseAdd "key"`

   where `"key"` is the license key that was provided to you, surrounded by double quotation marks. 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 Extended Fabrics license is listed, the feature is installed and immediately available. If the license is not listed, repeat step 3.

Installing the Extended Fabrics feature using TotalStorage Specialist

Perform the following steps to install Extended Fabrics using TotalStorage Specialist:

1. Launch the Web browser.
2. Type the switch name or IP address in the **Location/Address** field and press Enter. TotalStorage Specialist launches, displaying the Fabric view.
3. Click **Admin** on the relevant switch panel. The logon window displays.
4. Type a logon name and password with administrative privileges and press Enter. The Administration view displays.
5. Select the **License Admin** tab.
6. Type the license key in the **License Key** field and click **Add License**.

   The Extended Fabrics feature is available as soon as the license key is added.

Using Extended Fabrics

You can configure ports to support long distance links through Telnet or through TotalStorage Specialist. For information about using TotalStorage Specialist and how to configure ports, see Chapter 3, “TotalStorage Specialist” on page 37.

Support configurations

An Extended Fabric can be created with 3534 Model F08 and 2109 F series switches that are running Fabric OS version 3.0 or later. The 3534 1RU and 2109 S series switches require Fabric OS version 2.2 or later. An Extended Fabric can consists of:

- 3534 series switches only
- 2109 series switches only
- A combination of 3534 and 2109 series switches

Note: In a combination (3534 and 2109 series) configuration, the long-distance ISL that connects the fabrics must be installed between edge-port switches of the same series. An Extended Fabric does not work if the long distance ISL is installed between nonmatching edge port switches.

Configuring Extended Fabrics

In order to run Extended Fabrics, the following two parameters need to be set:

- Switch configuration to enable long distance
- Port configured to select the long distance mode

In the 3534 switches, each switch within the fabric must have the switch configuration turned on. In the 2109 series switches, only the edge-port switches need to have the switch configuration turned on.

Perform the following steps to set the long distance fabric mode bit:

1. Login to the switch through Telnet.
2. At the command line, type the following command:
   `switchDisable`
3. At the command line, type the following command:
   `configure`
4. Type `Y` at the Fabric parameters prompt.
5. Type `1` at the following prompt:
   `Long Distance Fabric [0]:`

There are three possible long distance levels for a port:

Level 0
Reconfigures the port as a regular switch port. The number of buffers reserved for the port supports up to 10 km (6.2 mi) links.

Level 1
Distances up to 50 km (31 mi) will support 1 Gbps and 2 Gbps switches (3534 and 2109 series).

Level 2
Distances up to 100 km (62 mi) will support 1 Gbps and 2 Gbps switches (3534 and 2109 series).

Ports are grouped into quads, each of which consists of four adjacent ports that share a common pool of frame buffers. The possible quad groupings are:

- Ports 0 - 3
- Ports 4 - 7
- Ports 8 - 11
- Ports 12 - 15

Certain buffers are dedicated for each port, and others are shared among the ports. In Extended Fabric mode, one port is given an increase of dedicated buffers from this pool.

L0 Represents an Extended Fabric mode of 10 km (6.2 mi).

L1 Represents an Extended Fabric mode of 50 km (31 mi).

L2 Represents an Extended Fabric mode of 100 km (62 mi).

F The F_port that is used when connected to devices.

E The E_port that is used for interswitch connectivity.

The total number of frame buffers in a quad is limited. Table 10 shows how the Extended Fabric port matrix introduces a combination of long distance ports that are available.

Table 10. Combination of long distance ports that are available

Port 0	Port	Port 2	Port 3
L1	F or E	F or E	F or E
L1	L1	F or E	F or E
L1	L1	L1	F or E
L1	L1	L1	L1
L2	F	F	F
L2	E	F	
L2	E		
L2	L1	F	
L2	L1		

Setting the port configuration

You can configure a port to support long distance links by using the **portCfgLongDistance** Telnet command. See the *IBM TotalStorage SAN Fibre Channel Switch 3534 Model F08 Command Reference Guide* for a complete description of this command.

Chapter 6. Fabric Watch

This chapter provides the following information about Fabric Watch:

Fabric Watch overview

Fabric Watch is an optionally licensed product used by SAN managers to monitor key fabric and switch 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 values exceed the defined boundaries. The SAN manager can configure which elements, such as error, status, and performance counters within a 3534 switch, are monitored.

Fabric Watch runs on 3534 Model F08 and 2109 F series switches that are running Fabric OS version 3.0 or later. The 3534 1RU and 2109 S series switches require Fabric OS version 2.2 or later. Fabric Watch can be accessed through:

- TotalStorage Specialist
- A Telnet interface
- An SNMP-based enterprise manager
- The Fabric Watch configuration file

Fabric Watch monitors the following elements:

- Fabric events (such as topology reconfigurations and zone changes)
- Switch environment (fans, power supplies, and temperature)
- Ports (state changes, errors, and performance)
- GBICs (for switches equipped with SMART GBICs, such as the Finisar SMART GBIC FTR-8519-3)

With Fabric Watch, each switch continuously monitors error and performance counters against a set of defined ranges. Fabric Watch makes this information available 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 break out of acceptable ranges, an event occurs. One or more reporting mechanisms called *alarms* are generated if configured for the relevant threshold:

- SNMP trap
- Entry in the switch event log
- Locking of the port log to preserve the relevant information
- E-mail alert
- Remote Asynchronous Notification (RAN) alert

Note: The RAN alert is only available if the optional Fabric Watch license has been purchased and turned on.

You can deploy Fabric Watch as shipped, or download a customized configuration profile from the following Web site:

www.ibm.com/support/

There are three behavior models for thresholds:

- Range threshold
- Rising or falling threshold
- Change monitor threshold

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. A range threshold can generate events while the value is outside the limits or when the value is within the prescribed range again.

Figure 88 shows an example of an error counter with a temperature range threshold.

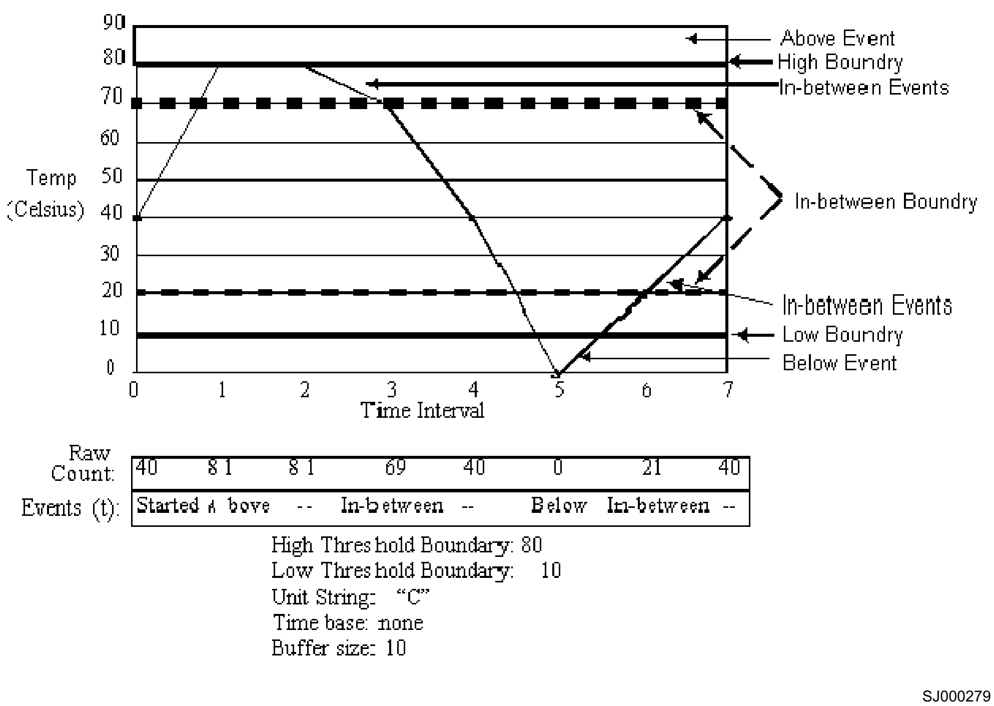


Figure 88. Example of range threshold: temperature (Celsius)

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 zero. Events can be selected for transitions between the boundaries. Rising or falling thresholds are typically used for rate-based counters.

Figure 89 shows an example of an error counter with a rising or falling threshold.

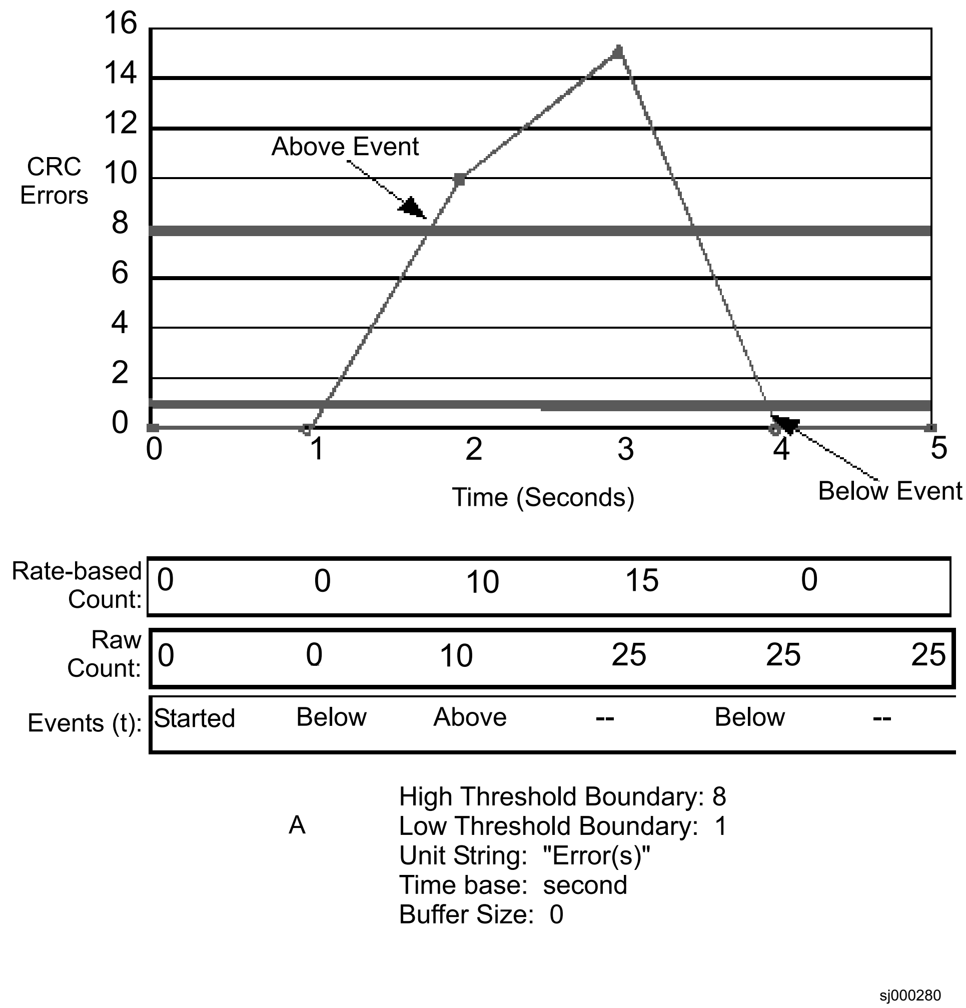


Figure 89. Example of rising or falling threshold: error rate

Change monitor threshold

A change monitor threshold generates events whenever a counter value changes, regardless of the type of change. This type of threshold is used to indicate state changes, such as zoning changes. Change monitor thresholds do not include boundaries.

Installing Fabric Watch

Each switch running Fabric Watch must have a Fabric Watch license installed. A license might have been installed in the switch at the factory. If not, contact IBM to obtain a license key. Fabric Watch requires a 3534 Model F08 or 2109 F series switch running Fabric OS version 3.0 or later. The 3534 1RU and 2109 S series switches require Fabric OS version 2.2 or later. A Fabric Watch license can be installed either using Telnet commands or using TotalStorage Specialist.

Installing Fabric Watch using Telnet

Perform the following steps to install Fabric Watch using Telnet.

1. Login to the switch through Telnet using an account that has administrative privileges. See “Logging into a switch” on page 19.
2. To determine whether a Fabric Watch license is already installed on the switch, type `licenseShow` on the Telnet command line.

   A list of all the licenses that are currently installed on the switch displays. For example:

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

   If the Fabric Watch license is correctly listed, the feature is installed and is immediately available. If the Fabric Watch license is not included in the list or is incorrect, continue with steps 3 and 4.
3. Type the following on the command line:

   `licenseAdd "key"`

   where `"key"` is the license key that was provided to you, surrounded by double quotation marks. 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.

Installing Fabric Watch using TotalStorage Specialist

Perform the following steps to install Fabric Watch using TotalStorage Specialist:

1. Launch the Web browser.
2. Type the switch name or IP address in the **Location/Address** field and press Enter.

   TotalStorage Specialist launches, displaying the Fabric view.
3. Click **Admin** on the relevant switch panel.

   The logon window displays.
4. Type a logon name and password with administrative privileges and press Enter.

   The Administration view displays.
5. Select the **License Admin** tab.
6. Type the license key in the **License Key** field and click **Add License**.

   The Fabric Watch feature is available as soon as the license key is added.

Using Fabric Watch

Fabric Watch provides the following information about each out-of-boundary condition discovered:

- 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 counter, used to compute the rate of change (for example, events per minute)
- Historical information about the last alarmed event that was generated

User interfaces

You can use either TotalStorage Specialist, a Telnet interface, an SNMP-based enterprise manager, or the configuration file to view and modify Fabric Watch settings.

TotalStorage Specialist

Through TotalStorage Specialist, you can:

- View fabric and switch events through the fabric-wide Event view.
- View and modify threshold and alarm configurations through the Fabric Watch view.
- Upload and download the configuration file through the **Config Admin** tab in the Administrative Interface.

Telnet interface

Through a Telnet interface, you can:

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

SNMP-based enterprise managers

The Fabric Watch configuration information is stored as MIB variables, allowing you to:

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

Configuration file

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

The configuration file can be uploaded and downloaded through either TotalStorage Specialist (from the **Config Admin** tab in the Administrative Interface) or using Telnet **configUpload** and **configDownload** commands. After downloading the file back to the switch, you must either restart the switch or use the Telnet **fwConfigReload** command to reload the configuration file.

Profiles

Each Fabric Watch profile contains unique threshold and alarm settings. The profiles are:

- Debug
- Workgroup errlog
- Workgroup snmp
- Enterprise errlog

- Enterprise snmp

Each profile is used for a different purpose, and contains only the information and configurations that are different from the default configuration.

The intention is to have distinct configuration settings for enterprise SANs and workgroup SANs.

The default information is always preserved. After loading the profile, you can specify whether the default or the profile information is to be used.

A profile might contain the following information:
- Threshold values:
  - Unit string
  - Time base
  - Lower boundary
  - Upper boundary
  - Buffer size
- Alarm values
  - Change
  - Exceed
  - Below
  - Above
  - In-between
  - Behavior type

Classes

Fabric and switch elements are organized into classes (also known as *agents*), which are groupings of closely related elements. The major classes are:

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

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

Port Monitors port error and performance counters.

E_port
Monitors E_port error and performance counters.

F_port and FL_port (optical)
Monitors optical F_port and FL_port error and performance counters.

F_port and FL_port (copper)
Monitors copper F_port and FL_port error and performance counters.

GBIC Monitors operational values for smart GBICs.

ALPA Monitors AL_PA devices of loop ports

Note: The AL_PA class is only available if the optional Performance Monitoring license has been purchased and turned on.

End-to-End

- Monitors transmitting performance predefined by the SID-DID pair. Configured at run time with either Telnet commands or TotalStorage Specialist.
- Monitors receiving performance predefined by the SID-DID pair. Configured at run time with either Telnet commands or TotalStorage Specialist.
- Monitors CRC errors of predefined SID-DID pair. Configured at run time with either Telnet commands or TotalStorage Specialist.

The configuration information of the End-to-End class is lost when the switch is started or restarted.

The End-to-End filter is preconfigured at run time with either a Telnet command or TotalStorage Specialist.

Note: The End-to-End class is only available if the optional Performance Monitoring license has been purchased and turned on.

Filter

Monitors the filter counter for a given port. Provides the following types of information about the filter:

1. Read command
2. SCSI or IP traffic
3. SCSI Read/Write

The type of filter is predefined by configuring it at run time with either a Telnet command or TotalStorage Specialist.

Note: The Filter class is only available if the optional Performance Monitoring license has been purchased and turned on.

Each Fabric Watch class is subdivided into areas, as listed in Table 11.

Table 11. 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 (FLOGI).
	GBIC change	Monitors insertion or removal of GBIC.

Table 11. Fabric Watch classes and areas (continued)

Class	Area	Description
Environmental	Temperature	Monitors switch temperature.
	Fan	Monitors operation of switch fans.
	Power supply	Monitors status of each power supply.
Port	Link failure count	Monitors the link failure count 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.
E_port	Link failure count	Monitors link failure of each E_port.
	Loss of synchronization count	Monitors 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.

Table 11. Fabric Watch classes and areas (continued)

Class	Area	Description
F_port or FL_Port (optical)	Link failure count	Monitors link failure of each optical F_port or FL_port.
	Loss of synchronization count	Monitors optical F_port or FL_port sync loss.
	Loss of signal count	Monitors optical F_port or FL_port signal loss.
	Primitive sequence protocol error	Monitors optical F_port or FL_port protocol errors.
	Invalid transmission word	Monitors optical F_port or FL_port invalid words.
	Invalid CRC count	Monitors optical F_port or FL_port CRC errors.
	Receive performance	Monitors optical F_port or FL_port receive performance.
	Transmit performance	Monitors optical F_port or FL_port transmit performance.
	State changes	Monitors optical F_port or FL_port state changes.
F_port or FL_port (copper)	Link failure count	Monitors link failure of each copper F_port or FL_port.
	Loss of synchronization count	Monitors copper F_port or FL_port sync loss.
	Loss of signal count	Monitors copper F_port or FL_port signal loss.
	Primitive sequence protocol error	Monitors copper F_port or FL_port protocol errors.
	Invalid transmission word	Monitors copper F_port or FL_port invalid words.
	Invalid CRC count	Monitors copper F_port or FL_port CRC errors.
	Receive performance	Monitors copper F_port or FL_port receive performance.
	Transmit performance	Monitors copper F_port or FL_port transmit performance.
	State changes	Monitors copper F_port or 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.
ALPA	CRC counter	Monitors all active AL_PA devices on loop ports.

Table 11. Fabric Watch classes and areas (continued)

Class	Area	Description
End-to-End	CRC counter	Monitors CRC errors of a predefined SID-DID pair at a given port.
	Transmit performance	Monitors the transmit performance of a predefined SID-DID pair at a given port.
	Receive performance	Monitors the receive performance of a predefined SID-DID pair at a given port.
Filter	Customer-defined fibre-channel word.	Monitors the filter counter for a given port.

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 simply when the monitored value has 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 switch error log, locking of the port log, or a combination of these options.

When an item such as an E_port, F_port or FL_port (optical), F_port or FL_port (copper), smart GBIC, fan, or power supply is removed, Fabric Watch can raise an event (such as a *below event*), then the threshold is hidden and disabled. When an item is added, the threshold is displayed and enabled, and Fabric Watch 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 these boundaries. For example, if the switch temperature exceeds the upper boundary, a triggered event is generated at the point the boundary is crossed, but is not repeated while the temperature remains above the upper boundary.

The following events can be generated as triggered events:

Started
No alarm is generated.

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

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

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

Changed
The counter value has changed.

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

Continuous events

A continuous event results in an event each time the boundary is initially exceeded until the threshold value has returned within the boundaries. For example, if port utilization is above the upper boundary, a new event is generated at each behavior interval until utilization 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 value has changed.

Alarms

Each event can generate one or more alarms. Fabric Watch supports the following types of alarms:

- SNMP trap
- Error log entry
- Locking of the port log
- RAN alert
- E-mail alert

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 that is 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 switch port log to retain detail information about a problem. It is typically used in conjunction with the error log entry.

RAN alert

This alarm sends messages to the remote agent proxy server.

Note: The RAN alert is only available if the optional Fabric Watch license has been purchased and turned on.

E-mail alert

Sends alarms to the corresponding e-mail addresses at run time. See the *IBM TotalStorage SAN Fibre Channel Switch 3534 Model F08 Command Reference*.

Note: This alert only works with firmware images that support TotalStorage Specialist.

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 if the switch is restarted. The following threshold values can be modified.

Status
Can be enabled or disabled. Status is set to enabled by default.

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

Behavior interval
The interval between the same type of alarm. Applies only to continuous events. The default interval is one second.

Threshold area values

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

The following boundary information can be modified:

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

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

Note: The time base boundary can only be modified using the Telnet **configure** command. The time base boundary does not apply to:
- The transmit performance area
- The receive performance area
- The filter class

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

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

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

The following alarms can be added or deleted:

ERRLOG
Logs an error to the switch. If configured properly, sends a message to syslog on the daemon.

SNMP-TRAP
Sends a trap to an SNMP agent.

PORT-LOG-LOCK
Freezes the port log to preserve the log information that was generated at the time of the event. Used for diagnostic purposes.

RAN Sends alarm messages to a remote agent.

Note: The RAN alert is only available if the optional Fabric Watch license has been purchased and turned on.

E-mail Alert
Sends alarm messages to the corresponding e-mail address.

Threshold naming conventions

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

- The abbreviation for the class name (alpha characters, lower case), as shown in Table 12.

Table 12. Threshold class names

Class	Abbreviation
Fabric	fabric
Environment	env
Port	port
E_port	eport
F_port or FL_port (optical)	fopport
F_port or FL_port (copper)	fcuport
GBIC	gbic
ALPA	alpa
End-to-End	ee
Filter	flt

- The abbreviation for the area name (alpha characters, title case) as shown in Table 13 on page 192. For example, Temp for the Temperature area.

Table 13. Threshold area names

Class name:	Area name:	Abbreviation:
Fabric	Domain ID	DI
	E_port down	ED
	Fabric login	FL
	Fabric to Quickloop	FQ
	Reconfigure	FR
	GBIC change	GS
	Segmentation	SC
	Zoning change	ZC
	Name server login	NL
	Name server request	NR
Environmental	Fan speed sensor	Fan
	Temperature (sensor)	Temp
	Power supply	PS
Port, E_port, F_port or F_port (optical), F_port or FL_port (copper)	Invalid CRCs	CRCs
	Link failures	Link
	Protocol errors	ProtoErr
	Receive performance	RXPerf
	Loss of signal	Signal
	State changes	State
	Loss of sync	Sync
	Transmit performance	TXPerf
	Invalid words	Words
GBIC	Temperature (sensor)	Temp
	Receiver power	RXP
	Transmitter power	TXP
	Current	Crnt
ALPA	Invalid CRCs	PerfCRC
End-to-end	Invalid CRCs	PerfCRC
	Transmit performance	PerfTX
	Receive performance	PerfRX
Filter	Filter frame counter	PerfPT

- The index number for the number of the item within the series. Consists of three numbers, for example: 000 for the first port, 001 for the next, and so on. Index numbers for the Fabric, Port, E_port, F_port or FL_port (optical), F_port or FL_port (copper), and GBIC classes begin with 000, and index numbers for the Environment class begin with 001.

Examples of threshold names:

Example 1:

class name = env,

Example 1:

area name = Fan,

element index = 000-002

threshold name is envFan000-envFan002

Example 2:

class name = gbic,

area name = Temp

element index = 001-00x

threshold name is gbicTemp001-gbicTemp00x

Example error message

The following example shows a typical Fabric Watch error log message.

```
0x1003f2d0 (tThad): May 22 19:20:23
   Error FW BELOW, 3, fopportState003   (FOP Port State Changes 3) is below low boundary
   current value : 0 Change(s)/minute. (normal)

0x1003f2d0 (tThad): May 22 19:13:57
   Error FW ABOVE, 3, fopportCRCs007    (FOP Port Valid CRCs 7) is above high boundary.
   current value : 5 Error(s)/minute. (faulty)

0x1003f2d0 (tThad): May 22 17:31:33
   Error FW-ABOVE, 3, fopportSync003    (FOP Port Loss of Sync 3) is above high boundary.
   current value : 3 Error(s)/minute. (faulty)

0x1003f2d0 (tThad): May 22 17:31:33
   Error FW ABOVE, 3, fopportLink003    (FOP Port Link Failures 3) is above high boundary.
   current value : 1 Error(s)/minute. (faulty)

0x1003f2d0 (tThad): May 22 17:31:33
   Error FW CHANGED, 4, fabricFL000     (Fabric Fabric login 4) value has changed.
   current value : 23 Login(s). (info)

0x1003f2d0 (tThad): May 22 17:17:33
   Error FW ABOVE, 3, alpaPerfCRC004    (ALPA Invalid CRCs 4) is above high boundary. (faulty)
```

As you can see in the first part of the example, `fopportState003` is the threshold name. `FOP Port State Changes 3` is the threshold label, where `3` refers to an index number. States shown in the example are `normal`, `faulty`, and `info`.

Fabric Watch Telnet commands

The Telnet commands become available through the shell *admin* account when the license key is installed. To use a Telnet command, login to the relevant switch with administrative privileges, type the command along with any required operands, and press Enter.

Note: Fabric Watch can be accessed simultaneously from different connections, by Telnet, SNMP, TotalStorage Specialist, or by modifying and uploading the Fabric Watch configuration file to the switch. If this happens, changes from one connection might not be updated to the other, and some may be lost. If "`Committing configuration...`" displays during a Telnet session, then the configuration might have recently been modified from another connection.

Table 14 summarizes the Fabric Watch Telnet commands.

Table 14. Fabric Watch Telnet commands

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

For more information about Fabric Watch Telnet commands, see the *IBM TotalStorage SAN Fibre Channel Switch 3534 Model F08 Command Reference*.

Chapter 7. QuickLoop

This chapter provides the following information about QuickLoop:

QuickLoop overview

QuickLoop is a unique fibre-channel topology that combines arbitrated loop and fabric topologies. It is an optional licensed product that allows arbitrated loops to be attached to a fabric. An arbitrated loop supports communication between devices that do not recognize fabrics. Such devices are called *private devices*, and arbitrated loops are sometimes called *private loops*. Without modifying their drivers, private devices on the arbitrated loops can be accessed by public or private hosts elsewhere on the fabric.

A QuickLoop consists of multiple private arbitrated looplets (a set of devices connected to a single port) that are connected by a fabric. All devices in a QuickLoop share a single AL_PA bit map and act as if they are in one loop. This allows private devices to communicate with other devices over the fabric, provided they are in the same QuickLoop.

A particular QuickLoop can be configured to consist of selected devices or looplets that are connected to the ports of one switch, or to a cascaded switch pair.

QuickLoop provides a possible migration path starting with deploying a single private loop and later deploying a fabric-based SAN. In this scenario, QuickLoop-enabled switches can be used to replace hubs when the SAN is first deployed and has only private devices attached. Then, as the SAN grows, fabric switches can be added without any detrimental effect to the QuickLoop-enabled switches.

When a Zoning license is also purchased, the set of storage devices that is visible to specific hosts can be carefully administered.

The QuickLoop and Zoning combination allows a private host to fully participate in a SAN.

Note: QuickLoop is used for 8-bit private loop initiators or hosts.

Address translation

Address translation is transparent and requires no actions on your part. It is achieved through hardware translative mode (also known as phantom mode), in which a device that is not physically located in a looplet is made addressable by a unique AL_PA in that looplet. There are two hardware translative modes available to a QuickLoop-enabled switch:

Standard translative mode
: Standard translative mode allows public hosts to communicate with private target devices across the fabric.

QuickLoop mode
QuickLoop mode allows private hosts to communicate with private target devices across the fabric, when configured in the same QuickLoop. It also allows the private host to communicate with public targets in the same QuickLoop.

In mixed mode, individual ports within a switch are set by configuration commands to either standard translative mode or to QuickLoop mode.

The switch automatically determines and sets the appropriate mode, based on factory defaults and configurations that are currently in effect.

Installing QuickLoop

When you install QuickLoop, you must also install a license on each switch that you want to enable for QuickLoop. A license might have been installed on the switch at the factory. If not, contact your switch supplier to obtain a license key.

QuickLoop requires a 2109 or 3534 series switch with Fabric OS version 3.0 or later installed. You can install a QuickLoop license either using Telnet or TotalStorage Specialist.

Installing QuickLoop using Telnet

Perform the following steps to install QuickLoop using Telnet:

1. Login to the switch through Telnet, using an account that has administrative privileges.
2. To determine whether a QuickLoop license is already installed on the switch, type `licenseShow` on the Telnet command line.

   A list of all the licenses that are currently installed on the switch displays. For example:

```
admin> licenseShow
1A1AaAaaaAAAA1a:
Release v3.0
Web license
Zoning license
SES license
```

   If the QuickLoop license is correctly listed, QuickLoop is installed and is immediately available. If the QuickLoop license is not included in the list or is incorrect, continue with steps 3 and 4.
3. Type the following on the command line:

   `licenseAdd "key"`

   where `"key"` is the license key that was provided to you, surrounded by double quotation marks. 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 license is not listed, repeat step 3.

Installing QuickLoop using TotalStorage Specialist

Perform the following steps to install QuickLoop using TotalStorage Specialist:

1. Launch a Web browser.
2. Type the switch name or IP address in the **Location/Address** field of the browser and press Enter.

   TotalStorage Specialist launches, displaying the Fabric view.
3. Click **Admin** on the relevant switch panel.

   The logon window displays.
4. Type a logon name and password with administrative privileges and press Enter.

   The Administration view displays.
5. Select the **License Admin** tab.
6. Type the license key in the **License Key** field, and click **Add license**.

   The QuickLoop feature is available as soon as the license key is added.

Administering QuickLoop

You can manage QuickLoops using Telnet commands or using TotalStorage Specialist.

Administering QuickLoop with Telnet commands

The Telnet commands for QuickLoop become available through the shell admin account when the basic QuickLoop license key is installed.

To use a QuickLoop Telnet command, login to the relevant switch with administrative privileges, type the command along with any required operands, and press Enter.

For a description of all the Telnet commands that are provided for managing QuickLoop, see the *IBM TotalStorage SAN Fibre Channel Switch 3534 Model F08 Command Reference Guide*.

Administering QuickLoop with TotalStorage Specialist

Using TotalStorage Specialist, you can view and modify the QuickLoop settings from the **QuickLoop Admin** tab on the Switch Admin Interface view. For detailed information about installing and using TotalStorage Specialist for the QuickLoop feature, see Chapter 3, “TotalStorage Specialist” on page 37.

Using QuickLoop

You can enable or disable QuickLoop for either the entire switch or for particular ports. When QuickLoop is disabled on a particular port, that port returns to Fabric mode. When QuickLoop is enabled on a port, the port is added to the same QuickLoop to which the switch belongs.

A QuickLoop is either single-switch, where all looplets are located on a single switch, or dual-switch, where looplets are located on either of two partnered switches. However, a switch can be in only one QuickLoop. A QuickLoop includes all or some of the ports on a switch or cascaded switch pair, and can have several private hosts. Public hosts in an arbitrated loop mode are considered private devices when connected to QuickLoop ports.

A switch can be configured to operate in any of the following modes:

QuickLoop mode
All ports on the switch, except for E_ports or loopback ports, are enabled for QuickLoop and participate in a logical Private Loop Direct Attach (PLDA). On request, this can be set as the manufacturing default. This mode can also be set using the Telnet **qlEnable** command.

Fabric mode
No ports are QuickLoop-enabled (none participate in any logical PLDAs), and all ports operate as Fibre Channel - Fabric Loop Attach standard (FC-FLA) compliant devices. This mode can be set using the Telnet **qlDisable** command.

Mixed mode
Each port is set to QuickLoop on an individual basis. The operating mode of the port can be reset during operation. Ports that are set to QuickLoop become looplets of the QuickLoop to which the switch belongs. Particular ports can be taken in and out of the QuickLoop using the Telnet **qlPortDisable** and **qlPortEnable** commands.

Note: These modes cannot be configured by SNMP.

A switch has a default mode, which depends on the switch model. When the switch is turned on, all the ports are set to the default mode.

QuickLoop topology

QuickLoop topologies have the following characteristics:

- A QuickLoop can include up to two switches and can support up to 126 AL_PA devices.
- Each particular switch can only be included in one QuickLoop.
- A QuickLoop can include either all of, or a subset of, the ports on a particular switch.
- Multiple non-overlapping QuickLoops can exist in a fabric of multiple switches.
- QuickLoop-enabled switches can exist in the same fabric as non-QuickLoop enabled switches.
- A device that is attached to a QuickLoop can communicate with all other devices that are attached to the same QuickLoop.
- A private device in a QuickLoop can only communicate with devices in the same QuickLoop. Existing PLDA-capable host drivers do not need to be modified to perform I/O operations with storage devices.
- Public devices that are arbitrated loop capable are treated as private devices when connected to QuickLoop ports (their fabric login, or FLOGI, is not valid).
- Legacy devices can be used in a QuickLoop and can be attached to a fabric and operate as if in a PLDA environment.
- QuickLoop functionality can be enabled or disabled for either the entire switch or for particular ports. When QuickLoop is disabled on a particular port, that port returns to Fabric mode.
- Each looplet in a QuickLoop has its own unshared bandwidth and can support transfer rates up to 100 MBps.
- Multiple devices can communicate simultaneously between at least four separate switch ports at full bandwidth within multiple looplets located in the same QuickLoop. These simultaneous conversations cannot involve overlapping looplets.

- If a looplet error is detected, QuickLoop automatically takes that looplet out of service. If the error condition is cleared, the looplet is automatically reinstated.

Implementing QuickLoop

You implement QuickLoop using a combination of hardware and software components. It requires no actions on your part after it is installed and configured. The hardware components are responsible for transporting frames among looplets and across switches, and the software components are responsible for initializing QuickLoop and for error handling.

Terminology

The terms and concepts introduced in this section are fundamental to understanding the use of QuickLoop mode with switches.

The following two port types are on host or storage devices, not on switches.

N_port (node port)
: An equipment port that is not loop capable. It is used to connect the equipment to the fabric.

NL_port
: An equipment port that is loop capable. It is used to connect an equipment port to the fabric in a loop configuration through the FL_port on a switch.

There are eight physical ports on the 3534 Model F08 switch. Each port can be independently configured as one of the following types.

F_port
: A fabric port that is not in loop mode. It is able to transmit under fabric protocol and interface over links. N_ports on equipment connect to F_ports on switches.

FL_port
: A fabric port on a switch that is loop capable. It is used to connect loop-capable NL_ports to the switch in a loop configuration.

E_port
: An expansion port that 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, or to build a two-switch QuickLoop configuration.

Sometimes, a single fabric loop device is attached to a port. In this case the port functions as an F_port. The attached device possesses either an N_port (if the device is fabric-capable) or an NL_port, in which case the device would be connected to the fabric in a loop configuration through an FL_port on a switch. In this latter case, a looplet is created.

looplet
: A set of devices connected in a loop to a port that is itself a member of an arbitrated loop. By contrast, a single device rather than a loop might be connected to a port.

Each device in a private loop must have a unique physical address. The devices in a QuickLoop are assigned a unique phantom AL_PA.

AL_PA
: Arbitrated loop physical address. It is a one byte value used to identify a device in an arbitrated loop.

When implementing and operating switches in a QuickLoop, messages are transmitted by devices as they come online. These messages, called LIPs, are in addition to normal data traffic.

LIP Loop initialization primitive

Dual-switch QuickLoop

In a dual-switch QuickLoop, the initialization process is driven by one of the switches, called the QuickLoop master. The role of the QuickLoop master is dynamically assigned at each instance of QuickLoop initialization, according to the following criteria:

- If one switch receives LIPs from its looplets and the other does not, the switch that receives the LIPs is the QuickLoop master.
- If both switches receive LIPs from their respective looplets, the switch with the lower domain ID is the QuickLoop master.

QuickLoop initialization

QuickLoop initialization includes two passes:

Pass 1: Sequential Looplet Initialization
This pass allows each device in the QuickLoop to obtain a unique AL_PA in a single AL_PA bitmap. Only those looplets from which LIPs were received are initialized, using the loop initialization procedure described in the FC-AL standard. The AL_PAs of devices in looplets from which no LIPs are received are preserved during initialization.

Pass 2: Full Initialization
This pass sets up the QuickLoop as a single logical PLDA. This is accomplished by making all assigned AL_PAs addressable by any device in the QuickLoop, regardless of whether the destination device and source device are in the same physical looplet. If the destination and source devices are not in the same physical looplet, the hidden FL_port in the source device looplet acts on behalf of the destination device, and the fabric provides the transport service.

If Zoning is in use, the looplets that are initialized depend upon the zoning configuration.

Error handling

QuickLoop isolates faulty switches or ports by excluding them from the initialization process. This allows the impact of a faulty looplet or switch to be minimized on normal QuickLoop operations, and is particularly important for QuickLoops that contain multiple looplets that are distributed across two switches.

Switch level errors

Switch level errors affect dual switch QuickLoops, and include the following conditions:

- No switch with the WWN of the configured partner switch can be found in the fabric.
- No response is received from the partner switch during the initial handshake.
- Inconsistent responses are received from the partner switch.
- Responses are not received in time during QuickLoop initialization.

If one of these errors is detected on a switch, the partner switch reinitializes, forming a separate QuickLoop that contains only the devices on the partner switch. This creates two QuickLoops. If the error condition is removed, the QuickLoops are reinitialized to form a single QuickLoop. If the recovery procedure fails, the switches remain in the single switch QuickLoops, and the procedure is run again after a timeout period.

Port level errors

Port level errors affect looplets, and include the following conditions:

- Any physical level errors occur, such as loss of synchronization or laser fault.
- The frequency of LIPs received from a port exceeds a threshold.
- A port fails to become the Loop Initialization Master within a timeout period after LIPs are either received from or sent to the port.
- A port does not receive a loop initialization sequence back within a timeout period after the sequence is sent.

If an error is detected on a looplet, the QuickLoop is reinitialized with the looplet excluded. The error condition is monitored, and if the condition is removed, the looplet is included again into the QuickLoop.

The looplet error recovery procedure includes the following steps:

1. LIPs are issued to the looplet, and it is determined whether the hidden FL_port enters OPEN-INIT and becomes the Loop Initialization Master.
2. The rest of the standard loop initialization sequences are completed, and it is determined whether the looplet can be fully initialized within a timeout period.
3. The looplet is kept idle and it is determined whether it remains stable.

If the procedure fails at any time, the looplet remains isolated from the QuickLoop, and the procedure is run again after the timeout period. If all the steps are successfully completed, the looplet is reinstated into the QuickLoop by full initialization.

Sample configurations

The following section includes examples that show possible configurations of one or two switches to form a QuickLoop.

Configuration 1
A simple configuration in which a QuickLoop-enabled switch is used as a hub emulator or concentrator. See Figure 90 on page 204.

Configuration 2
A dual-switch configuration in which two switches are cascaded by a local fiber connection to make up a QuickLoop. See Figure 91 on page 205.

Configuration 3
A dual-switch configuration in which two switches up to 10 km apart are connected to make up a QuickLoop. See Figure 92 on page 206.

Configuration 4
A mixed-mode configuration in which only some of the ports of two cascaded switches are enabled for QuickLoop. See Figure 93 on page 207.

In each of these examples, the dotted line represents the logical QuickLoop or the ports that form the QuickLoop.

A QuickLoop zone is a subset of a QuickLoop.

Configuration 1: Emulating a hub

Figure 90 shows multiple hosts and devices that are connected to a QuickLoop-enabled switch. The switch serves as a concentrator, similar to a hub except that the switch offers throughput performance of 100 MBps on each looplet .

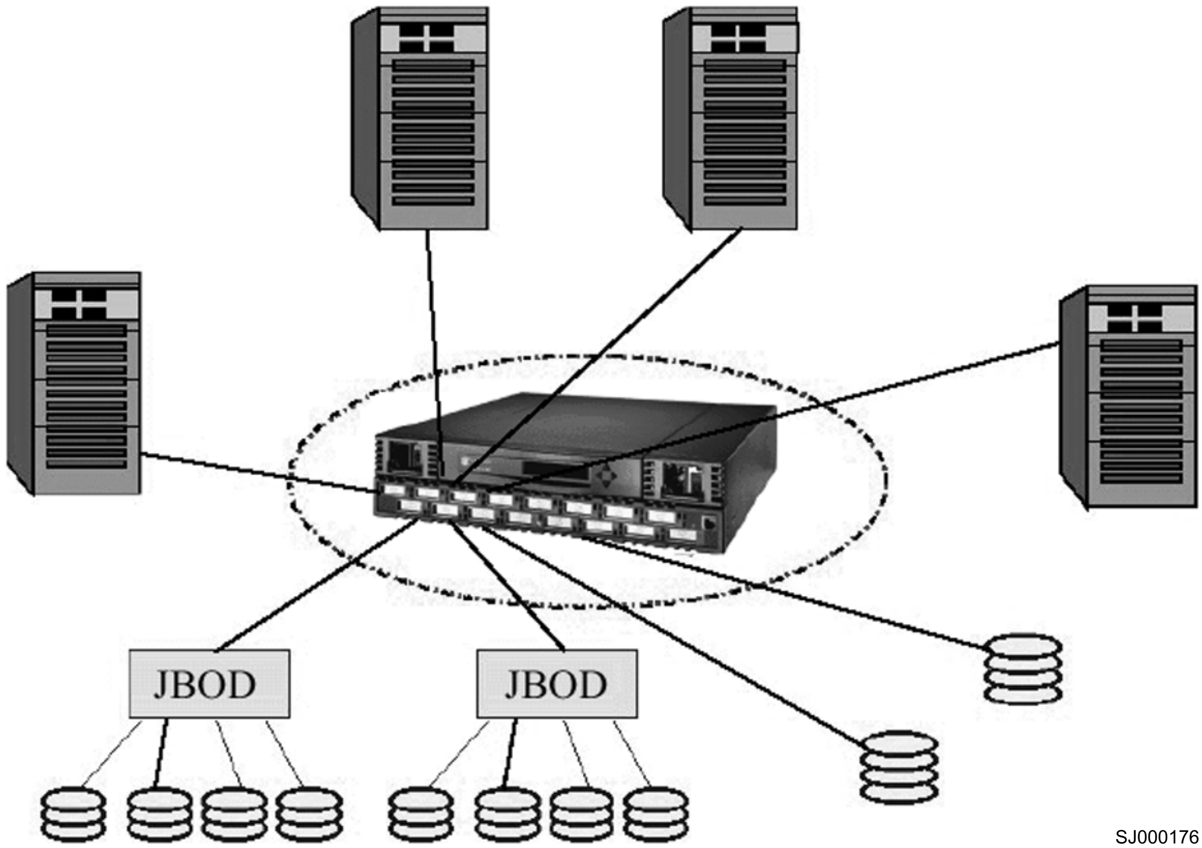


Figure 90. QuickLoop-enabled switch used as concentrator

Configuration 2: Dual-switch QuickLoop

Figure 91 shows two switches cascaded by a local fiber connection between E_ports into a single logical PLDA. The ports that are configured on both switches in the QuickLoop share a single AL_PA space. Neither switch can participate in a different QuickLoop. The QuickLoop can be further subdivided into one or more QuickLoop zones.

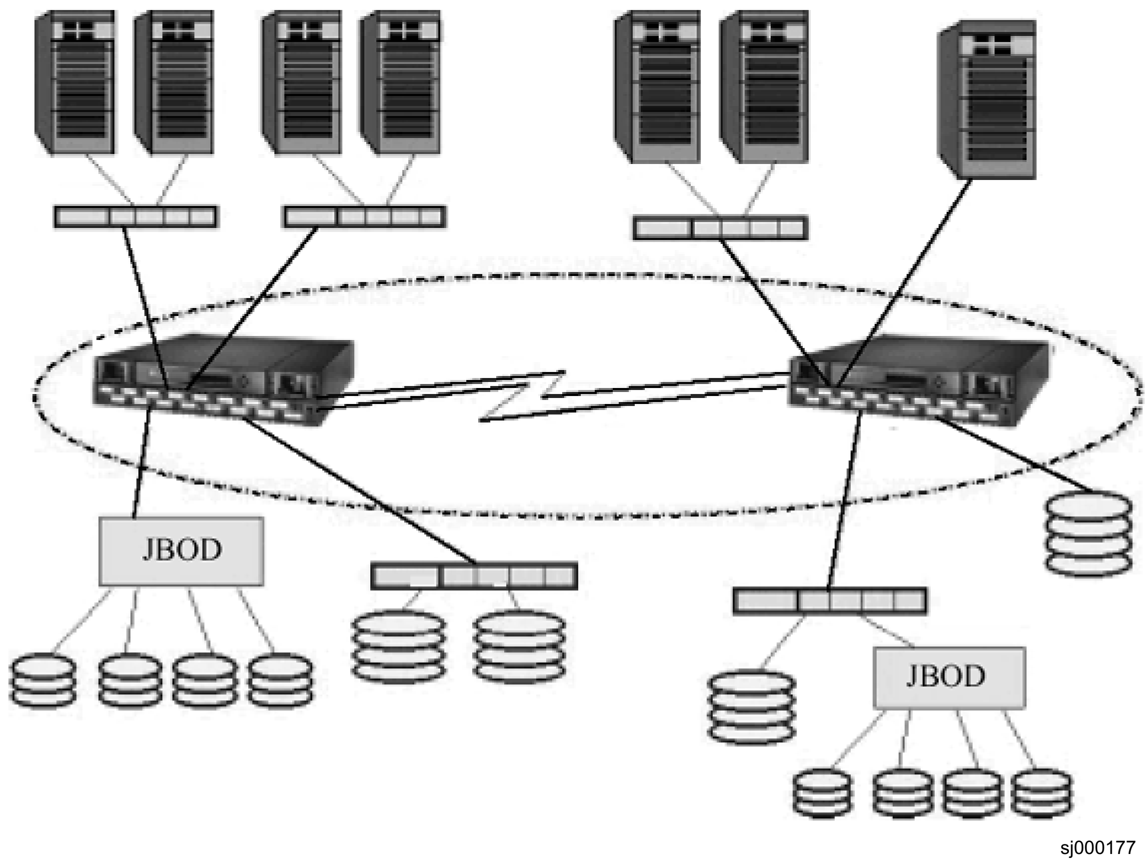


Figure 91. Dual-switch QuickLoop configuration

Configuration 3: Long distance QuickLoop

Figure 92 shows two switches cascaded by a longwave laser into a single logical PLDA. Both switches operate in QuickLoop mode and connect devices at distances of up to 10 km (6.21 mi).

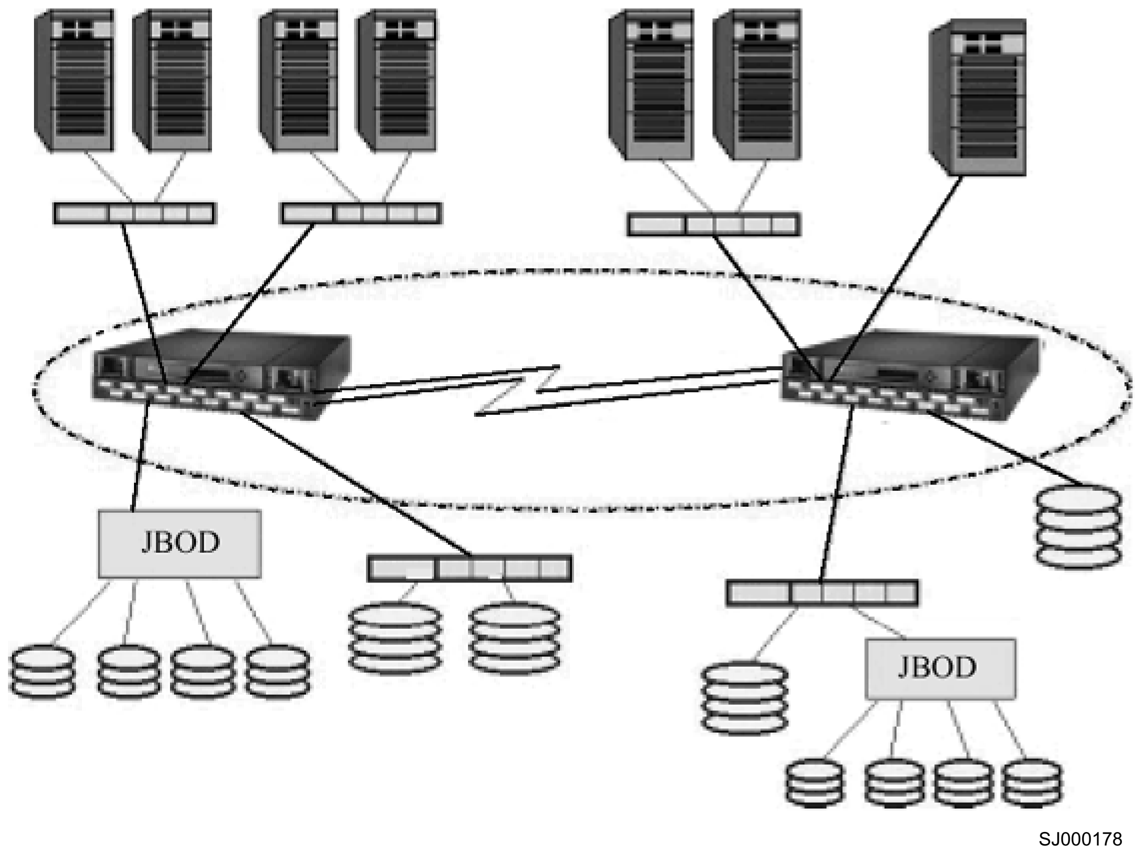


Figure 92. Long-distance QuickLoop configuration

Configuration 4: Mixed QuickLoop mode and fabric mode

Figure 93 shows a sample configuration of a mixed mode environment, with ports set on an individual basis to either QuickLoop mode or Fabric mode. In this example, a fabric is formed from two cascaded switches: 3534 Model F08 No. 1 and 3534 Model F08 No. 2.

- The ports to which the looplets within the QuickLoop are attached, ports (1,14), (1,15), (2,0), and (2,1), are all QuickLoop-enabled FL_ports.
- Private target device **a** and public target device **f** are attached to FL_ports (1,0) and (2,14).
- Public host **G** is attached to an F_port, (1,1).
- Because it is in the same QuickLoop, private host **J** can access the private target devices **b** and **c** even though they are attached to a different switch.

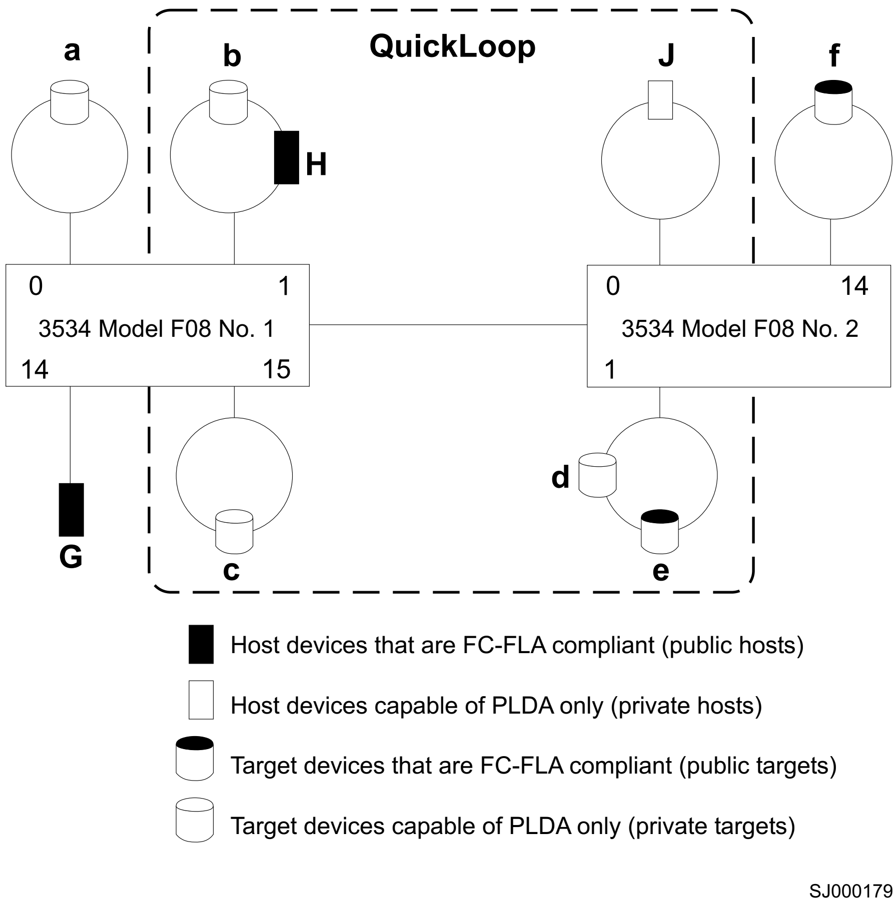


Figure 93. Mixed mode QuickLoop configuration

Table 15 lists the methods that the hosts in this example would use to communicate with the targets.

Table 15. Configuration access methods

Host	Target a	Target b	Target c	Target d	Target e	Target f
G	Fabric[1] (standard translative) mode	Fabric[1] (standard translative) mode	Fabric[1] (standard translative) mode	Fabric[1] (standard translative) mode	Fabric[1] (standard translative) mode	Fabric (FLA)
H	No access[2]	PLDA	QuickLoop mode	QuickLoop mode	QuickLoop mode	No access[2]
J	No access	QuickLoop mode	QuickLoop mode	QuickLoop mode	QuickLoop mode	No access

Notes:

1. A public host accesses a device on QuickLoop by translative mode (phantom), in the same way that it accesses a private device that is attached to an FL_port.
2. Devices that are connected to QuickLoop lose their public functions. FLOGIs sent by these devices are dropped, forcing them back to a private loop attachment.

Chapter 8. SCSI-3 Enclosure Services (SES)

This chapter provides the following information about SCSI-3 Enclosure Services (SES):

SES overview

SES allows a host that is connected to a fabric switch to manage all the switches in the SAN. This is done remotely, in-band through a fibre-channel link. SES serves as the access management method for SCSI-based legacy environments where no fibre-channel IP driver is available. A host with fibre-channel IP capability typically does not need SES.

Features

The SES implementation complies with the SCSI-3 protocol standard that is used for implementing SES. The following features are available with SES:

- Accessing and managing every 2109 and 3534 switch in the fabric
- SES capability of the fabric that cannot be stopped by any single failure
- Managing a fabric of 2109 and 3534 switches in a storage environment that is exclusively SCSI-based
- Configuring switches in a fabric (for example, enabling or disabling a port)
- Performance monitoring (for example, view frame and word counters of a port)
- Enclosure monitoring (for example, view temperature sensor readings)
- SES management is scalable as the fabric enlarges
- SES-enabled host can immediately begin managing 2109 and 3534 switches
- Availability of industry-standard SES commands

SES requirements

SES requires the following:

- An SES-enabled host workstation
- A physical connection through a fibre-channel link from the host to one switch in the SAN
- Fabric OS version 1.4 or later on all switches
- An SES software license key

Managing a fabric with SES

To manage a SAN using SES, a host must have a fibre-channel link to a switch in the fabric. The host must support fibre-channel protocol (FCP) for SCSI-3 and must recognize the FCP target at the management server well-known address (FFFFFAh).

The host must perform the normal N_port login procedure with the management server. It can then initiate an appropriate SES request.

Based on the management information obtained through SES, the host can perform a configuration, performance, or enclosure function on the switch. For example, it can enable or disable a switch port, take the temperature sensor readings of a switch, or monitor the performance or error counters of a switch port.

FCP constructs, SES commands, and diagnostic pages

You use FCP constructs and SES commands to manage and sense the operational status of the power supplies, cooling devices, displays, indicators, individual drives, and other non-SCSI elements that are installed in a switch.

The following FCP constructs are supported:

- FCP information unit
- FCP transfer ready information unit
- FCP data information unit
- FCP response information unit

The following basic SES commands are supported:

- Inquiry
- Report LUNs
- Request sense
- Test unit ready
- Reject

The following extended SES commands are supported:

- Read buffer
- Receive diagnostics results
- Send diagnostic
- Write buffer

The following diagnostic pages are supported:

- Supported diagnostics pages
- Switch page
- Sensor table page
- Fabric page
- Neighborhood table page
- Fibre-channel port table page
- Name server local table page
- Event table page
- Port error and interrupt statistics table page
- Fabric inquiry data page

- MIB-II system group page
- Port log table page
- Unicast route table page

FCP constructs, SES commands, and diagnostic pages are discussed in more detail later in this chapter.

SES address allocation

A switch is identified at the FCP level by its LUN. The switch domain ID is used to assign the LUN address for each switch in the fabric, including the switch that is used to access the fabric. To get a list of LUNs in the fabric, the FCP host sends a command to LUN 0 of the target at the management server well-known address. From there the host specifies a specific LUN address during an SES command request.

Figure 94 shows a sample fabric managed by a host that is connected to the switch LUN L5.

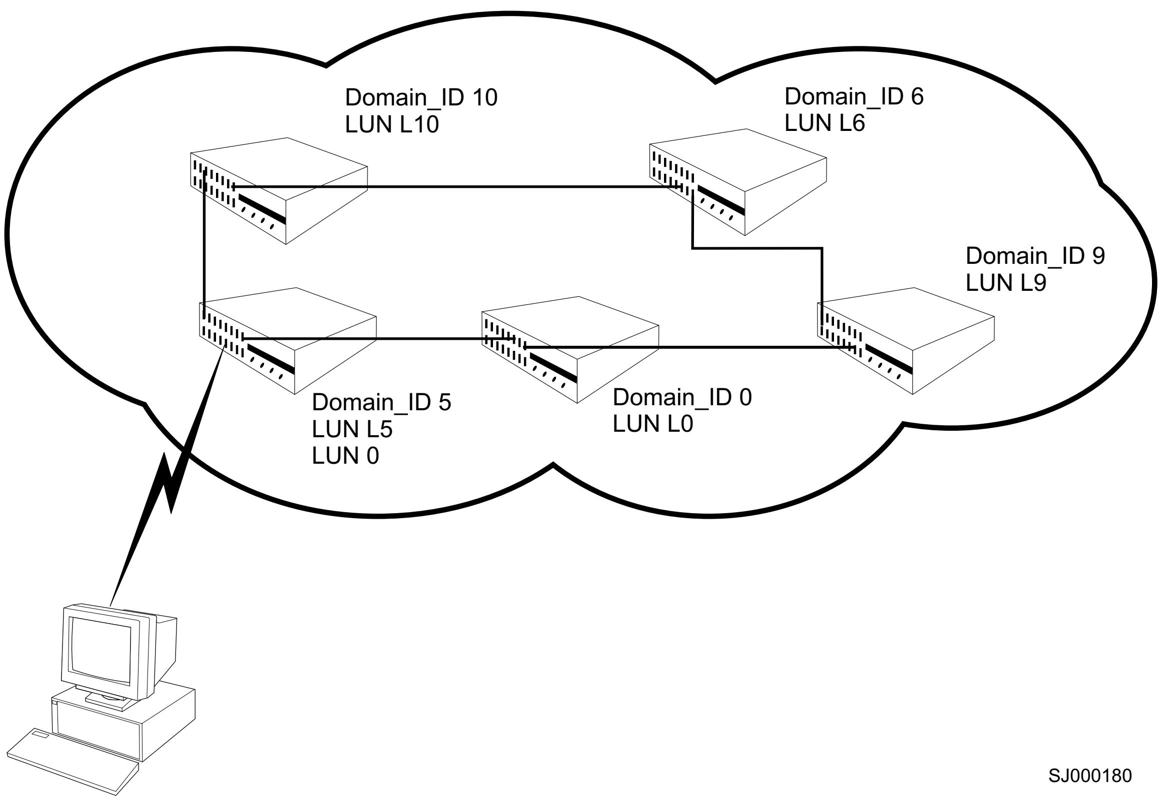


Figure 94. SES switch management

Outside the fabric, other SCSI-3 enclosures can also run SES. For example, JBODs, RAID-5 arrays, SCSI-3 hard drives, and SCSI-3 tape drives can run SES. These devices are identified by their fabric and SCSI addresses, and are assigned LUNs using standard SCSI-3 host adapter LUN addressing.

Installing SES

SES is an optional feature and requires a license key to be fully activated. Without a license key, only the basic FCP commands are supported.

Note: A license key might have been installed at the factory.

Perform the following steps to install an SES license using Telnet:

1. Login to the switch using Telnet, using an account that has administrative privileges.
2. To determine whether an SES license is already installed on the switch, type `licenseShow` on the Telnet command line.

   A list of all the licenses that are currently installed displays. For example:

```
admin> licenseShow
9A9AaAabaATAS0a:
    Web license
    Zoning license
```

   If the SES license is correctly listed, SES is fully installed. If the SES license is not included in the list, continue with steps 3 and 4.
3. On the Telnet command line, type:

   `licenseAdd "key"`

   where `"key"` is the license key surrounded by quotation marks. The license key is case sensitive and must be entered exactly as given. For example, `9A9AaAabaATAS0b`.

   Attention: Make sure that you type the license key exactly as shown in your license agreement. If you type an invalid license key, any existing license is overwritten.
4. After the license key is added, verify that it was installed correctly by typing `licenseShow` on the Telnet command line. If the license is not listed, repeat 3. If the license is listed, restart the switch.

```
admin> licenseshow
9A9AaAabaATAS0a:
    Web license
    Zoning license
9A9AaAabaATAS0b:
    SES license

admin> reboot
```

SES concepts

This section provides detailed information about SES concepts.

SES fabric distribution

SES is distributed transparently throughout the fabric, with an instance of a distributed SES device (SESD) on each switch. Each switch must be upgraded with a license key to activate the software. Without the license key on a particular switch, the associated SESD only responds to the basic set of FCP commands.

SES functional model

Each SESD can be accessed by an SES application client by specifying the associated unique LUN. Additionally, SES implementation also provides an SES application client and an in-band mechanism for managing any fabric switch that it is attached to. Figure 95 shows the SES functional model.

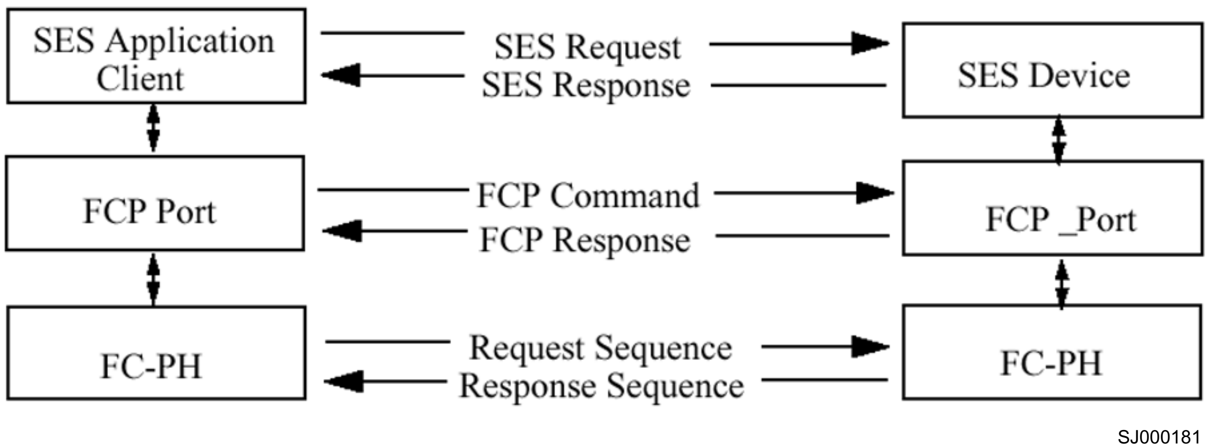


Figure 95. SES functional model

At the fibre-channel level, each SESD is accessible using the management server well-known address, FFFFFAh. At the SCSI-3 level, the SESD is associated with a LUN. An SES application client can refer to any distributed SESD within the fabric using its LUN. A LUN value of 0 is always associated with the local switch that is physically attached to the SES application client. The unique LUN value is mapped based on peripheral device addressing.

The bus number for each switch is set to 010000b, as shown in Table 16. Byte 1 of the target or LUN is set using the Domain_ID of the switch. Bytes 2 through 7 are set to zero.

Table 16. Bus number

Byte/Bit	7	6	5	4	3	2	1	0
0	0	0	Bus Number = 010000b					
1	Target or Logical Unit Number (LUN)							
2 - 7								

An SES application client can easily find the LUN values of all distributed SESDs inside the fabric by sending the **Report LUN** command (see “Report LUN command” on page 218).

Access to the SES process

An SES application client can monitor all enclosures that are capable of processing the SES command set. SES monitors both devices inside and outside of the enclosure (for example, a UPS device). However, the 3534 Model F08 SES pertains only to SESDs inside the fabric.

An SES application client connects to any 3534 Model F08 switch running FCP using the management server well known address, FFFFFAh. The SES command set uses the **receive diagnostic results** and **send diagnostic** commands to any switch that supports SES.

Access using an SESD

The application client requests information from the SESD to examine the status and warning information from the switch. An application client using FCP calls the SES process that is running on any 2109 or 3534 switch as a LUN that has SES enabled. The SESD sets the SES bit (EncServ) in the **inquiry** command to indicate that it can transport SES information. See “Inquiry command” on page 216 for more information.

Indicators and control management

An application client uses the **send diagnostic** command to transport control information to the SESD that is running SES. The control information can include operations to perform or to modify its operating mode.

The application client uses the **receive diagnostic results** command with the Page Code Valid (PCV) bit to obtain enclosure status. See “Receive Diagnostic Results command” on page 223 for more information.

Additionally, the instructions from the application client can be ignored or overwritten by the SES processor to ensure proper state information. For example, the enclosure can ignore an instruction to clear an error condition because the condition is valid or because the instruction is not supported by the enclosure.

FCP constructs

Before initiating any FCP request, the N_port that is associated with the SES application client (FCP initiator) must complete an N_port login (PLOGI) with the management server in Class 2 or 3. The destination address in the PLOGI request must be set to FFFFFAh. The FCP process login (PRLI) is not required but it is supported by the SESD.

The format of an FCP command (FCP_CMND), FCP transfer ready (FCP_XFER_RDY), FCP data (FCP_DATA), and FCP response (FCP_RSP) conforms to those formats that are defined in the SCSI-3 FCP, Revision 12, X3T10/269, working draft.

FCP construct summary

Table 18 lists descriptions of the FCP information units (IUs):

Table 17. FCP construct summary

Information Unit	Description
FCP information unit (FCP_CMD)	Contains a SCSI command to be run or a task management request on a target.
FCP transfer ready information unit (FCP_XFER_RDY)	Indicates that the target is ready to perform the data transfer that is associated with an FCP_CMD.
FCP data information unit (FCP_DATA)	Contains data that is associated with an I/O operation.
FCP response information unit (FCP_RSP)	Contains status and sense information.

FCP_CMND information unit

The FCP_CMND IU carries either a SCSI command to be run or a task management request to be performed. Table 18 lists the values and control fields defined in its payload.

Table 18. FCP_CMND format

Field name	Description	Byte number	Byte size
FCP_LUN	Logical unit number	0 - 7	8
FCP_CNTL	Control flags and bits for task management	8 - 11	4
FCP_CDB	SCSI command descriptor block	12 - 27	16
FCP_DL	Data length	28 - 31	4

For local switches, the FCP_LUN value is 0. For remote switches, the FCP_LUN value is determined as described in "SES functional model" on page 213. The FCP_CNTL value is set to 1 or 2 depending on whether you are specifying write data or read data, respectively. All other values are invalid. The FCP_CDB value contains the appropriate command descriptor. The FCP_DL field contains a count of the maximum number of data bytes to be transferred to or from the target for the command.

FCP_XFER_RDY information unit

The FCP_XFER_RDY IU contains SCSI-3 data delivery service parameters that are required by the initiator and that must be transmitted preceding each read or write FCP_DATA IU.

FCP_DATA information unit

The FCP_DATA IU transfers the actual data.

FCP_RSP information unit

The FCP_RSP IU carries the response status and sense information that is associated with a particular FCP_CMND. Table 19 shows the fields that are associated with FCP_RSP.

Table 19. FCP_RSP format

Field name	Description	Byte size
Reserved	Reserved	8
FCP_STATUS	Status of the linked or previous request	4
FCP_RESID	Residual count	4
FCP_SNS_LEN	Length of sense information (FCP_SNS_INFO)	4
FCP_RSP_LEN	Length of response information (FCP_RSP_INFO)	4
FCP_RSP_INFO	FCP response information (FCP_RSP_INFO)	m
FCP_SNS_INFO	SCSI sense information (FCP_SNS_INFO)	n

Table 20 shows the format of the FCP_STATUS field.

Table 20. FCP_STATUS format

Byte	Bit	Definition
0	7 - 0	Reserved
1	7 - 0	Reserved
2	7 - 4	Reserved
	3	FCP_RESID_UNDER
	2	FCP_RESID_OVER
	1	FCP_SNS_LEN_VALID
	0	FCP_RSP_LEN_VALID
3	7 - 0	SCSI status byte code from the SCSI logical unit

The reserved bits are set to 0 by the SESD. FCP_RESID_UNDER indicates that the FCP_RESID field is valid and contains the number of bytes expected to be transferred, but were not transferred. FCP_RESID_OVER indicates that the FCP_RESID field is valid and contains the number of bytes that have been truncated because the FCP_DL was not sufficient. These two bits can be set by the SESD.

SES commands

This section provides information about the SES commands.

Basic SES commands

Table 21 shows the basic SES commands that are supported by SESD. These commands do not require an SES license key.

Table 21. Basic SES command summary

Command	Operation code	Description
Inquiry	12h	Contains information about the devices and sensors in an enclosure.
Report LUN	A0h	Contains information returned from SESD containing the LUNs that are attached to the SESD.
Request Sense	03h	Used to sense information from the SESD.
Test Unit Ready	00h	Used to test the operation state of a LUN.
Reject		Contains information and status about a failing unit.

Inquiry command

An SES application client can send an **Inquiry** command to obtain information about a switch in the fabric. The FCP_CDB format is shown in Table 22.

Table 22. Inquiry command format

Byte/Bit	7	6	5	4	3	2	1	0
0	Operation Code = 12h							
1	Reserved						CmdDt=0	EVPD=0
2	Page Code							

Table 22. Inquiry command format (continued)

Byte/Bit	7	6	5	4	3	2	1	0
3	Reserved							
4	Allocation Length							
5	Control = 0							

If the Enable Vital Product Data (EVPD) field is set to 0, the value of the page code must be 0. The SESD then returns the standard inquiry data as shown in Table 23. If the Page Code field is not 0 when both the EVPD and CmdDt are 0, the SESD returns a CHECK CONDITION status.

Table 23. Standard Inquiry data format

Byte/ Bit	7	6	5	4	3	2	1	0
0	Peripheral Qualifier = 0			Peripheral Device Type = 0Dh				
1	RMB=0	Reserved = 0						
2	ISO version = 0		ECMA version = 0			ANSI version = 3		
3	AERC=0	TrmTsk=0	NormACA=0	Reserved=0	Response data format = 2			
4	Additional Length = 31 (1Fh)							
5	Reserved							
6	Reserved	EncServ=1	VS = 0	MultiP=1	MChngr=0	ACKREQQ=0	Addr32=0	Addr16=0
7	RelAdr=0	WBus32=0	Wbus16=0	Sync=0	Linked=0	Trandis=0	CmdQue=0	VS=0
8-15	Vendor identification							
16 - 31	Product identification = (by default the value is FC Switch)							
32 - 35	Product revision level = v{N}{m}{p} where {N} is a single number designating the major release number, {m} is a single number designating the minor release number, and {p} is a single alpha character designating a patch. There might be a space indicating that there is no patch. For example, v2.2.							

If the switch does not have the SES license key installed, the following values are returned:

- Peripheral Device Type = 1Fh (for unknown or no device type)
- EncServ = 0

If EVPD is set to 1, then the value of the Page Code can be set to one of the following:

- Page Code 00h (Supported Vital Product Data pages)
- Page Code 80h (Unit Serial Number Page)
- Page Code 83h (Device Identification Page)

If the Page Code is set to 00h, the SESD returns the following, as shown in Table 24.

Table 24. Supported Vital Product Data pages

Byte/Bit	7	6	5	4	3	2	1	0
0	Peripheral Qualifier = 0			Peripheral Device Type = 0Dh (for Enclosure services device)				

Table 24. Supported Vital Product Data pages (continued)

Byte/Bit	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
1	Page Code = 00h							
2	Reserved							
3	Page length = 3							
4	00h							
5	80h							
6	83h							

If the Page Code is set to 80h, the SESD returns the following, as shown in Table 25.

Table 25. Unit Serial Number page

Byte/Bit	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
0	Peripheral Qualifier = 0			Peripheral Device Type = 0Dh				
1	Page Code = 80h							
2	Reserved							
3	Page length = 24							
4	Product Serial Number = the WWN of the switch in ASCII string format For example, 10:00:00:60:69:00:01:b4							
...								
27								

If the Page Code is set to 83h, the SESD returns the following, as shown in Table 26.

Table 26. Device Identification page

Byte/Bit	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
0	Peripheral Qualifier = 0			Peripheral Device Type = 0Dh				
1	Page Code = 83h							
2	Reserved							
3	Page length = 32							
4	Reserved = 0				Code set = 2			
5	Reserved = 0				Identifier type = 1			
6	Reserved = 0							
7	Identifier length = 28							
8								
...								
35								

Note: If the switch does not have the SES license key installed, the Peripheral Device Type is set to 1Fh in all three pages.

Report LUN command

An SES application client sends a **Report LUN** command to obtain the number of logical units in the fabric, as shown in Table 27 on page 219.

Table 27. Report LUN command format

Byte/Bit	7	6	5	4	3	2	1	0
0	Operation Code = A0h							
1 - 5	Reserved							
6 - 9	Allocation Length							
10	Reserved							
11	Control = 0							

The allocation length should be at least 16 bytes. If not, the SESD returns a CHECK CONDITION status.

The SESD reports the LUNs of associated switches with the format shown in Table 28.

Table 28. Reported LUNs format

Byte	Description
0 - 3	LUN list length (n-7) in unit of bytes
4 - 7	Reserved
8 - 15	0
..	..
(n-7) - n	LUN Lj

The LUN list length is 48, and the LUN list consists of 0, L0, L5, L6, L9 and L10.

Request Sense command

An SES application client sends a **Request Sense** command to obtain sense data. The FCP_CDB format is shown in Table 29.

Table 29. Request Sense command format

Byte/Bit	7	6	5	4	3	2	1	0
0	Operation Code = 03h							
1 - 3	Reserved							
4	Allocation length							
5	Control = 0							

The SESD returns a sense key of NO SENSE and an additional sense code of NO ADDITIONAL SENSE INFORMATION.

Test Unit Ready command

An SES application client sends a **Test Unit Ready** command to check if the logical unit is ready. The FCP_CDB format is shown in Table 30.

Table 30. Test Unit Ready command format

Byte/Bit	7	6	5	4	3	2	1	0
0	Operation Code = 00h							
1 - 4	Reserved							
5	Control = 0							

The SESD returns the status of GOOD or CHECK CONDITION with a sense key of NOT READY and an additional sense code of LOGICAL UNIT NOT READY.

Reject command

The SESD sends a reject status (CHECK CONDITION) in the FCP_SNS_INFO field of the FCP_RSP IU when any SES command that was previously sent in the FCP_CMND IU by the client fails. The FCP_SNS_LEN_VALID bit is turned on when the FCP_SNS_LEN field contains a valid length and the sense data such as the Sense Key (SK), Additional Sense Code (ASC), and Additional Sense Code Qualifier (ASCQ) is returned in the FCP_SNS_INFO field. Table 31 shows the format of the sense data that is returned.

Table 31. Sense data

Sense key	**ASC**	**ASCQ**	**Description**
SK_NOT_READY (02)	ASC_LUN_NOT_READY (04)	0	Logical unit not ready. Request of FCP_CMND or FCP_DATA to a remote switch failed.
	ASC_ENC_SVC_FAILED (35)	0	Enclosure Service failed. Not enough memory in a local switch for data that was returned by a remote switch.
	ASC_ENC_SVC_UNAVAIL (35)	2	Enclosure Service unavailable. Firmware download already in progress. Not enough memory in a local switch for data that was returned by a local switch.
	ASC_PARLIST_LEN_ERR (1A)	0	Incorrect parameter list length in a command descriptor block of FCP_CMND payload (Send Diag or Write Buffer).
	ASC_INVALID_CMDCODE (20)	0	Invalid or not supported command operation code in FCP_CDB.
	ASC_INVALID_FIELD_CDB (24)	0	Invalid field in FCP_CDB. For example, invalid bit combination or incorrect buffer ID, mode, buffer offset, parameter length, allocation length, or page code.
	ASC_LUN_NOT_SUPPORTED (25)	0	Logical unit not supported. Command issued to remote domain (= LUN) for commands that do not support remote requests. Domain is not part of this fabric or invalid LUN value in FCP_CDB.
	ASC_INVALID_FIELD_PARLIST (26)	2	Invalid field in parameter list. Invalid page code. For Receive Diag, PCV bit = 0 in FCP_CDB with no previous Send Diag command. For Send Diag, invalid page length in a specified page of FCP_DATA payload.
	ASC_INVALID_PARVALUE (26)	0	Invalid parameter value in a specified page of FCP_DATA payload for writable fields.
	ASC_ENC_SVC_FAILED (35)	0	Enclosure Service failed. FCP_DATA payload null.
	ASC_DATA_PHASE_ERR (4B)	0	FCP_DATA phase failed.

Table 31. Sense data (continued)

Sense key	ASC	ASCQ	Description
	ASC_DATA_NOT_AVAIL (82)	0	Requested supportShow data not available yet.
SK_VENDOR_SPECIFIC (09)	ASC_ENC_SVC_FAILED (35)	0	Enclosure Service failed. Failed to get event information from switch for Event table.
SK_ABORTED_COMMAND (0B)	ASC_PARLIST_LEN_ERR (1A)	0	Parameter list length error. Firmware image too large or too small. FCP_CDB parameter list length not equal to FCP_DATA payload size (Send Diag or Write Buffer).
	ASC_LUNCOMM_TIME_OUT (08)	1	Logical unit communication timeout. R_A_TOV timeout occurred for firmware download. Requested supportShow data discarded due to a timeout.
	ASC_INVALID_DATA (26)	5	Firmware header data invalid or not for this switch model.
	ASC_CSUM_ERR (80)	0	Firmware checksum error.
	ASC_INTERNAL_ERR (81)	0	Switch internal error. Writing to flash failed.

Extended SES commands

Table 32 shows the extended SES commands that are supported by SESD. Extended SES commands require a license key to activate. Without a license key installed, only the basic SES commands are supported.

Table 32. Supported operation codes for extended SES commands

Command	Operation code	Description
Read Buffer	3Ch	Used to upload diagnostic or configuration data for the SESD.
Receive Diagnostic Results	1Ch	Contains information that is returned by the SESD about an enclosure.
Send Diagnostic	1Dh	Used to configure or diagnose a logical unit.
Write Buffer	3Bh	Used to download firmware or configuration data for the SESD.

Read Buffer command

This command enables an SES application client to upload configuration data or switch information from the SESD for debugging purposes. The FCP_CDB format is shown in Table 33.

Table 33. Read Buffer command format

Byte/Bit	7	6	5	4	3	2	1	0
0	Operation Code = 3Ch							
1	Reserved				Mode			
2	Buffer I D							

Table 33. Read Buffer command format (continued)

Byte/Bit	7	6	5	4	3	2	1	0
3 - 5	Buffer Offset							
6 - 8	Allocation Length							
9	Control = 0							

The Buffer IDs are defined as follows:

- 0x00h **-** upload switch information, equivalent to the **supportShow** command.
- 0x01h **-** upload configuration data, equivalent to the **configUpload** command.

The **Read Buffer** command is not distributed throughout a fabric. The SESD only responds with information on locally-attached SES clients. If the command is addressed to a remote switch, a CHECK CONDITION status is returned to the client (KEY/ASC=05/25, ILLEGAL REQUEST with LOGICAL UNIT NOT SUPPORTED).

Upload switch information: Buffer ID 0x00h is intended to upload switch information similar to the **supportShow** command. For detailed information about this command, see the *IBM TotalStorage SAN Fibre Channel Switch 3534 Model F08 Command Reference*.

When you run multiple **Read Buffer** commands, the Mode field should be set to 0010b, except in the first command. The Mode field in the first command should be set to 0000b. For the first **Read Buffer** command (where the Mode is 0000b), a 4-byte Read Buffer header is returned to the application client. The Buffer Capacity field of the header indicates the total size of the requested information that is available in the SESD. The maximum size of Buffer Capacity is 320K. Buffer Offset and Allocation Length of the command descriptor block is ignored for this mode. Table 34 shows upload switch information.

Table 34. Upload switch information

Byte/Bit	7	6	5	4	3	2	1	0
0	Reserved							
1	Buffer Capacity							
2								
3								

The Buffer Offset starts at 0 in the second command of multiple **Read Buffer** commands, assuming that the first command was already issued and that the client knows how much data the SESD has to upload. The subsequent value of the Buffer Offset field is the previous Buffer Offset plus the previous Allocation Length. The Allocation List Length for all transfers except the last is 32K. For example, the second **Read Buffer** command can contain Buffer Offset = 0 with Allocation Length = 32K and the third command can contain Buffer Offset = 32K with Allocation Length = 32K (with the Mode being 0010b). In the last command, the Allocation Length can be less than 32K.

The application client is responsible for keeping track of offsets and allocation length in order to obtain valid switch information from the SESD. The SESD does not record how much data it returned to the client in the previous commands. It only validates that the offset is a multiple of 32K and that the Mode is 0010b.

If the command contains illegal or invalid fields in the command descriptor block, a CHECK CONDITION status is returned to the client (KEY/ASC=05/24, ILLEGAL REQUEST with INVALID FIELD IN CDB). The client can then resend the command with legal fields.

After receiving the first **Read Buffer** command, the SESD can take about 20 seconds to collect and store requested switch information in a pre-allocated volatile memory before it sends a status to the requesting client. The client application should wait for a GOOD status before sending subsequent **Read Buffer** commands. The SESD keeps the requested data for 40 seconds. The client must obtain the entire data with subsequent **Read Buffer** commands within this time frame. This timeout is necessary in order to free up the allocated memory at the SESD side for efficiency.

If a timeout error occurs while the client is obtaining data, the client receives a Reject error with the sense key of 0Bh, Aborted Command. The client should then restart by sending the very first **Read Buffer** command requesting Buffer Capacity. After timeout or any time the client sends the command before it received the capacity, a CHECK CONDITION status is returned to the client (KEY/ASC=05/82, ILLEGAL REQUEST with ASC_DATA_NOT_AVAIL).

Upload configuration data: Buffer ID 0x01h is intended to upload configuration data similar to the **configUpload** command. For detailed information about this command, see the *IBM TotalStorage SAN Fibre Channel Switch 3534 Model F08 Command Reference*.

One **Read Buffer** command with a maximum Allocation Length of 32K is sufficient to upload configuration data to the SESD. The Mode and Buffer Offset fields can be ignored.

If the allocation length is less than or equal to 32K, the SESD provides data up to the allocation length or the actual size of the configuration data, whichever is less.

If the command contains illegal or invalid fields in the command descriptor block, a CHECK CONDITION status is returned to the client (KEY/ASC=05/24, ILLEGAL REQUEST with INVALID FIELD IN CDB). The client then resends the command with valid fields.

Receive Diagnostic Results command

This command enables an SES application client to receive diagnostic or management data. The FCP_CDB format is shown in Table 35.

Table 35. Receive Diagnostic Results command format

Byte/Bit	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
0	Operation Code = 1Ch							
1	Reserved							PCV
2	Page Code							
3 - 4	Allocation Length							
5	Control = 0							

A Page Code Valid (PCV) bit of 0 indicates that the most recent **Send Diagnostic** command defines the data returned by this command. A value of 1 indicates that the Page Code field defines the data to be returned for this command. The page codes and formats are defined in “Diagnostic pages” on page 226.

Send Diagnostic command

This command enables an SES application client to configure or diagnose a logical unit. After the command is completed, the SES application client can send a **Receive Diagnostic Results** command to confirm the configuration or diagnostic changes made by the most recent **Send Diagnostic** command. Table 36 shows the FCP_CDB format of this command.

Table 36. Send Diagnostic command format

Byte/Bit	7	6	5	4	3	2	1	0
0	Operation Code = 1Dh							
1	Reserved			PF	Reserved	selfTest	DevOfL	UnitOfL
2	Reserved							
3 - 4	Parameter List Length (in bytes)							
5	Control = 0							

A Page Format (PF) bit of 1 specifies that the **Send Diagnostic** command parameters conform to the page structure as specified in SCSI-3 Primary Command (SPC), Revision 11a, X3T10/995D, working draft. A value of 0 specifies that all parameters are vendor-specific. The SESD only supports the vendor-specific page structures, therefore the PF bit should always be 0.

The selfTest, DevOfL and UnitOfL bits are ignored by the SESD.

The Parameter List Length field specifies the length, in bytes, of the parameter list that is transferred from the SES application client to the SESD. If the parameter list length is zero, it is not an error condition, but no data is transferred. The Parameter List Length should be equal to 4 plus the Page Length in the supported pages. Otherwise, the SESD returns a CHECK CONDITION status.

Three diagnostic pages are supported with the **Send Diagnostic** command:
- 80h Switch page
- 82h Fabric page
- 84h Fibre Channel Port Table page

All other page codes, including the Page Code=0x00h, cause a CHECK CONDITION status, as these three pages are the only ones that contain writable fields in the pages.

Write Buffer command

This command enables an SES application client to download firmware or configuration data to the SESD. The format of the FCP_CDB is shown in Table 37.

Table 37. Write Buffer command format

Bit/Byte	7	6	5	4	3	2	1	0
0	Operation Code = 3Bh							
1	Reserved				Mode			
2	Buffer ID							
3 - 5	Buffer Offset							
6 - 8	Parameter List Length							
9	Control = 0							

The Buffer IDs are defined as follows:

- 0x00h - download firmware, equivalent to the **firmwareDownload** command
- 0x01h - download configuration data, equivalent to the **configDownload** command

The **Write Buffer** command is not distributed throughout a fabric. The SESD only responds to the locally-attached SES clients with respect to firmware or configuration data download. If the command is addressed to one of the remote switches, a CHECK CONDITION status is returned to the client (KEY/ASC = 05/25, ILLEGAL REQUEST with LOGICAL UNIT NOT SUPPORTED).

Only one SES client can download firmware or configuration data at a time. An SES client with multiple fibre-channel host bus adapters (HBAs) is considered to be multiple clients, as each HBA has its own S_ID in the fibre-channel frame headers. An SES client can initiate only one instance of download.

The **Write Buffer** command can be issued at any time to initiate downloading firmware or configuration data. There is no required state of the SESD before downloading starts.

Download firmware: The download firmware Buffer ID (0x00h) is equivalent to the **firmwareDownload** command. For detailed information about this command, see the *IBM TotalStorage SAN Fibre Channel Switch 3534 Model F08 Command Reference*.

In multiple **Write Buffer** commands to download firmware, the Mode field is always 0110b except in the last command. The Mode field in the last command is 0111b.

The Buffer Offset starts at 0 in the first command in multiple **Write Buffer** commands. The subsequent value of the Buffer Offset field is the previous Buffer Offset plus the previous Parameter List Length. The current Parameter List Length for all transfers except the last frame is 32 768 bytes (32K).

For example, the first transfer contains Buffer Offset = 0 with Parameter List Length = 32K, and the second transfer contains Buffer Offset = 32K with Parameter List Length = 32K. In last transfer the Mode should be 0111b and the Parameter List Length could be less than 32K.

In multiple Write Buffer transfers, if the subsequent **Write Buffer** commands contain illegal or invalid fields in the command block, any data that is received up to that point is discarded by the SESD and a CHECK CONDITION status is returned to the client (KEY/ASC=05/24, ILLEGAL REQUEST with INVALID FIELD IN CDB). The client then starts transferring data from the beginning.

A timeout (R_A_TOV) value of 10 seconds is used between each data transfer. If the next data is not received within R_A_TOV, all the previously received data is discarded and the client must transfer the firmware again.

The SESD allocates a flash block size of volatile memory buffer (currently 128K) at a time to save the received data from the SES client. When this buffer becomes full, the SESD writes the buffer content to the corresponding block of flash memory and the buffer is reinitialized. After writing the last block, the SESD immediately reads back the entire firmware from the first flash in order to verify the checksum. Upon the successful checksum verification, the SESD continues to write the same firmware image to the second flash, if the flash exists.

If the checksum is not valid, the firmware download process fails and the client receives a Reject message with a sense key of 0Bh, Aborted Command. The client then restarts the firmware download process. If the second flash does not exist and the checksum verification fails, the flash image remains damaged and will not restart until a good image of the firmware is successfully downloaded.

During the last FCP_CMND sequence, the client receives a good FCP_RSP before the SESD completes writing to the flash memory. This avoids any unnecessary timeouts at the FCP driver level due to a lengthy operation of writing to flash.

You can restart either by a power recycle or by the Switch_Administrative_Status field of the Switch Page (80h) in the **Send Diagnostic** command (1Dh).

Note: IBM recommends that the SESD be quiescent before restarting.

Download configuration data: The download configuration data Buffer ID (0x01h) is intended to download configuration data, which is equivalent to the **configDownload** command. For detailed information about this command, see the *IBM TotalStorage SAN Fibre Channel Switch 3534 Model F08 Command Reference*.

One **Write Buffer** command with a maximum Parameter List Length of 32 768 bytes (32K) is sufficient to download configuration data to the SESD, so the Mode and Buffer Offset fields are ignored.

The Parameter List Length must be less than or equal to 32K. If the command contains illegal or invalid fields in the command block, a CHECK CONDITION status is returned to the client (KEY/ ASC=05/24, ILLEGAL REQUEST with INVALID FIELD IN CDB). The client then resends the command with valid fields.

As soon as the SESD receives data successfully, it returns a GOOD status to the client and immediately disables itself so that it can parse the received data and write valid configuration changes to the configuration database in the switch. If data is invalid, the configuration of the database remains unchanged. When the client receives a GOOD status from the SESD, the client must login to the SESD again (that is, FLOGI or PLOGI) to communicate with effective parameters and continue its operations. When the client logs in again, it is especially important that fabric settings such as E_D_TOV or BB credit are changed. The client can use the **Read Buffer** command to read the configuration back to the database to verify changes.

The configuration data is in ASCII text file format and might have been generated using the Telnet **configUpload** command or the SES **Read Buffer** command with Buffer ID = 0x01h. You can also create the file if specific configuration data needs to be changed. In this case, use extreme care because inadvertent changes to configuration data might cause malfunctioning of the SESD during the next restart. Consult with your IBM representative before making any changes to the saved configuration data.

Diagnostic pages

Table 38 on page 227 shows a list of supported vendor-specific diagnostic pages. They are particularly relevant to two SES commands:

- Receive Diagnostic Results
- Send Diagnostics

Table 38. Diagnostic page summary

Diagnostic page	Page code	Description
Supported diagnostics pages	00h	Contains a list of the diagnostic pages that are supported.
Switch page	80h	Contains status information about the switch, its operational state, and firmware.
Sensor Table page	81h	Contains status information about the state of all sensors in the switch.
Fabric page	82h	Contains information about the fabric, its neighbors, and its Domain_ID.
Neighborhood Table page	83h	Contains information about the neighbors of a switch in the fabric.
Fibre-channel Port Table page	84h	Contains information about the fibre-channel ports of a switch.
Name Server Local Table page	85h	Contains information about the SESD local name server.
Event Table page	86h	Contains a list of event messages that have been logged.
Port Error and Interrupt Statistics Table page	87h	Contains information about the port errors and interrupt statistics.
Fabric Inquiry Data page	8Ah	Contains information about fabric data.
MIB-II System Group page	90h	Contains information about the MIB-II system group.
Port Log Table page	B0h	Contains information about the port log.
Unicast Route Table page	B1h	Contains the unicast route table that is currently configured for the switch.

Table 39 shows the page codes 80h through 86h. These are vendor-specific pages and are roughly mapped from the switch management information base (MIB) definition for Fabric OS version 2.3.

Table 39. Switch MIB groups

Page Code	Switch MIB group
80h	System Group, variables 1 - 8, 20, 21
81h	System Group, Sensor Table
82h	Fabric Group, variables 1, 2, and 8
83h	Fabric Group, Neighborhood Table
84h	Fibre-Channel Port Table
85h	Name Server Local Table
86h	Event Table page

Byte 0 - 3 of the diagnostics pages contain the Reserved byte. Byte 3 and 4 contain the Page Length. Byte 5 through the end of the page are called swValidity (or swvalidity [i] in cases where there are multiple entries to a table). The field is used to indicate which subsequent data fields are valid. Each subsequent data field has an associated field number. If the data field is valid, the associated bit in swValidity is set. In most cases, all data fields are valid in the response to the **Receive**

Diagnostic Results command. For example, if data fields 0, 1 and 2 are valid, then the related swValidity field contains the value 7. This is also a flexible mechanism for the **Send Diagnostic** command to indicate which data fields the client writes to.

Supported diagnostics pages

The following structure is used for the supported diagnostics pages of the **Receive Diagnostic Results** command. If requested using the **Receive Diagnostic Results** command, the SESD returns the response shown in Table 40.

Table 40. Page code 0 format

Byte	Description
0	
1	
2	
3	
4	00h
5	80h
6	81h
7	82h
8	83h
9	84h
10	85h
11	86h
12	87h
13	8Ah
14	90h
15	B0h
16	B1h

Switch page

The structure in Table 41 is used for the Switch page of the **Send Diagnostic** or **Receive Diagnostic Results** commands.

Table 41. Switch page format

Byte	Field number	Access	Description	Size
0	not available	read or write	Page Code = 80h	1
1	not available	not available	Reserved = 0	1
2 - 3	not available	read or write	Page Length = 404	2
4 - 7	not available	read or write	swValidity = 3FFh	4
8 - 71	0	read only	Current_Date (in ASCII text)	64
72 - 135	1	read only	Boot_Date (in ASCII text)	64

Table 41. Switch page format (continued)

Byte	Field number	Access	Description	Size
136 - 199	2	read only	Firmware_Last_Updated_Date (in ASCII text)	64
200 - 263	3	read only	FLASH_Last_Updated_Date (in ASCII text)	64
264 - 327	4	read only	Boot_PROM_Last_Updated_Date (in ASCII text)	64
328 - 391	5	read only	Firmware_Version_Information (in ASCII text)	64
392 - 395	6	read only	Switch_Operational_Status	4
396 - 399	7	read or write	Switch_Administrative_Status	4
400 - 403	8	read only	Diagnostics_Result	4
404 - 407	9	read only	Number_of_Sensors	4

Following is a description of the Switch page fields:

Current_Date
The current date and time. For example:

Wed Feb 10 15:04:28 1999.

Boot_Date
The start date and time.

Firmware_Last_Updated_Date
The last date and time that the Fabric OS was updated.

FLASH_Last_Updated_Date
The last date and time that the flash memory was updated.

Boot_PROM_Last_Updated_Date
The last date and time that the boot PROM was updated.

Firmware_Version_Information
Fabric OS version information. For example, v2.2.

Switch_Operational_Status
The current operational status to an external fibre-channel port. The valid values are:

Online
The switch is accessible.

Offline
The switch is not accessible.

Testing
The switch is in testing mode, is not accessible, and SESD is not available.

Faulty The switch is faulty, is not accessible, and SESD is not available.

Switch_Administrative_Status
The desired administrative status of the switch. An SES client can place the switch in a desired state by setting this field. The valid values are:

Online
The switch is accessible.

Offline
The switch is not accessible and SESD is not available.

Testing
The switch not accessible and SESD is not available.

Faulty The switch not accessible and SESD is not available.

Reboot
The switch restarts.

Fastboot
The switch performs a warm start (skipping POST).

Diagnostics_Result
The POST result. The valid values are:

OK
Central memory fault
Embedded port fault

Number_of_Sensors
The number of sensors in the switch.

Sensor Table page

If requested, using the **Receive Diagnostic Results** command, the SESD returns the response shown in Table 42.

Table 42. Sensor Table page format

Byte	Field number	Access	Description	Size
0	not available	read or write	Page Code = 81h	1
1	not available	not available	Reserved = 0	1
2 - 3	not available	read only	Page Length = n - 3	2
4 - 7	not available	read only	swNumEntries = i. Specifies the number of set entries received for bytes 8 - 91; if the number is 5 there are five sets of outputs for bytes 8 - 91.	4
8 - 11	not available	read only	swValidity[0] = 1Fh	4
12 - 15	0	read only	swSensorIndex[0]	4
16 - 19	1	read only	swSensorType[0]	4
20 - 23	2	read only	swSensorStatus[0]	4
24 - 27	3	read only	swSensorValue[0]	4
28 - 91	4	read only	swSensorInfo[0]	64
..	More instances of swSensorEntry (swValidity ..swSensorInfo) if applicable.			...
(n-63) - n	4	read only	swSensorInfo[i-1]	64

Following is a description of the Sensor Table page fields:

swSensorIndex
Identifies the sensor.

swSensorType
Identifies the sensor type. Valid values are:

Temperature
Fan
Power supply

swSensorStatus
The current status of the sensor. The valid values are:

Unknown
Faulty
Below-min
Nominal
Above-max
Absent

swSensorValue
The current value (reading) of the sensor. Value -2147483648 represents an unknown quantity indicating that the sensor does not have the capability to measure the actual value. The temperature sensor value is in degrees Celsius, the fan value is in revolutions per minute (RPM). The power supply sensor reading is a value of -2147483648 (unknown).

swSensorInfo
Additional information about the sensor. It contains the sensor type and number, in text format. For example, “Temp 3”, or “Fan 6”.

Fabric page

The structure in Table 43 is used for the Fabric page of the **Send Diagnostic** or **Receive Diagnostic Results** commands.

Table 43. Fabric page

Byte	Field number	Access	Description	Size
0	not available	read or write	Page Code = 82h	1
1	not available	not available	Reserved	1
2 - 3	not available	read or write	Page Length = 20	2
4 - 7	not available	read or write	swValidity = 7	4
8 - 11	0	read or write	swDomainID	4
12 - 15	1	read only	PrincipalSwitchFlag	4
16 - 19	2	read only	NumberOfImmediateNeighbor	4
20 - 23	3	read only	reserved	4

Following is a description of the Fabric page fields:

swDomainID
The current fibre-channel domain ID of the switch.

PrincipalSwitchFlag
Indicates whether the switch is the principal switch as per FC-SW. Valid values are:

1 yes

2 no

NumberOfImmediateNeighbor
The number of inter-switch links (ISLs) in the immediate neighborhood.

Neighborhood Table page

The structure in Table 44 is used for the Neighborhood Table page of the **Receive Diagnostic Results** command.

Table 44. Neighborhood Table page format

Byte	Field number	Access	Description	Size
0	not available	read or write	Page Code = 81h	1
1	not available	not available	Reserved = 0	1
2 - 3	not available	read only	Page Length = n - 3	2
4 - 7	not available	read only	swNumEntries = i. Specifies the number of set entries received for byte 8. Note that each entry consists of swValidity[0] field through swNbIslState[0] field.	4
8 - 11	not available	read only	swValidity[0] = 3Fh	4
12 - 15	0	read only	swNbIndex[0] = 1	4
16 - 19	1	read only	swNbMyPort[0]	4
20 - 23	2	read only	swNbRemoteDomain[0]	4
24 - 27	3	read only	swNbRemotePort[0]	4
28 - 91	4	read only	swNbBaudRate[0]	4
32 - 35	5	read only	swNbIslState[0]	4
..	More instances of swNbEntry (swValidity .. swNbIslState) if applicable.			...
(n-3) - n	0 - 5	read only	swNbIslState[i-1]	4

Note: The fabric-wide ISL table is not supported.

Following is a description of the Neighborhood Table page fields:

swNbIndex
Identifies the neighbor ISL entry.

swNbMyPort
The port index that has an ISL to another switch.

swNbRemoteDomain
The fibre-channel domain on the other end of the ISL.

swNbRemotePort
The port index on the other end of the ISL.

swNbBaudRate
The baud rate of the ISL (should be 16 for 1 gigabit).

swNbIslState
The current state of the ISL (should be 5 for active).

Fibre-channel Port Table page

The structure in Table 45 is used for the Fibre-channel Port Table page for the **Send Diagnostic** or **Receive Diagnostic Results** commands.

Table 45. Fibre-channel Port Table page format

Byte	Field number	Access	Description	Size
0	not available	read or write	Page Code = 84h	1
1	not available	not available	Reserved	1
2 - 3	not available	read or write	Page Length = n - 3	2
4 - 7	not available	read or write	swNumEntries = i. Specifies the number of set entries received. Note that each entry consists of swValidity[0] field through swFCPortLipLastAlpa field.	4
8 - 11	not available	read or write	swValidity[0] = FFFFFFFh	4
12 - 15	0	read only	swFCPortIndex[0]	4
16 - 19	1	read only	swFCPortType[0]	4
20 - 23	2	read only	swFCPortPhyState[0]	4
24 - 27	3	read only	swFCPortOpStatus[0]	4
28 - 31	4	read or write	swFCPortAdmStatus[0]	4
32 - 35	5	read only	swFCPortTxWords[0]	4
36 - 39	6	read only	swFCPortRxWords[0]	4
40 - 43	7	read only	swFCPortTxFrames[0]	4
44 - 47	8	read only	swFCPortRxFrames[0]	4
48 - 51	9	read only	swFCPortRxC2Frames[0]	4
52 - 55	10	read only	swFCPortRxC3Frames[0]	4
56 - 59	11	read only	swFCPortRxLCs[0]	4
60 - 63	12	read only	swFCPortRxMcasts[0]	4
64 - 67	13	read only	swFCPortTooManyRdys[0]	4
68 - 71	14	read only	swFCPortNoTxCredits[0]	4
72 - 75	15	read only	swFCPortRxEncInFrs[0]	4
76 - 79	16	read only	swFCPortRxCrcs[0]	4
80 - 83	17	read only	swFCPortRxTruncs[0]	4

Table 45. Fibre-channel Port Table page format (continued)

Byte	Field number	Access	Description	Size
84 - 87	18	read only	swFCPortRxTooLongs[0]	4
88 - 91	19	read only	swFCPortRxBadEofs[0]	4
92 - 95	20	read only	swFCPortRxEncOutFrs[0]	4
96 - 99	21	read only	swFCPortRxBadOs[0]	4
100 - 103	22	read only	swFCPortRxC3Discards[0]	4
104 - 107	23	read only	swFCPortMcastTimedouts[0]	4
108 - 111	24	read only	swFCPortTxMcasts[0]	4
112 - 115	25	read only	swFCPortLipIns[0]	4
116 - 119	26	read only	swFCPortLipOuts[0]	4
120 - 123	27	read only	swFCPortLipLastAlpa[0]	4
...	More instances of swFCPortEntry (swValidity - swFCPortLipLastAlpa) if applicable.			...
(n-3) - n	0 - 27	read only	swFCPortLipLastAlpa[i-1]	4

Following is a description of the Fibre-channel Port Table page fields:

swFCPortIndex
Identifies the switch port index. Note that the value of a port index is always one higher than the port number labeled on the front panel. For example, port index 1 correspond to port number 0.

swFCPortType
Identifies the type of switch port. It can be of type stitch(1), flannel(2), loom(3), or bloom(4).

swFCPortPhyState
Identifies the physical state of the port. The valid states are:

noCard(1)
No card is present in this switch slot.

noGbic(2)
No GBIC module is in this port.

laserFault(3)
The module is signaling a laser fault (defective GBIC).

noLight(4)
The module is not receiving light.

noSync(5)
The module is receiving light but is out of sync.

inSync(6)
The module is receiving light and is in sync.

portFault(7)
The port is marked faulty (defective GBIC, cable, or device).

diagFault(8)
The port failed diagnostics: defective G_port or FL_port card or system board.

lockRef(9)
The port is locking to the reference signal.

swFCPortOpStatus
Identifies the operational status of the port. The online(1) state indicates that user frames can be passed. The unknown(0) state indicates that it is likely that the port module is physically absent.

swFCPortAdmStatus
The desired state of the port. A management station can place the port in a desired state by setting this object accordingly. The testing(3) state indicates that no user frames can be passed. As the result of either explicit management action or per configuration information that is accessible by the switch, swFCPortAdmStatus is then changed to either the online(1) state, testing(3) state, or remains in the offline(2) state.

swFCPortTxWords
Counts the number of fibre-channel words that the port has transmitted.

swFCPortRxWords
Counts the number of fibre-channel words that the port has received.

swFCPortTxFrames
Counts the number of fibre-channel frames that the port has transmitted.

swFCPortRxFrames
Counts the number of fibre-channel frames that the port has received.

swFCPortRxC2Frames
Counts the number of Class 2 frames that the port has received.

swFCPortRxC3Frames
Counts the number of Class 3 frames that the port has received.

swFCPortRxLCs
Counts the number of link control frames that the port has received.

swFCPortRxMcasts
Counts the number of multicast frames that the port has received.

swFCPortTooManyRdys
Counts the number of times that readys (RDYs) exceed the frames received.

swFCPortNoTxCredits
Counts the number of times that the transmit credit has reached zero.

swFCPortRxEncInFrs
Counts the number of encoding errors or disparity errors that inside frames have received.

swFCPortRxCrcs
Counts the number of CRC errors detected for the frames received.

swFCPortRxTruncs
Counts the number of truncated frames that the port has received.

swFCPortRxTooLongs
Counts the number of received frames that are too long.

swFCPortRxBadEofs
Counts the number of received frames that have bad EOF delimiters.

swFCPortRxEncOutFrs
Counts the number of encoding errors or disparity errors outside frames received.

swFCPortRxBadOs
Counts the number of invalid ordered sets received.

swFCPortRxC3Discards
Counts the number of Class 3 frames that the port has discarded.

swFCPortMcastTimedouts
Counts the number of multicast frames that have been timed out.

swFCPortTxMcasts
Counts the number of multicast frames that have been transmitted.

swFCPortLipIns
Counts the number of loop initializations that have been initiated by loop devices attached.

swFCPortLipOuts
Counts the number of loop initializations that have been initiated by the port.

swFCPortLipLastAlpa
Indicates the physical address (AL_PA) of the loop device that initiated the last loop initialization.

Name Server Local Table page

If requested using the **Receive Diagnostic Result** command, the SESD returns the following response as shown in Table 46.

Table 46. Name Server Local Table page format

Byte	Field number	Access	Description	Size
0	not available	read or write	Page Code = 85h	1
1	not available	not available	Reserved	1
2 - 3	not available	not available	Page Length = n - 3	2
4 - 7	not available	not available	swNumEntries = i. Specifies the number of set entries received. Note that each entry consists of swValidity[0] field through swNsFc4Types[0] field.	4
8 - 11	na	read only	swValidity[0] = 7FFh	4
12 - 15	0	read only	swNsEntryIndex[0]	4
16 - 19	1	read only	swNsPortType[0]	4
20 - 23	2	read only	swNsPortID[0]	4
24 - 31	3	read only	swNsPortName[0]	8
32 - 287	4	read only	swNsPortSymb[0]	256
288 - 295	5	read only	swNsNodeName[0]	8
296 - 551	6	read only	swNsNodeSymb[0]	256
552 - 559	7	read only	swNsIPA[0]	8
560 - 575	8	read only	swNsIpAddress[0]	16
576 - 579	9	read only	swNsCos[0]	4
580 - 611	10	read only	swNsFc4[0]	32

Table 46. Name Server Local Table page format (continued)

Byte	Field number	Access	Description	Size
612 - 615	not available	read only	swValidity[1] - if applicable (n > 612)	4
......	More instances of swNsEntry as applicable.			...

Following is a description of the Name Server Local Table page fields:

swNsEntryIndex
Identifies the name server database entry. Valid values are:

0 unknown

1 N_port

2 NL_port

swNsPortType
Identifies the port type: N_port, NL_port, and so on, for this entry. The type is defined in FC-GS-2.

swNsPortID
Identifies the fibre-channel WWN of the port entry.

swNsPortName
Identifies the fibre channel WWN of the port entry.

swNsPortSymb
Identifies the symbolic name contents of the port entry. In FC-GS-2, a symbolic name consists of an array of 1 - 256 bytes. The first byte of the array specifies the length of its contents.

swNsNodeName
Identifies the fibre-channel WWN of the associated node as defined in FC-GS-2.

swNsNodeSymb
Identifies the symbolic name contents of the node that is associated with the entry. In FC-GS-2, a symbolic name consists of an array of 1 - 256 bytes. The first byte of the array specifies the length of its contents.

swNsIPA
Identifies the initial process associator (IPA) of the node for the entry, as defined in FC-GS-2.

swNsIpAddress
Identifies the IP address of the node for the entry, as defined in FC-GS-2. The address format is IPv6.

swNsCos
Identifies the class of services that are supported by the port. The value is a bitmap defined as follows:

bit 0 class F

bit 1 class 1

bit 2 class 2

bit 3 class 3

bit 4 class 4

swNsFc4
Identifies the FC-4s that are supported by the port, as defined in FC-GS-2.

Event Table page

If requested using the **Receive Diagnostic Results** command, the SESD returns the following response as shown in Table 47.

Table 47. Event Table page format

Byte	Field number	Access	Description	Size
0	not available	read or write	Page Code = 86h	1
1	not available	not available	Reserved	1
2 - 3	not available	not available	Page Length = n - 3	2
4 - 7	not available	not available	swNumEntries = i	4
8 - 11	not available	read only	swValidity[0] = 1Fh	4
12 - 15	0	read only	swEventIndex[0]	4
16 - 47	1	read only	swEventTimeInfo[0]	32
48 - 51	2	read only	swEventLevel[0]	4
52 - 55	3	read only	swEventRepeatCount[0]	4
56 - 311	4	read only	swEventDescr[0]	256
...	More instances of (swValidity .. swEventDescr) if applicable.			

Following is a description of the Event Table page fields:

swEventIndex
Identifies the event entry in the table.

swEventTimeInfo
Identifies the date and time when this particular event occurred, in text format.

swEventLevel
The level of severity associated with the event. Valid levels are:

1 critical

2 error

3 warning

4 informational

5 debug

swEventRepeatCount
Identifies how many times this particular event has occurred.

swEventDescr
Additional description of the event, in text format.

Port Error and Interrupt Statistics Table page

If requested using the **Receive Diagnostic Result** command, the SESD responds as shown in Table 48.

Table 48. Port Error and Interrupt Statistics Table page format

Byte	Field number	Access	Description	Size
0	not available	read or write	Page Code = 87h	1
1	not available	not available	Reserved	1
2 - 3	not available	not available	Page Length = n -3	2
4 - 7	not available	not available	swNumEntries = i	4
8 - 11	not available	read only	swValidity[0] = 7FF1FFFh	4
12 - 15	0	read only	swFCPortIndex[0]	4
16 - 19	1	read only	swFCPortLinkFailures[0]	4
20 - 23	2	read only	swFCPortSyncLosses[0]	4
24 - 27	3	read only	swFCPortSignalLosses[0]	4
28 - 31	4	read only	swFCPortPrimSeqProtoErrors[0]	4
32 - 35	5	read only	swFCPortInvalidTxWords[0]	4
36 - 39	6	read only	swFCPortInvalidCrcs[0]	4
40 - 43	7	read only	swFCPortDelimiterErrors[0]	4
44 - 47	8	read only	swFCPortAddressIdErrors[0]	4
48 - 51	9	read only	swFCPortLinkResetIns[0]	4
52 - 55	10	read only	swFCPortLinkResetOuts[0]	4
56 - 59	11	read only	swFCPortOlsIns[0]	4
60 - 63	12	read only	swFCPortOlsOuts[0]	4
64 - 67	13	read only	reserved	4
68 - 71	14	read only	reserved	4
72 - 75	15	read only	reserved	4
76 - 79	16	read only	TotalNumberOfInterrupts (sum of subsequent interrupts below)	4
80 - 83	17	read only	UnknownInterrupts	4
84 - 87	18	read only	LinkLevelInterrupts	4
88 - 91	19	read only	ProcessingRequiredInterrupts	4
92 - 95	20	read only	TimedoutInterrupts	4
96 - 99	21	read only	RxFlushedInterrupts	4
100 - 103	22	read only	TxUnavailableInterrupts	4
104 - 107	23	read only	FreeBufferInterrupts	4
108 - 111	24	read only	OverrunInterrupts	4
112 - 115	25	read only	Suspended_Interrupts	4
116 - 119	26	read only	ParityErrorInterrupts	4
120 - 123	27	read only	Reserved_last	4
...	More instances of (swValidity..reserved_last) if applicable.			

Following is a description of the Port Error and Interrupt Statistics Table page fields:

swFCPortIndex
The switch port index.

Note: The value of a port index is always one higher than the port number labeled on the front panel. For example, port index 1 correspond to port number 0.

swFCPortLinkFailures
The number of link failures.

swFCPortSyncLosses
Loss of synchronization.

swFCPortSignalLosses
Loss of signal (no light).

swFCPortPrimSeqProtoErrors
Protocol error.

swFCPortInvalidTxWords
Invalid word (encoding errors inside of frames).

swFCPortInvalidCrcs
Invalid CRC in a frame.

swFCPortDelimiterErrors
Delimeter error (order set).

swFCPortAddressIdErrors
Address ID error (SID, DID).

swFCPortLinkResetIns
Link reset in (primitive sequence). Does not apply to an FL_port.

swFCPortLinkResetOuts
Link reset out (primitive sequence). Does not apply to an FL_port.

swFCPortOlsIns
Offline resent in (primitive sequence). Does not apply to an FL_port.

swFCPortOlsOuts
Offline resent in (primitive sequence). Does not apply to an FL_port.

UnknownInterrupts
The number of interrupts that are not counted in all other categories.

LinkLevelInterrupts
The number of low-level interface (LLI) interrupts.

ProcessingRequiredInterrupts
The number of interrupts with processing (CPU) required.

TimedoutInterrupts
The number of timed-out interrupts.

RxFlushedInterrupts
The number of flushed transmissions.

TxUnavailableInterrupts
The number of interrupted transmissions.

FreeBufferInterrupts
The number of buffer interrupts.

OverrunInterrupts
The number of buffer overruns.

Suspended_Interrupts
The number of suspended interrupts.

ParityErrorInterrupts
The number of parity errors.

Fabric Inquiry Data page

If requested using the **Receive Diagnostic Results** command the SESD returns the response shown in Table 49.

Table 49. Fabric Inquiry Data page format

Byte	Field number	Access	Description	Size
0	not available	read or write	Page Code = 8Ah	1
1	not available	not available	Reserved	1
2 - 3	not available	not available	Page Length = n - 3	2
4 - 7	not available	read only	swValidity = FEFh	4
8 - 15	0	read only	switchWorld_wide_name	8
16 - 47	1	read only	switchName	32
48 - 51	2	read only	switchModelInfo	4
52 - 55	3	read only	firmwareVersion	4
56 - 119	4	read only	Reserved	64
120 - 123	5	read only	numberOfIpInterfaces = i	4
124 - 127	6	read only	interfaceType[0]	4
128 - 143	7	read only	interfaceName[0] - in ASCII format	16
144 - 159	8	read only	ipAddress[0] in IPv6 format	16
(n-15) - n	0 - 8	read only	ipAddress[i-1] in IPv6 format	16

Following is a description of the Fabric Inquiry Data page fields:

switchWorld_wide_name
The worldwide name of the switch. The format is as defined in the fibre channel standards.

switchName
The switch name in ASCII text, ending with a null character. This name is the same as the one that is displayed by the Telnet **switchName** command or the MIB-II variable *sysName*.

switchModelInfo
The first two bytes (byte 48 and 49) are reserved. The third byte (byte 50) represents the product model:

2 2109 S16

3 2109 S08

4 3534

5 2109 F16

The fourth byte (byte 51) represents the revision of the system board.

firmwareVersion
A 4-byte ASCII string of the format v{N}{m}{p}, where:

{N} is a single number designating the major firmware release number

{m} is a single number designating the minor release number

{p} is a single alpha character designating a patch; {p} can be a space indicating that there is no patch

An example of this value is v20. See the product revision level in the Fabric Inquiry Data page (Table 49 on page 241).

numberOfIpInterfaces
An integer that indicates the number of IP interfaces that are supported by the switch. This number is likely to be 2. This also indicates how many interface entries follow. Each interface entry contains the interface type, interface name, and its IP address.

interfaceType
A value that designates the type of network (IP) interface type as defined in RFC1213 - MIB-II. Note that the following enumerated values would apply:

ethernetCsmacd(6) – for the Ethernet interface.

fibreChannel(56) – for the fibre-channel interface.

interfaceName
A 16-byte ASCII text representing the name of the interface.

ipAddress
The IP address of the interface in IPv6 format.

MIB-II System Group page

If requested using the **Receive Diagnostic Result** command the SESD returns the response shown in Table 50. This page contains the System Group, SNMP MIB-II, as defined in the Internet Engineering Task Force (IETF) standard document, RFC 1213.

Table 50. MIB-II System Group page format

Byte	Field number	Access	Description	Size
0	not available	read or write	Page Code = 90h	1
1	not available	not available	Reserved	1
2 - 3	not available	not available	Page Length =1200	2
4 - 7	not available	read only	swValidity = 7Dh	4
8 - 263	0	read only	sysDescr	256
264 - 427	1	not available	Reserved for sysObjectID. It is not necessary to map this variable at present; note that bit 1 in validity is set to 0.	164
428 - 431	2	ro	sysUpTime	4

Table 50. MIB-II System Group page format (continued)

Byte	Field number	Access	Description	Size
432 - 687	3	ro	sysContact	256
688 - 943	4	ro	sysName	256
944 - 1199	5	ro	sysLocation	256
1200 - 1203	6	ro	sysServices	4

Following is a description of the MIB-II System Group page fields:

sysDescr
System (switch) description is also available as the Product Identification field of the standard Inquiry Data (see Table 23 on page 217). If sysDescr is more than 16 bytes long, then only the first 16 bytes are mapped to the Product Identification field. This information can be set with the Telnet **agtcfgSet** command or the SNMP-SET request. The factory default value is Fibre-Channel Switch.

sysUpTime
The time, in hundredths of a second, since the SNMP agent was started (at start time).

sysContact
The textual identification of the contact person for this managed switch, together with information about contacting this person. This information can be set with the Telnet **agtcfgSet** command or the SNMP-SET request. The factory default value is Field Support.

sysName
An administratively-assigned name for this switch. This information can be set with the Telnet **switchName** command or the SNMP-SET request.

sysLocation
The physical location of this switch. This information can be set with the Telnet **agtcfgSet** command or the SNMP-SET request. The factory default value is End User Premise.

sysServices
A value which indicates the set of network services that this switch firmware offers. Initially, the sum value is zero. For each network layer, L, in the range 1 - 7, that the fabric operating system performs a transaction for, 2 raised to (L-1) is added to the sum. In the context of the Internet suite of protocols, values should be calculated accordingly:

layer – functionality

1 physical

2 datalink or subnetwork

3 internet

4 end-to-end

7 applications

This value is set to 79. That is, layers 1, 2, 3, 4, and 7 are supported.

Port Log Table page

If requested using the **Receive Diagnostic Result** command the SESD returns the response shown in Table 51. To interpret the contents of this page, a UNIX utility, portlogDump, is provided.

Table 51. Port log table page format

Byte	Field number	Access	Description	Size
0	not available	read or write	Page Code = B0h	1
1	not available	not available	Reserved	1
2 - 3	not available	not available	Page Length = n - 3	2
An array of port log entries to follow, as applicable, where p = (n-3)/40				
4	0	read only	reserved[0]	1
5	1	read only	duplicate_count[0]	1
6	2	read only	portNumber[0]	1
7	3	read only	logType[0]	1
8 - 11	4	read only	argument0[0]	4
12 - 15	5	read only	argument1[0]	4
16 - 19	6	read only	argument2[0]	4
20 - 23	7	read only	argument3[0]	4
24 - 27	8	read only	taskID	4
28 - 31	9	read only	timeStamp_sec[0]	4
32 - 35	10	read only	timeStamp_nanoSec[0]	4
...	More instances of the above as applicable.			

Unicast Route Table page

If requested using the **Receive Diagnostic Result** command, the SESD returns the response shown in Table 52.

Table 52. Unicast Route Table page format

Byte	Field number	Access	Description	Size
0	not available	read or write	Page Code = B1h	1
1	not available	not available	Reserved	1
2 - 3	not available	not available	Page Length = n - 3	2
4 - 7	not available	not available	swNumEntries = i	4
8 - 11	not available	read only	swValidity[0] = 1FFh	4
12 - 15	0	read only	swEntryIndex[0]	1
16 - 19	1	read only	swInPortNum[0]	1
20 - 23	2	read only	swDestinationDomainID[0]	4
24 - 27	3	read only	swOutPortNum[0]	4
28 - 31	4	read only	swMetricCount[0]	4
32 - 35	5	read only	swHopCount[0]	4
36 - 39	6	read only	swFlags	4
40 - 43	7	read only	swNextDomainID	4

Table 52. Unicast Route Table page format (continued)

Byte	Field number	Access	Description	Size
44 - 47	8	read only	swNextOutPortNum	4
...	More instances of (swValidity .. swNextOutPortNum) if applicable.			

Following is a description of the Unicast Route Table page fields:

swEntryIndex
Identifies the event entry in the table.

swInPortNum
Identifies the incoming port number of the frame.

swDestinationDomainID
The destination domain of an incoming frame.

swOutPortNum
Identifies the outgoing port to which the frame is forwarded in order to reach the destination domain.

swMetricCount
The cost of reaching the destination domain.

swHopCount
The number of hops that are required to reach the destination domain.

swFlags
Indicates whether the route is dynamic (0) or static (1). A dynamic route is discovered automatically by fibre-channel shortest path first (FSPF) path selection protocol; a static route is assigned using the **uRouteConfig** command. A nonzero value when static indicates the bit position of the swInPortNum. For example, if swInPortNum = 3 for a static route, swFlags = 0x00 00 00 08.

swNextDomainID
The domain of the next hop that is connected to the outgoing port.

swNextOutPortNum
The port number of the next hop that is connected to the outgoing port.

SES troubleshooting

This section discusses the **Send Diagnostic** command error messages.

License reject

A license reject error message is generated when the SES license key is improperly entered or is not installed.

Note: When you install the license, you must surround the license key with double quotation marks.

Check condition

A check condition message is generated when the SESD ends an operation because an error was encountered. These error conditions can be invalid operations, warning indications, and failure conditions. The sense key and sense code describe the error. For more information, see Table 31 on page 220.

Chapter 9. ISL Trunking

This chapter provides the following information about interswitch link (ISL) trunking:

ISL Trunking overview

ISL Trunking is an optionally licensed product available on 3534 Model F08 and 2109 F series switches that are running Fabric OS version 3.0 or later. The 3534 1RU and 2109 S series switches require Fabric OS version 2.2 or later and do not support trunking. The 3534 1RU and 2109 series switches support ISL only. Trunking is managed using Telnet commands or the TotalStorage Specialist interface.

The ISL Trunking feature allows up to four inter-switch links (ISLs) to merge logically into a single link. An ISL is a connection between two switches through an expansion port (E_port). When using ISL Trunking to aggregate bandwidth of up to four ports, the speed of the ISLs between switches in a fabric is quadrupled. For example, at 2 Gbps speeds, trunking delivers ISL throughput of up to 8 Gbps.

ISL Trunking supports high-bandwidth, large-scale SANs which include core switches. The primary task of ISL Trunking is to route data and edge switches that aggregate connections to servers and storage. ISL Trunking simplifies network design and reduces the cost of storage management by optimizing bandwidth utilization and enabling load balancing of traffic at the frame level.

Advantages of ISL Trunking

The ISL Trunking feature has many advantages, for example, it ensures optimal ISL bandwidth use across trunked links, while preserving in-order delivery. ISL Trunking uses frame-level load balancing, as opposed to fibre-channel shortest path first (FSPF), to achieve faster fabric convergence, as well as higher availability in the fabric.

Routing without the ISL Trunking feature

Prior to ISL Trunking, device-level load sharing was done through fibre-channel networks that created ISLs and operated using the FSPF routing protocol. The FSPF routing protocol established and communicated the shortest paths for data to be carried from source to destination.

Although FSPF-compliant switches ensure fixed routing paths, and guarantee that all frames are delivered in order, congestion occurs if the aggregation of the stream exceeds the capacity of one of the ISLs in the path.

Routing with the ISL Trunking feature

ISL Trunking ensures that all links are used efficiently, eliminating congestion on one link while distributing the load of the links. This feature is designed to significantly reduce traffic congestion. The ISL Trunking feature distributes the workload across all the ISLs in a trunk. Each incoming frame is sent across the first available ISL. As a result, transient workload peaks for one system or application are much less likely to impact the performance of other parts of the SAN fabric. Because the full bandwidth of each physical link is available, the bandwidth is efficiently allocated.

Trunking groups, ports, and masters

At the frame level, ISL Trunking dynamically performs load balancing across a set of available links between two adjacent switches to establish a trunking group. Ports that belong to a trunking group are called *trunking ports*. One port is used to assign traffic for the group, and is referred to as the *trunking master*.

Trunking groups

A trunking group is identified by the trunking master that represents the entire group. The rest of the group members are referred to as *slave links*. Slave links help the trunking master direct traffic across ISLs, allowing efficient and balanced in-order communication.

Trunking ports

Trunking ports in a trunking group should meet the following criteria:

- Port must be configured as E_ports.
- Ports must reside in the same contiguous four-port groups. For example: 0-3, 4-7, 8-11, 12-15.
- Ports must run at 2 Gbps.
- The cable difference between all ports in a trunking group must be less than 500 m (164 ft).

Trunking masters

The trunking master implicitly defines the trunking group. All ports with the same trunking master are considered to be part of the same group. Each trunking group includes a single trunking master and several trunking slave links. The first ISL found in any trunking group is assigned to be the trunking master, also known as the principle ISL. After the trunking group is fully established, all data packets that are intended for transmission across the trunk are dynamically distributed at frame level across the ISLs in the trunking group, while preserving in-order delivery.

Installing ISL Trunking

Installing the ISL Trunking feature involves activating a license for each switch that you want to enable for trunking. A license might have been installed in the switch at the factory. If not, contact your switch supplier to obtain a license key.

The ISL Trunking feature requires a 3534 series switch with Fabric OS version 3.0. The ISL Trunking license can be installed using either Telnet or TotalStorage Specialist.

Installing ISL Trunking using Telnet

Perform the following steps to install ISL Trunking using Telnet:

1. Login to the switch through Telnet using an account that has administrative privileges. For example:

   ```
   Z:\/telnet account
   ```

   where `account` is replaced with the assigned account number.
2. To determine whether an ISL Trunking license is already installed on the switch, type `licenseShow` on the Telnet command line. A list of all the licenses that are currently installed on the switch displays. For example:

```
admin> licenseShow
1A1AaAaaaAAAA1a:
Release v3.0
Web license
Zoning license
SES license
```

If the Trunking license is included in the list, ISL Trunking is installed and is available. If the Trunking license is not included in the list or is incorrect, continue with steps 3 and 4.

3. Type the following on the command line:

   `licenseAdd "key"`

   where `"key"` is the license key that was provided to you, surrounded by double quotation marks. 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 license is not listed, repeat step 3.

5. Disable the switch by typing the following command:

   `switchDisable`

6. Enable the switch by typing the following command:

   `switchEnable`

Installing ISL Trunking using TotalStorage Specialist

Perform the following steps to install ISL Trunking using TotalStorage Specialist:

1. Launch the Web browser.
2. Type the switch name or IP address in the **Location/Address** field and press Enter.

   TotalStorage Specialist launches, displaying the Fabric view.

3. Click **Admin** on the relevant switch panel.

   The logon window displays.

4. Type a logon name and password with administrative privileges and press Enter.

   The Administration view displays.

5. Select the **License Admin** tab. Type the license key in the **License Key** field and click **Add License**.

   The ISL Trunking feature is available as soon as the license key is added.

6. Select the **Switch Settings** tab and disable the switch by selecting **Disable**.
7. Enable the switch by selecting **Switch Enable**.

Using ISL trunking

The ISL Trunking feature is managed by performing administration tasks. These tasks include enabling or disabling the trunking, enabling and disabling ports of a switch, setting the speed of a port, and debugging a trunking link failure.

The ISL Trunking feature is administered using Telnet commands or TotalStorage Specialist.

Administering ISL Trunking using Telnet commands

Table 53 shows the Telnet commands that are used to manage the ISL Trunking feature.

Table 53. ISL Trunking Telnet commands

Telnet command	Description	Example

portCfgTrunkport	Use this command to configure a port to be enabled or disabled for trunking.	To enable port 5 for ISL Trunking, type:
		`portCfgTrunkport 5, 1`
		To disable port 5 for ISL Trunking, type:
		`portCfgTrunkport 5, 0`

switchCfgTrunk	Use this command to enable or disable trunking on all ports of a switch.	To enable trunking on all ports of a switch, type:
		`switchCfgTrunk 1`
		To disable trunking on all ports of a switch, type:
		`switchCfgTrunk 0`

trunkDebug	Use this command to debug a trunk link failure.	To debug ports 1 and 2, type: `trunkDebug 1, 2`
trunkShow	Use this command to display ISL Trunking membership information.	To display ISL Trunking membership information about users, type: `trunkShow`

For detailed information about how to use these commands, see the *IBM TotalStorage SAN Fibre Channel Switch 3534 Model F08 Command Reference*.

Administering ISL Trunking using TotalStorage Specialist

You can use TotalStorage Specialist to view and modify ISL Trunking options through the **Trunk Information** tab and the **Port Settings** tab on the Switch Administration interface. For information about installing and using TotalStorage Specialist, see Chapter 3, “TotalStorage Specialist” on page 37.

You use the TotalStorage Specialist **Trunk Information** tab to view a summary of trunk groups and associated master and member ports. Table 54 lists the fields that are displayed from the **Trunk Information** tab.

Table 54. Trunk Information tab description

Trunk Information tab	Description
Trunk Group	A numerical number is displayed.
Master Port	The associated master port for the group is displayed.
Member Ports	The member ports that are associated with the group, separated by a comma, are displayed.

Table 55 lists the fields that are displayed and the tasks that you can perform using the **Port Setting** tab.

Table 55. Port Setting tab description

Port Setting tab	Description
Port Number	Each port is assigned a number. The port numbers are displayed under this heading.
Trunking Enable:Disable	Use this to enable or disable trunking on a per-port basis.
Port Enable:Disable	Use this to enable or disable a port.
Port Speed	Use this to set the speed of the port.

Frequently-asked questions about ISL Trunking

Following are some of the most frequently-asked questions about ISL Trunking.

Does ISL trunking replace dense wavelength digital multiplexing (DWDM)?
No. DWDM is a ring, and if a failure occurs it reroutes the allocated wavelength over alternate routes, and therefore changes the effective cable lengths.

What happens if an ISL in the trunk slave port fails?
If one of the trunk slave ports fails, the logical ISL stays up. However, its capacity is reduced by 2 Gbps, and no route failure or rerouting of traffic occurs.

What happens if a trunk master fails?
If a trunk master fails, the ISL goes down, and FSFP perceives a momentary route failure. The trunk immediately forms again without the failed ISL, and traffic resumes over the re-formed trunk with capacity reduced to 2 Gbps.

Are trunks automatically established when the trunking feature is enabled?
Yes. Trunks are automatically established on available ports when the trunking feature is enabled.

Is it possible to have more than one trunk between a pair of switches?
Yes.

Is there a limit to the number of trunks that I can have on one switch?
No.

Is there a limit to the number of trunks that I can have between a pair of switches?
No.

Is it possible to trunk between a switch and an edge devices host or storage?
No.

Should port statistics be the same across all participating ISLs within a trunk?
Not necessarily. It depends on the payload variations at the frame level. While optimal bandwidth utilization is the goal of the ISL Trunking feature, traffic might not be distributed exactly the same across all ISL links within a trunk.

Chapter 10. Zoning

This chapter contains general information about managing and monitoring a switch using zoning and includes the following topics:

Zoning overview

Zoning is an optionally licensed product that runs on 3534 Model F08 series switches. Zoning allows you to partition your SAN into logical groupings of devices that can access each other. Using zoning, you can arrange fabric-connected devices into logical groups, or *zones*, over the physical configuration of the fabric.

Zones can be configured dynamically. They can vary in size depending on the number of fabric-connected devices. Devices can belong to more than one zone. Because zone members can access only other members of the same zone, a device that is not included in a zone is not available to members of that zone.

You can use zones to:

Administer security
: Use zones to provide controlled access to fabric segments and to establish barriers between operating environments. For example, isolate systems with different uses or protect systems in a heterogeneous environment.

Customize environments
: Use zones to create logical subsets of the fabric to accommodate closed user groups or to create functional areas within the fabric. For example, include selected devices within a zone for the exclusive use of zone members, or create separate test or maintenance areas within the fabric.

Optimize IT resources
: Use zones to consolidate equipment, logically, for IT efficiency, or to facilitate time-sensitive functions. For example, create a temporary zone to back up non-member devices.

Figure 96 on page 254 shows three zones with some overlap. It also shows devices that are not assigned to a zone, and are thus not active in the fabric if zoning is enabled.

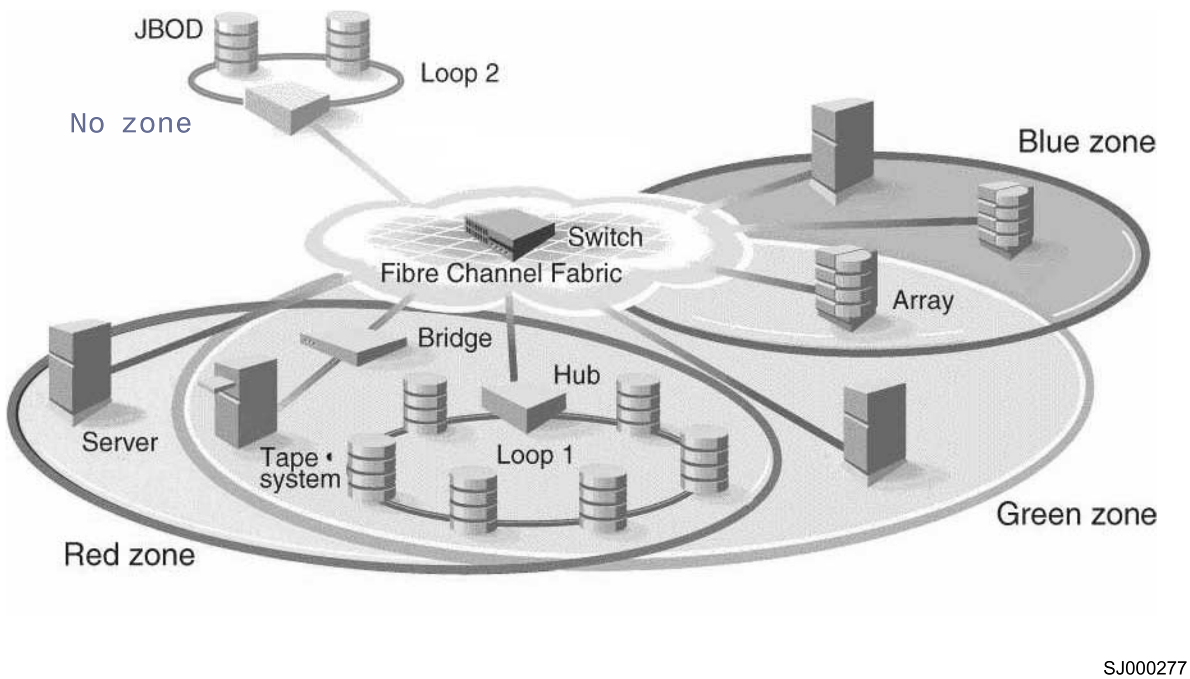


Figure 96. A fabric with three zones

Zoning concepts

Implementing zoning simplifies the zoning process in several ways.

- Zoning can be administered from any switch in the fabric.

  Changes that are configured to one switch automatically replicate to all switches in the fabric; if a new switch is added to an existing fabric, all zone characteristics are automatically applied to the new switch. Because each switch stores zoning information, zoning ensures a high level of reliability and redundancy.
- Zones can be configured dynamically.

  Configuring new zones does not interrupt traffic on unaffected ports or devices. And, they do not affect data traffic across inter-switch links (ISLs) in cascaded switch configurations.
- Zoning uses policy-based administration.

  Because zoning uses policy-based administration (separating zone specification from zone enforcement) you can manage multiple zone configurations and easily enable a specific configuration when it is required. A fabric can store any number of zone configurations; however, only one configuration is active at a time. But, because the configurations are predetermined and stored, a new configuration can be easily enabled.
- Zoning can be configured and administered using Telnet commands or TotalStorage Specialist. For information about zoning Telnet commands, see “Zoning Telnet commands” on page 264. For information about TotalStorage Specialist, see Chapter 3, “TotalStorage Specialist” on page 37.

Using and managing zoning

This section explains zoning in more detail and discusses how to use zoning to partition a fabric into logical groupings of devices.

A zone is a group of fabric-connected devices that are arranged into a specified grouping. Any device that is connected to a fabric can be included in one or more zones. Devices within a zone possess an awareness of other devices within the same zone; they are not aware of devices outside of their zone. Therefore, if zoning is enabled, any device not in a zone is not able to communicate with any other device.

Zone members (ports, WWNs, or aliases) are grouped into a zone; in turn, zones are grouped in a zone configuration (a collection of zones). Zones can overlap; a device can belong to more than one zone and a fabric can consist of multiple zones. A zone configuration can include both hard and soft zones. There can be any number of zone configurations resident on a switch; however, only one configuration can be active (enabled) at a time. Because the number of allowable zones is limited only by memory usage, the maximum number is virtually limitless.

Zone types

There are three types of zones:

Port level zone
A zone containing members that are specified by switch ports (domain ID, port number) only. Port level zoning is hardware enforced in the IBM 3534 and 2109 S series of switches and later models.

WWN zone
A zone containing members that are specified by device WWN only. WWN zones are hardware enforced in the 3534 and 2109 F series of switches and later models.

Mixed zone
A zone containing some members that are specified by WWN and some members that are specified by switch port. Mixed zones are software enforced through the fabric name server.

Zones can be hard (hardware enforced), soft (advisory), or Broadcast. In a hardware enforced zone, zone members can be specified by physical port number or through WWN, but not within the same zone. A software enforced zone is created when a port member and WWN member are in the same zone.

Hardware enforced zones
In a hardware enforced zone, all zone members can be specified as switch ports or WWN. Any number of ports or WWNs in the fabric can be configured to the zone. When a zone member is specified by port number or WWN, the individual device port or WWN is included in the zone. Hard zones are not necessarily position independent anymore. If WWNs are used exclusively in a zone, new devices can be attached without regard to physical location.

In hardware enforced zones, switch hardware ensures that there is no data transferred between unauthorized zone members. However, devices can transfer data between ports within the same zone. Consequently, hard zoning provides security.

Software enforced zones

In a software enforced zone, at least one zone member is specified by WWN, and one member is specified as a port. In this way, you have a mixed zone that is software enforced. When a device logs in, it queries the name server for devices within the fabric. If zoning is in effect, only the devices in the same zones are returned. Other devices are hidden from the name server query reply. When a mixed zone of WWNs and ports are specified, all ports on the specified device are included in the zone.

Software enforced zones are created when a combination of WWNs and ports are used. When using software enforced zones, the switch does not control data transfer, and there is no guarantee of data being transferred from unauthorized zone members. Use software zoning where flexibility and security is ensured by the cooperating hosts.

Broadcast zone

Only one broadcast zone can exist within a fabric. It is named broadcast and is used to specify those nodes that are to receive broadcast traffic. This type of zone is hardware enforced; the switch controls data transfer to a port.

Enforcing a zone

Zones can be enforced in hardware through access control lists on the switch ASIC (default) or by the fabric name server.

When zoning is disabled, the fabric is in nonzoning state and devices can communicate without regard to zone restrictions. When zoning is enabled, zoning is enforced throughout the fabric and devices can communicate only within their zones.

A switch can maintain any number of zone configurations; however, only one zone configuration can be enabled, or enforced, at a time. Because multiple configurations reside in the switch, you can switch from one configuration to another as needed. For example, you can set up a prespecified zone configuration to be enabled at certain times of the day; or, in the event of a disaster, you can quickly enable a defined configuration to implement your disaster policy.

Zone configurations can be:

Defined

This is the complete set of all zone objects that are defined in the fabric. When zone objects are defined, the information initially resides on RAM. The information must be saved to ensure that it is saved to flash memory and is not lost during power down or when a new zone configuration is enabled.

Changes are replicated to all switches in the fabric whenever the zone information is changed. However, changes must be saved to flash memory to be committed to persistent store (that is, to remain across restart).

Enabled

This is the zone configuration that is enabled (active). It resides on RAM; it must be saved to ensure that it is not lost when a new configuration is enabled or during power down. Any changes are replicated to all switches in the fabric when the configuration is enabled or saved.

Saved This is the zone configuration that was last saved. It resides in flash memory and it is persistent.

In Figure 97, the defined and enabled configurations are saved to flash:

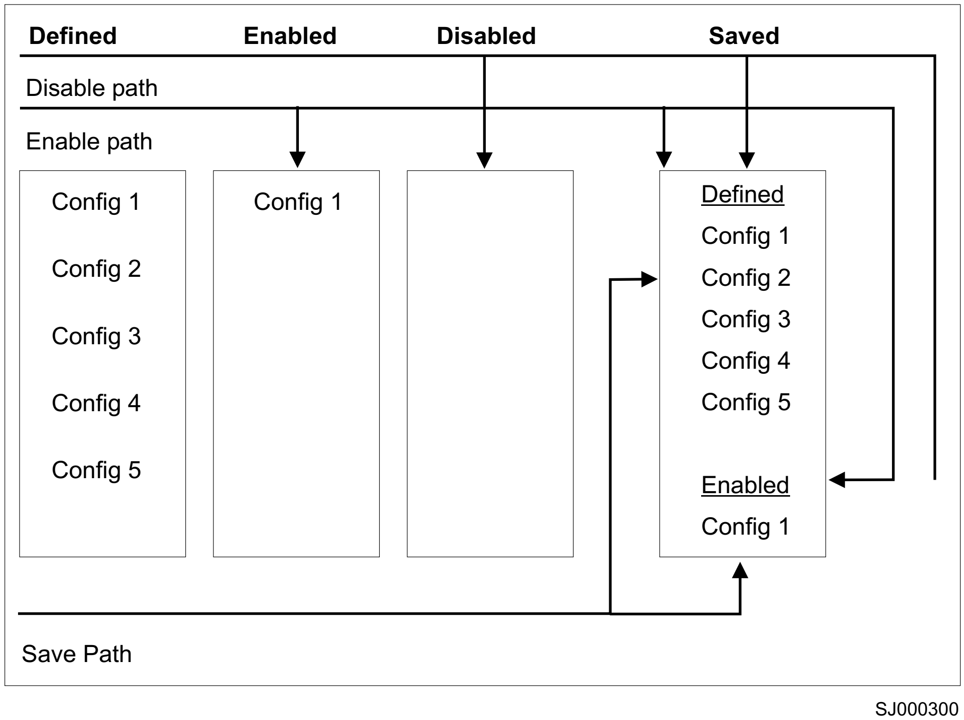


Figure 97. Saving a zone configuration

In Figure 98 on page 258, Config5 is defined (created). When it is defined, it resides only in RAM. To transfer it to flash memory, to be permanently stored and accessible across restarts, it must be saved. This can be accomplished in one of two ways:

- Save it directly to flash (the recommended method), or
- Enable it first, then save it to flash.

But, until it has been saved to flash, it is not permanently stored and available across restarts.

Note: Only the enabled configuration (in the shaded area) is enforced.

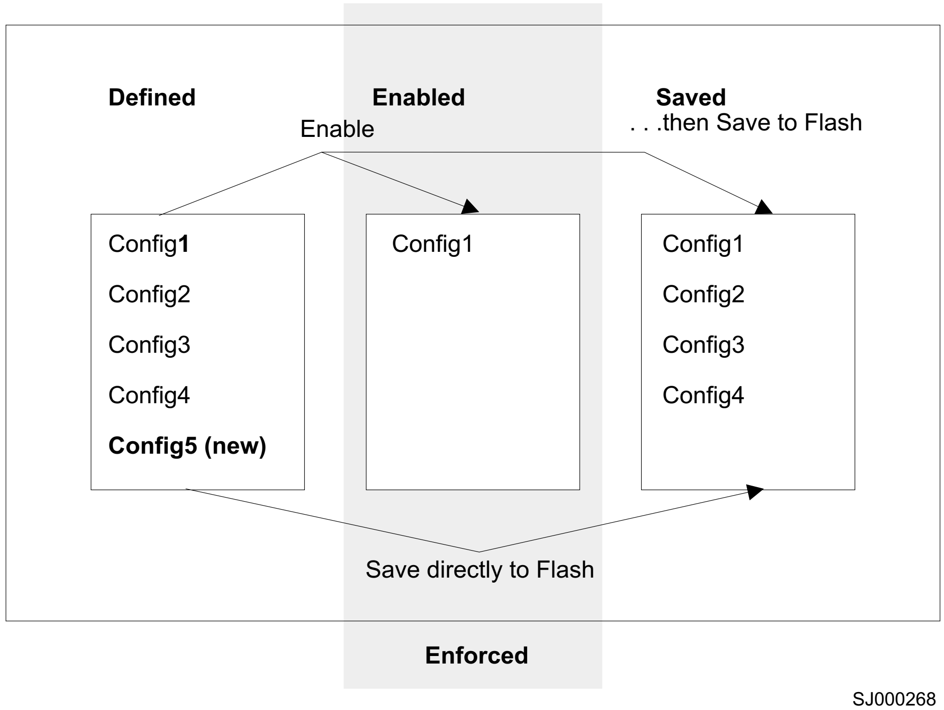


Figure 98. Saving a zone configuration

Enabling a zone configuration

When a zone configuration is enabled, all zones within the configuration are enabled. All devices within an enabled zone are visible to each other; however, they cannot communicate outside of their zone. Zones can overlap within a zone configuration.

When a zone configuration is enabled, the following happens:

1. All aliases are expanded.
2. Inconsistencies are checked.

   If any inconsistencies are discovered, an error occurs and the previous state of the fabric is preserved. (For example, if zoning was disabled, it remains disabled; if an existing configuration was enabled, it remains enabled.)
3. Switch hardware is loaded with the zoning information.
4. Zone members are loaded.
5. Registered state change notifications (RSCNs) are generated.

Implementing zoning

Zoning can be implemented and administered from any switch in the fabric. Changes that are made to one switch are automatically distributed to all switches in the fabric. For that reason, zoning requires that all switches in the fabric have an active zoning license.

Zoning can be administered either using Telnet or TotalStorage Specialist.

See the *IBM TotalStorage SAN Fibre Channel Switch 3534 Model F08 Command Reference* for the Telnet commands. See Chapter 3, "TotalStorage Specialist" on page 37 for information about TotalStorage Specialist.

Configuring zoning

Zoning is implemented by following these steps:

1. Create an alias (this step is optional).
2. Define the zone.
3. Define the zone configuration.
4. Enable the zone configuration.

Each zone object that is defined (alias, zone, zone configuration) must have a unique name; that is, an alias cannot have the same name as another alias, and it cannot have the same name as a zone or a zone configuration.

Note: During the following configuration process, changes should be saved periodically to ensure that they are stored in flash memory and protected against loss due to power outage.

Create an alias (optional)

An alias is a name that is assigned to a device or group of devices. By creating an alias you can assign a familiar name to a device, or you can group multiple devices into a single name. This can simplify cumbersome entries and it can allow an intuitive naming structure, such as using NT_Hosts to define all NT hosts in the fabric.

An alias must be a unique alphanumeric string beginning with an alphabetic character. The underscore character (_) is allowed and alias names are case sensitive. For example, nt_hosts is not the same name as NT_Hosts.

Aliases can greatly simplify the administrative process; however, they are not required to define zones.

Define the zone

A zone is a group of devices that can communicate with each other. Zone membership can include ports, WWNs, or aliases, or any combination of these. And, a device can be included in more than one zone.

To define a zone, specify the list of members to be included and assign a unique zone name; the zone name must be a unique alphanumeric string beginning with an alphabetic character. The underscore character (_) is allowed and zone names are case sensitive. For example, green_zone is not the same name as Green_Zone.

Specify zone members by port number, WWN, alias, or a combination of any of these.

To specify zone members by port number, you must specify the switch domain ID and port number. For example, 2,12 indicates switch domain ID 2, port number 12. When a zone member is specified by port number, all devices that are connected to the port are included in the zone.

To specify zone members by WWN, specify the node name or port or device as an 8-hex number separated by colons, for example, 10:00:00:60:69:00:8a. These eight numbers are compared to the node and port name presented in a login frame (FLOGI or PLOGI). When a zone member is specified by node name, all ports on the device are included in the zone. When a zone member is specified by port name, only that port on the device (node) is included in the zone.

To specify zone members by alias, specify the alias name.

Zone members can also be designated by a combination of these methods. For example, the following zone definition

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

contains any devices connected to switch 2, ports 12 and 14, the device with a node name or port name of 10:00:00:60:69:00:00:8a, as well as devices associated with the alias nt_hosts.

Define the zone configuration

A zone configuration is a group of zones that are enforced whenever that zone configuration is enabled. A zone can be included in more than one zone configuration.

To define a zone configuration, specify the list of zones to be included and assign a zone configuration name; the zone configuration name must be a unique alphanumeric string beginning with an alphabetic character. The underscore character (_) is allowed and zone names are case sensitive. For example, configuration1 is not the same name as Configuration1.

Enable the zone configuration

To enable a zone configuration, select the zone configuration to be enabled. The configuration is downloaded to the switch hardware. RSCNs are sent to all fabric devices that are registered for state changes. This notifies these devices to requery the name server to discover available devices that can be accessed.

Modifying configurations

To make changes to an existing configuration, either add or remove individual elements to create the desired configuration. After the changes have been made, save the configuration. This ensures that the configuration is permanently saved in the switch and it also ensures that the configuration is replicated throughout the fabric.

The switch configuration file can also be uploaded to the host for archiving and it can be downloaded from the host to all switches in the fabric.

Adding a switch

When a new switch is added to the fabric, it automatically takes on the zone configuration information from the fabric. To add the new switch, attach the E_ports and the new switch is incorporated into the fabric and the enabled zone configuration.

Merging fabrics

When a new fabric (with no zone configuration information) is added to an existing zoned fabric, all switches in the new fabric take on the zoning characteristics that are present in the existing fabric.

If two fabrics that both contain zone configuration information are joined, the fabrics attempt to merge the two sets of zone configuration data.

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

If the fabrics have different zone configuration data, the two sets of zone configuration data are merged if possible. If not possible, ISL is segmented. A merge is not possible if any of the following conditions exist:

Configuration mismatch
: Zoning is enabled in both fabrics and the zone configurations that are enabled are different in each fabric.

Type mismatch
: The name of a zone object in one fabric is used for a different type of zone object in the other fabric.

Content mismatch
: The definition of a zone object in one fabric is different from the definition of a zone object with the same name in the other fabric.

Transactional model

Zoning commands are run under the transactional model. A working copy of defined configurations is created by copying all information from zone or cfg lists at the start of a transaction.

The following commands are issued to open a transaction:

- cfgCreate
- cfgAdd
- cfgDelete
- cfgRemove

The following commands are issued to end a transaction:

- cfgSave
- cfgEnable
- cfgDisable

Using QuickLoop zones

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

Fabric zones and QuickLoop zones are independent of each other; both types of zones can coexist in the same zone configuration. QuickLoop devices can be included within a fabric zone configuration. However, while devices within a QuickLoop can be seen by a public host, devices within each QuickLoop are only visible to devices within their own QuickLoop.

In QuickLoop zoning, devices within a QuickLoop can be partitioned off within that QuickLoop to form QuickLoop zones; for example, a QuickLoop zone is a subset of a QuickLoop and can include only QuickLoop devices.

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

QuickLoop zone members are designated by looplet (port number), or by Arbitrated Loop Physical Address (AL_PA). There are 126 unique AL_PAs per QuickLoop; therefore, a QuickLoop zone can contain no more than 126 devices.

QuickLoop zoning advantages

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

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

Configuring QuickLoop zones

Perform the following steps to configure QuickLoop zoning:

1. Create a QuickLoop.

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

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

2. Define the QuickLoop zone.

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

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

   To create a QuickLoop zone, specify QuickLoop zone members by looplet, by AL_PA, or by combination of the two.

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

   ```
   "QLZoneName", "0,0; 0,1; 2,6; 2.7; 2,8"
   ```

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

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

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

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

3. Define the QuickLoop zone configuration.

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

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

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

Combining QuickLoop and zoning

QuickLoop can be used in conjunction with zoning.

In addition to zoning fabrics, zoning also allows you to zone QuickLoops, enhancing management of a Fibre Channel Arbitrated Loop (FC-AL) in a legacy environment.

In QuickLoop zoning, devices within a QuickLoop can be partitioned off within that QuickLoop to form QuickLoop zones; for example, a QuickLoop zone is a subset of QuickLoop and can include only devices in QuickLoop.

Fabric zones and QuickLoop zones are independent of each other; both types of zones can coexist in the same zone configuration. Hosts in a QuickLoop can only see targets contained within a QuickLoop.

Purchasing a zoning license adds the following features:

- Devices from multiple QuickLoops can be added to the definition for a fabric zone. Even an identical AL_PA from two different QuickLoops could be configured under a fabric zone. Zoning can correctly direct traffic to the different devices.
- Additional control over access to QuickLoop devices. Fabric devices in a zoned fabric can only access the QuickLoop (and fabric) devices that are in the same zone.
- Zones can be created within QuickLoops. Zoning can be used to partition QuickLoops. This creates QuickLoop zones (as opposed to fabric zones), whose members are identified by either physical port number or AL_PA.

Zoning Telnet commands

To use a Telnet command, log in with administrative privileges to any switch in the fabric, type the command with required operands, if any, and press Enter. Changes that are made to the zoning configuration on one switch are replicated through all switches within the fabric.

Note: When accessing the switch using simultaneous multiple connections (Telnet, TotalStorage Specialist) it is possible that a change resulting from one connection might not transfer to another connection. Also, it is possible that a change from one connection can overwrite a change from another connection. Therefore, use care when making changes using simultaneous connections.

Grouped by function, Table 56 shows the Telnet commands that are used to administer zoning. For more information on Zoning Telnet commands, see the *IBM TotalStorage SAN Fibre Channel Switch 3534 Model F08 Command Reference*.

Table 56. Zoning Telnet commands

Command	Description
Zone alias	
aliAdd	Add a member to a zone alias.
aliCreate	Create a zone alias.
aliDelete	Delete a zone alias.
aliRemove	Remove a member from a zone alias.
aliShow	Show the zone alias definition.
Zoning	
zoneAdd	Add a member to a zone.
zoneCreate	Create a zone.
zoneDelete	Delete a zone.
zoneRemove	Remove a member from a zone.
zoneShow	Show the zone information.
QuickLoop zoning	
qloopAdd	Add a member to a QuickLoop.
qloopCreate	Create a QuickLoop.
qloopDelete	Delete a QuickLoop.
qloopRemove	Remove a member from a QuickLoop.
qloopShow	Show the QuickLoop information.
Zone configuration	
cfgAdd	Add a zone to a zone configuration.
cfgCreate	Create a zone configuration.
cfgDelete	Delete a zone configuration.
cfgRemove	Remove a zone from a zone configuration.
cfgShow	Show the zone configuration definition.
Configuration management	
cfgClear	Clear all zone configurations.
cfgDisable	Disable a zone configuration.

Table 56. Zoning Telnet commands (continued)

Command	Description
cfgEnable	Enable a zone configuration.
cfgSave	Save a zone configuration in flash memory.
cfgShow	Show the zone configuration definition.

Appendix A. Error messages

This appendix explains the error message formats and possible errors, including:

System error message formats

There is only one error message format for the switch, whether you are gathering information from the local RS-232 serial port or using a remote Telnet session.

Errors are listed in reverse chronological order. Up to 64 messages can be held in the buffer. If the 64 message limit is exceeded, the oldest message is deleted to make room for the newest message.

The **errShow** command displays all detected errors. The output provides additional information that displays on the front panel. The following information is displayed by the **errShow** command:

- Task ID
- Task name
- Date and time of the error
- Number of occurrences
- Error type
- Error level
- A description of the error
- The error number (displayed for diagnostic errors)

Note: The error counter goes to a maximum of 999.

The display halts after each error is displayed, prompting you to either press Enter to continue or type a `Q` to quit. Continue pressing Enter until the prompt (=>) is displayed. In Figure 99 on page 268, Error 02 represents a system error and Error 01 represents a diagnostic error (error number #004). Only diagnostic errors are assigned error numbers.

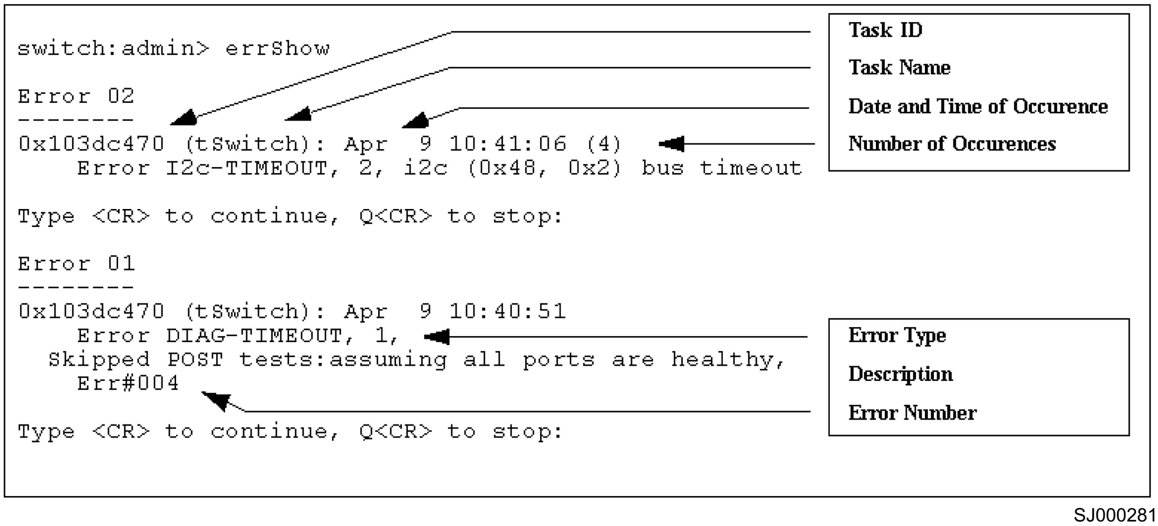


Figure 99. errShow command example

To display error messages using Telnet:

1. From the prompt, type `errShow`.
2. To scroll through the error list, type `CR`.
3. Scroll through error log (if no errors are encountered, the command returns `No Error`.

Diagnostic error message formats

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

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

Some messages contain the following abbreviations:

```
sb = Should Be
er = Bits in error
```

Note: If you run the **portStatsShow** or the **diagShow** command prior to running a test, errors might occur as a result of the normal synchronization process. These errors should be addressed if the number of errors that are found increases after running the **portStatsShow** command again.

Table 57 lists probable failure actions.

Table 57. Probable failure actions

Failed test	Action
ramTest (See Note)	Replace DRAM module or main board assembly
portRegTest (See Note)	Replace main board assembly
centralMemoryTest (See Note)	Replace main board assembly
cmiTest (See Note)	Replace main board assembly

Table 57. Probable failure actions (continued)

Failed test	Action
cmemRetentionTest	Replace main board assembly
sramRetentionTest	Replace main board assembly
camTest (See Note)	Replace main board assembly
portLoopbackTest (See Note)	Replace main board assembly
crossPortTest	Replace main board assembly, GBIC or fiber cable
spinSilk	Replace main board assembly, GBIC or fiber cable
Note: These tests are run during the POST. For more information about these tests, refer to the individual command description in the *IBM TotalStorage SAN Fibre Channel Switch 3534 Model F08 Command Reference*.	

Error message numbers

An error number ERR#xxxx is displayed at the end of a diagnostic error message. Table 58 matches each error number with the test that caused the error and the name of the error. Look up the complete definition of the error name and the actions that will correct it in “Diagnostic error messages” on page 272.

Table 58. Error message code defined

Error number	Test name	Error name
0001	not applicable	DIAG-CLEAR_ERR
0004	not applicable	DIAG-POST_SKIPPED
0B15	sramRetentionTest	DIAG-REGERR
0B16		DIAG-REGERR_UNRST
0B0F		DIAG-BUS_TIMEOUT
1F25	cmemRetentionTest	DIAG-LCMRS
1F26		DIAG-LCMTO
1F27		DIAG-LCMEM
0110	ramTest (See Note)	DIAG-MEMORY
0111		DIAG-MEMSZ
0112		DIAG-MEMNULL
0415	portRegTest (See Note)	DIAG-REGERR
0416		DIAG-REGERR_UNRST
040F		DIAG-BUS_TIMEOUT
1020	centralMemoryTest (See Note)	DIAG-CMBISRTO
1021		DIAG-CMBISRF
1025		DIAG-LCMRS
1026		DIAG-LCMTO
1027		DIAG-LCMEM
1028		DIAG-LCMEMTX
1029		DIAG-CMNOBUF
102A		DIAG-CMERRTYPE
102B		DIAG-CMERRPTN

Table 58. Error message code defined (continued)

Error number	Test name	Error name
102C		DIAG-INTNOTCLR
1030		DIAG-BADINT
106F		DIAG-TIMEOUT
2030	cmiTest (See Note)	DIAG-BADINT
2031		DIAG-INTNIL
2032		DIAG-CMISA1
2033		DIAG-CMINOCAP
2034		DIAG-CMIINVCAP
2035		DIAG-CMIDATA
2036		DIAG-CMICKSUM
223B	camTest (See Note)	DIAG-CAMINIT
223C		DIAG-CAMSID
2640	portLoopbackTest (See Note)	DIAG-ERRSTAT (ENCIN)
2641		DIAG-ERRSTAT (CRC)
2642		DIAG-ERRSTAT (TRUNC)
2643		DIAG-ERRSTAT (2LONG)
2644		DIAG-ERRSTAT (BADEOF)
2645		DIAG-ERRSTAT (ENCOUT)
2646		DIAG-ERRSTAT (BADORD)
2647		DIAG-ERRSTAT (DISCC3)
264F		DIAG-INIT
265F		DIAG-PORT_DIED
266E		DIAG-DATA
266F		DIAG-TIMEOUT
2660		DIAG-STATS(FTX)
2661		DIAG-STATS(FRX)
2662		DIAG-STATS(C3FRX)
2670		DIAG-PORTABSENT
2671		DIAG-XMIT
3040	crossPortTest	DIAG-ERRSTAT(ENCIN)
3041		DIAG-ERRSTAT(CRL)
3042		DIAG-ERRSTAT(TRUNC)
3043		DIAG-ERRSTAT(2LONG)
3044		DIAG-ERRSTAT(BADEOF)
3045		DIAG-ERRSTAT(ENCOUT)
3046		DIAG-ERRSTAT(BADORD)
3047		DIAG-ERRSTAT(DISC3)
304F		DIAG-INIT
305F		DIAG-PORTDIED

Table 58. Error message code defined (continued)

Error number	Test name	Error name
3060		DIAG-STATS (FTX)
3061		DIAG-STATS (FRX)
3062		DIAG-STATS (C3FRX)
306E		DIAG-DATA
306F		DIAG-TIMEOUT
3070		DIAG-PORTABSENT
3071		DIAG-XMIT
3078		DIAG-PORTWRONG
3080	spinSilk	DIAG-PORTM2M
3081		DIAG-NOSEGMENT
384F		DIAG-INIT
385F		DIAG-PORTDIED
3840		DIAG-ERRSTAT (ENCIN)
3841		DIAG-ERRSTAT (CRC)
3842		DIAG-ERRSTAT (TRUNC)
3843		DIAG-ERRSTAT (2LONG)
3844		DIAG-ERRSTAT (BADEOF)
3845		DIAG-ERRSTAT (ENCOUT)
3846		DIAG-ERRSTAT (BADORD)
3847		DIAG-ERRSTAT (DISCC3)
3870		DIAG-PORTABSENT
3871		DIAG-XMIT
3874		DIAG-PORTSTOPPED
3880		DIAG-PORTM2M
3881		DIAG-NOSEGMENT
Note: These tests are run during the POST. For more information about these tests, refer to the individual command descriptions in the *IBM TotalStorage SAN Fibre Channel Switch 3534 Model F08 Command Reference*.		

Repair action codes for diagnostic error messages

Table 59 lists the action codes and the recommended repair action for each action code.

Table 59. Action codes and recommended repair actions

Action code	Recommended action
1	Replace the 3534 Model F08 switch. **Note:** Switch replacement disrupts all switch traffic.
2	Further diagnostic action is required. Failure can be the switch, SFP, or cable. This is typically the result of running a wrap test. The tests should be run again after swapping cables, SFPs, and other components to determine the cause. It is unlikely that the switch is at fault, as most switch failures cause a POST failure.

Table 59. Action codes and recommended repair actions (continued)

Action code	Recommended action
3	Fan malfunction. Replace the switch.
4	Power supply malfunction. Replace the switch.

Diagnostic error messages

This section provides information about the probable cause of a diagnostic error and what actions to take. Table 60 shows the diagnostic error messages. For more information about the action code numbers, see Table 59 on page 271.

Table 60. Diagnostic error messages

Message	Failing test	Description	Probable cause	Action
DIAG-BADINT Err#1030 Err#2030	centralMemoryTest cmiTest	The port received an interrupt when not expecting one.	ASIC failure	1
DIAG-BUS_TIMEOUT Err#0B0F Err#4040F	portRegTest sramRetentionTest	The ASIC register or ASIC SRAM did not respond to an ASIC data access.	ASIC failure	1
DIAG-CAMINIT Err#223B	CamTest	The port failed to initialize due to one of the following reasons: • Switch is not disabled • Diagnostic queue absent • Malloc failed • Chip is not present • Port is not in loopback mode • Port is not active	Software operational setup error or main board failure	Retry, restart or replace the switch
DIAG-CAMSID Err#223C	camTest	The ASIC failed SID NO translation test.	ASIC failure	1
DIAG-CLEAR_ERR Err#0001		The diag error flag (OK or BAD) of the port is cleared.	Informational only	None required
DIAG-CMBISRF Err#1021	centralMemoryTest	The central memory SRAMs of the ASIC did not complete the built-in self-repair (BISR) within the timeout period.	ASIC failure	1
DIAG-CMBISRTO Err#1020	centralMemoryTest	The central memory SRAMs of the ASIC did not complete the BISR within the timeout period.	ASIC failure	1
DIAG-CMERRPTN Err#102B	centralMemoryTest	An error was detected at the wrong port.	ASIC failure	
DIAG-CMERRTYPE Err#102A	centralMemoryTest	The port got the wrong central memory (CMEM) error type.	ASIC failure	1
DIAG-CMICKSUM Err#2036	cmiTest	The CMI message that was received failed the 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

Table 60. Diagnostic error messages (continued)

Message	Failing test	Description	Probable cause	Action
DIAG-CMIINVCAP Err#2034	cmiTest	An unintended ASIC erroneously got CMI capture flag.	ASIC or system board failure	1
DIAG-CMINOCAP Err#2033	cmiTest	The CMI intended receiver ASIC failed to get the CMI capture flag.	ASIC or system board failure	1
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 Err#306E	portLoopbackTest crossPortTest	The payload that was received by the port did not match the payload that was transmitted.	System board, GBIC module, or fiber cable failure	2
DIAG-ERRSTAT Err#2640-2647 Err#3040-3047 Err#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, or fiber cable failure	2
DIAG-INIT Err#264F Err#304F Err#384F	portLoopbackTest crossPortTest spinSilk	The port failed to go active in the loopback mode requested.	ASIC, system board, GBIC module, or fiber cable failure	2
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	Data that was read from the central memory location did not match data that was previously written into the same location.	ASIC failure	1
DIAG-LCMEMTX Err#1F27 Err#1028	centralMemoryTest	A central memory transmit path failure: ASIC 1 failed to read ASIC 2 using the transmit path.	System board failure	1
DIAG-LCMRS Err#1F25 Err#1025	centralMemoryTest cmemRetentionTest	A central memory read short: M bytes requested but got less than M bytes.	ASIC failure	1

Table 60. Diagnostic error messages (continued)

Message	Failing test	Description	Probable cause	Action
DIAG-LCMTO Err#1F26 Err#1026	centralMemoryTest cmemRetentionTest	A 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	The memory size to be tested is less than or equal to zero.	System board failure	1
DIAG-MEMORY Err#0110	ramTest	Data that was read from the RAM location did not match data that was previously written into the same location.	CPU RAM failure	1
DIAG-NOSEGMENT Err#3081 Err#3881	crossPortTest spinSilk	The port failed to go into loopback mode.	Improper GBIC or cable connection	Reseat the GBICs and cables and rerun the test
DIAG-PORTABSENT Err#2670 Err#3070 Err#3870	portLoopbackTest crossPortTest spinSilk	The port is not present.	ASIC or system board failure	1
DIAG-PORTDIED Err#265F Err#305F Err#385F	portLoopbackTest crossPortTest spinSilk	The port was in loopback mode and then went inactive.	ASIC, GBIC module, or fiber cable failure	2
DIAG-PORTM2M Err#3080 Err#3880	crossPortTest spinSilk	The port is found to be connected to itself (self loopback). This port M to port M connection is not allowed by this test.	Improper cable connection	Reconnect port (M) to another port (N) and rerun the test
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, or fiber cable failure	2
DIAG-PORTWRONG Err#3078	crossPortTest	The frame was erroneously received by port M instead of the intended port N.	ASIC failure	1
DIAG-POST_SKIPPED Err# 0004	switch initialization	The POST is skipped. The message recommended that POST be performed.	Informational only	None required
DIAG-REGERR Err#0B15 Err#0415	portRegTest sramRetentionTest	Data that was read from the ASIC register or the ASIC SRAM did not match the data that was previously written into the same location.	ASIC failure	1
DIAG-REGERR_UNRST Err#0B16 Err#0416	portRegTest sramRetentionTest	The port failed to unreset.	ASIC failure	1

Table 60. Diagnostic error messages (continued)

Message	Failing test	Description	Probable cause	Action
DIAG-STATS Err#2660-2662 Err#3060-3062	portLoopback Test crossPortTest	The port counter value did not match the number of frames that were actually transmitted. Possible counters reporting are: • FramesTx - number of frames transmitted. • FramesRx - number of frames received. • Cl3FrmRx - number of class 3 frames received.	ASIC, GBIC module, or fiber cable failure	2
DIAG-TIMEOUT Err#266F Err#306F Err#386F	portLoopbackTest crossPortTest centralMemoryTest	For the **portLoopbackTest** and the **crossPortTest**: The port failed to receive frame within the timeout period. For the **centralMemoryTest**: The port failed to detect an interrupt within the timeout period.	ASIC, GBIC module, or fiber cable failure	2
DIAG-XMIT Err#2271 Err#2671 Err#3071 Err#3871	portLoopbackTest crossPortTest spinSilk camTest	The port failed to transmit frame.	ASIC failure	1

System error messages

This section provides information about the probable cause of a system error and what actions to take. Table 61 shows the system error messages.

Table 61. System error messages

Message	Description	Probable cause	Action
ASIC, MINI_BUFFER, LOG_WARNING	ASIC failure	Bad main board	Contact customer support
CONFIG CORRUPT	The switch configuration information has become irrevocably corrupted.	OS error	The system automatically reverts to the default configuration settings.
CONFIG OVERFLOW	The switch configuration information has grown too large to be saved or has an invalid size.	OS error	Contact customer support
CONFIG VERSION	The switch has encountered an unrecognized version of the switch configuration.	OS error	The system automatically reverts to the default configuration settings.
FABRIC, SEGMENTED, LOG_WARNING	The fabric segmented.	Incompatible fabric parameters and switches Conflict zones	Reconfigure fabric or zones. See the *IBM TotalStorage SAN Fibre Channel Switch 3534 Model F08 Command Reference*.

Table 61. System error messages (continued)

Message	Description	Probable cause	Action
FABRIC, BADILS, LOG_WARNING	Bad ISL-ELS size	The ISL-ELS payload is wrong.	Contact customer support
FABRIC, NO_ALIASID, LOG_WARNING	No free multicast alias	Too many multicast groups in use	Remove some of the groups
FANS, 1_FAILED, LOG_WARNING	Switch overheated	Fan failure	Contact customer support
FANS, 2_FAILED, LOG_ERROR	Switch overheated	Fan failure	Contact customer support
FANS, 3_FAILED, LOG_CRITICAL	Switch overheated	Fan failure	Contact customer support
FANS, 4_FAILED, LOG_CRITICAL	Switch overheated	Fan failure	Contact customer support
FANS, 5_FAILED, LOG_CRITICAL	Switch overheated	Fan failure	Contact customer support
FANS, 6_FAILED, LOG_CRITICAL	Switch overheated	Fan failure	Contact customer support
FCIU, IUBAD, L, S	Invalid IU	OS error	Contact customer support
FCIU, IUCOUNT, L, S	Total number of IUs Count < 0	OS error	Contact customer support
FCPH, EXCHBAD, L, S	Bad exchange	OS error	Contact customer support
FCPH, EXCHFREE, L, S	Unable to free an exchange	OS error	Contact customer support
FLANNEL, PHANTOM, LOG_WARNING	Port PLT limit exceeded	OS error	Contact customer support
FLASH, BAD_MIRROR, LOG_WARNING	The system flash memory has encountered an error.	OS error	The system attempts to recover from its mirrored backup. Contact customer support
FLOOD, INVLSU, LOG_WARNING	Discard received LSU	OS error	Contact customer support
FLOOD, INVLSR, LOG_WARNING	Unknown LSR type	OS error	Contact customer support
FLOOD, LSRLEN, LOG_ERROR	Excessive LSU length	OS error	Contact customer support
FSPF, INPORT, LOG_ERROR	Input port out of range	OS error	Contact customer support
FSPF, NBRCHANGE, LOG_WARNING	Wrong neighbor ID in Hello message from port	OS error	Contact customer support
FSPF, REMDOMAIN, LOG_ERROR	Remote Domain ID out of range	OS error	Contact customer support
FSPF, SCN, LOG_WARNING	Illegal SCN	OS error	Contact customer support

Table 61. System error messages (continued)

Message	Description	Probable cause	Action
FSPF, SECTION, LOG_ERROR	Wrong Section ID	OS error	Contact customer support
FSPF, VERSION, LOG_ERROR	FSPF version not supported	OS error	Contact customer support
HLO, DEADTIMEOUT, LOG_ERROR	Incompatible Inactivity timeout from port	OS error	Contact customer support
HLO, HLOTIMEOUT, LOG_ERROR	Incompatible Hello timeout from port OS error	OS error	Contact customer support
HLO, INVHLO, LOG_ERROR	Invalid Hello received from port	OS error	Contact customer support
LSDB, LSID, LOG_ERROR	Link State ID'd out of range	OS error	Contact customer support
LSDB, MAXINCARN, LOG_WARNING	Local Link State Record reached max incarnation	OS error	Contact customer support
LSDB, NOLOCALENTRY, LOG_CRITICAL	No database entry for local Link State Record	OS error	Contact customer support
LSDB, NOLSR, LOG_WARNING	No Link State Record for domain	OS error	Contact customer support
MCAST, ADDBRANCH, LOG_ERROR	Add branch failed	OS error	Contact customer support
MCAST, ADDPORT, LOG_WARNING	Add port failed	OS error	Contact customer support
MCAST, REMBRANCH, LOG_ERROR	Remove branch failed	OS error	Contact customer support
MCAST, REMPORT, LOG_WARNING	Remove port failed	OS error	Contact customer support
MCAST, NOPARENT, LOG_ERROR	Null parent	OS error	Contact customer support
MCAST, NOPARENTLSR, LOG_ERROR	Null lsrP	OS error	Contact customer support
MQ, QWRITE, L, M	Message queue overflow	Task blocked	Contact customer support
MQ, QREAD, L, M	Message queue unread	OS error	Contact customer support
MQ, MSGTYPE, E, M	Unknown message type	OS error	Contact customer support
NBFSM, NGBRSTATE, LOG_ERROR	Wrong input to neighbor FSM	OS error	Contact customer support
PANIC, TASKSPAWN, LOG_PANIC	Task creation failed	OS error	Contact customer support

Table 61. System error messages (continued)

Message	Description	Probable cause	Action
PANIC, SEMCREATE, LOG_PANIC	Semaphore creation failed	OS error	Contact customer support
PANIC, SEMDELETE, LOG_PANIC	Semaphore deletion failed	OS error	Contact customer support
PANIC, QCREATE, LOG_PANIC	Message queuer failed	OS error	Contact customer support
PANIC, QDELETE, LOG_PANIC	Message queuer deletion failed	OS error	Contact customer support
PANIC, MALLOC, LOG_PANIC	Memory allocation failed	OS error	Contact customer support
PANIC, FREE, LOG_PANIC	Memory free failed	OS error	Contact customer support
PANIC, INCONSISTENT, LOG_PANIC	Data out of sync	OS error	Contact customer support
PANIC, INTCONTEXT, LOG_PANIC	Data out of sync	OS error	Contact customer support
PANIC, ZOMTIMSET, LOG_PANIC	Attempt to set a zombie timer	OS error	Contact customer support
PANIC, ZOMTIMKILL, LOG_PANIC	Zombie timer destroyed	OS error	Contact customer support
PANIC, FREETIMRLSD, LOG_PANIC	Free timer released	OS error	Contact customer support
PANIC, TIMEUSECNT, LOG_PANIC	Timer use count exceeded	OS error	Contact customer support
PANIC, LSDB_CKSUM, LOG_PANIC	Link State Database checksum failed	OS error	Contact customer support
POWER, 1_FAILED, LOG_CRITICAL	Switch power failure	Power supply failure	Contact customer support
POWER, 2_FAILED, LOG_CRITICAL	Switch power failure	Power supply failure	Contact customer support
QL, QUICKLOOP PARTNER INCOMPATIBLE	The QuickLoop partner switch is running an earlier (than v2.1.3) version of the software.	OS error	Upgrade to a higher version of the fabric OS
RPC, SVC_EXIT	An RPC service daemon has ended prematurely or unexpectedly.	OS error	Contact customer support
RPC, SVC_REG	An RPC service daemon could not establish service for a particular protocol handler.	OS error	Contact customer support
SEMA, SEMGIVE, L, M	Unable to give a semaphore	OS error	Contact customer support

Table 61. System error messages (continued)

Message	Description	Probable cause	Action
SEMA, SEMTAKE, L, M	Unable to take a semaphore	OS error	Contact customer support
SEMA, SEMFLUSH, L, M	Unable to flush a semaphore	OS error	Contact customer support
SYS, NOMEM, LOG_CRITICAL	No memory	OS error	Contact customer support
SYS, SYSCALL, LOG_ERROR	System call failed	OS error	Contact customer support
SYS, BADPTR, LOG_ERROR	Bad system pointer	OS error	Contact customer support
SYS, INTRPT, LOG_CRITICAL	Bad system interrupt	OS error	Contact customer support
SYS, FLASHRD, LOG_ERROR	Flash memory read error	OS error	Contact customer support
SYS, FLASHWR, LOG_ERROR	Flash memory write error	OS error	Contact customer support
TEMP, 1_FAILED, LOG_WARNING	Switch overheated	Fan failure	Contact customer support
TEMP, 2_FAILED, LOG_ERROR	Switch overheated	Fan failure	Contact customer support
TEMP, 3_FAILED, LOG_CRITICAL	Switch overheated	Fan failure	Contact customer support
TEMP, 4_FAILED, LOG_CRITICAL	Switch overheated	Fan failure	Contact customer support
TEMP, 5_FAILED, LOG_CRITICAL	Switch overheated	Fan failure	Contact customer support
TIMERS, ENQFAIL, LOG_CRITICAL	Invalid timeout value	OS error	Contact customer support
TIMERS, MSG, LOG_WARNING	Invalid message	OS error	Contact customer support
UCAST, ADDPATH, LOG_CRITICAL	Add path failed	OS error	Contact customer support
UCAST, ADDPORT, LOG_WARNING	Add port failed	OS error	Contact customer support
UCAST, REMPORT, LOG_WARNING	Remove port failed	OS error	Contact customer support
UCAST, RRTIM, LOG_CRITICAL	Invalid reroute timer ID	OS error	Contact customer support
UCAST, SPFCOST, LOG_WARNING	No minimum cost path in candidate	OS error	Contact customer support
UCAST, RELICPDB, LOG_WARNING	Relic PDB to Domain	OS error	Contact customer support

Appendix B. Standards and protocol compliance

IBM is committed to providing products that comply with industry standards and protocols.

Standards

The 3534 Model F08 is compliant with the following standards:

- Fibre-Channel ANSI Specifications
  - FC-PH, version 4.3 (Fibre-Channel Physical)
  - FC-PH-2, version 7.4 (Fibre-Channel Physical, Enhanced) for Multicast and Broadcast functions
  - FC-PH-3, version 9.4
  - FC-SW-2, version 4.4 (Fibre-Channel Switched Fabric)
  - FC-FG Revision 3.5 (Fabric Generic Requirements)
  - FC-AL, version 4.5 (Arbitrated Loop)
  - FC-AL-2, version 5.7 (Arbitrated Loop Extensions)
  - FC-FLA, version 2.7 (Fabric Loop Attach)
  - FC-GS-2, version 5.3 (Generic Services)
  - FC-GS-3, version 6.42 or later (Generic Services)
  - FC-PLDA, version 2.1 (Private Loop Direct Attach)
  - FC-Tape Fibre-Channel Tape (FC-Tape)
  - FCP-2Rev4 (Fibre-Channel Protocol)
  - FC-FS Revision 0.2 or later
  - FC-IP
- SCSI Enclosure Services, Rev 8a
- EA/TIA RS-232 Serial Port specification
- Gigabit Interface Converter Definition Document, Sun, and so on
- IEEE 802.3 for Ethernet

Protocol compliance

The 3534 Model F08 complies with the following standards and protocols.

Support for fibre-channel ports

All ports on the 3534 Model F08 are universal ports and support F_port (point-to-point), FL_port (loop), and E_port (switch-to-switch) port connections.

Fibre-channel class operation

The 3534 Model F08 supports fibre-channel Class 2, Class 3, and Class F operations on all ports.

Auto-configuration

All ports support E_ports to allow for cascading switches to form larger fabrics. E_ports are auto-configuring. Linking ports from any two switches automatically configures an E_port connection to form the fabric. The 3534 Model F08 supports a trunking option that binds up to four ports together as a high-performance trunk group. In this trunking configuration, inter-switch data transfers can occur at an aggregate rate of 800 MBps in both directions. The trunk group is automatically configured on the ports of the switch as the links between the switches are connected.

In-order delivery

The 3534 Model F08 guarantees in-order delivery of frames between source F or FL and destination F or FL ports. In-order delivery is supported across any arbitrary switch configurations or fabric topologies.

Flexibility of fabric topology and operation

The 3534 Model F08 implements the FSPF routing protocol as specified in the T11 FC-SW-2 standard. Fabric topology and operation are automatically adjusted and dynamically distributed to the fabric as new switches and links are added to the fabric. This is completed with no operator intervention. When a link is added or removed, the routes are recalculated. The switch adopts a minimal disruption algorithm to minimize the impact of the route recalculation. To minimize disruption, the switch only reroutes traffic due to a new shortest path (if one has been established) or if new load sharing is required.

Fibre-channel simple name service

Fabric OS includes support for the fibre-channel simple name service as specified in FC-GS-3 version 6.42 or the latest published standard.

Fibre-channel state change notification service

Fabric OS supports the fibre-channel state change notification service as specified in FC-GS-3 version 6.42 or the latest published standard.

Fibre-channel alias and multicast services

Fabric OS supports the alias and multicast services as specified in FC-GS-3 version 6.42 or the latest published standard.

Support for fibre-channel protocol

The 3534 Model F08 supports the FCP-2Rev4 standard.

Support for FC-IP

Fabric OS supports FC-IP (as defined by IETF), including the address resolution protocol (ARP) service for IP nodes that are connected to the switch.

Appendix C. Safety certifications and regulatory compliance

The 3534 Model F08 switch complies with all the safety and regulatory standards listed in this chapter.

Safety

The 3534 Model F08 switch is certified to :

- UL1950/CSA950 binational
- IEC950/EN 60950 (Nemko & TUV; CE)

Additionally, the following Product Safety/Country or Region Testing/Certifications has been completed.

- Federal Communications Commission (FCC) statement (United States)
- Voluntary Control Council for Interference (VCCI) mark (Japan)
- BSMI (Taiwan)
- C-tick mark (Australia)
- CE Mark (Europe)
- Canada class number
- GOST approval (Russia)
- NOM mark (Mexico)

EMI/EMC

Radiated Electro-Magnetic Interference (EMI) emissions for the 3534 Model F08 power supply operating in a single or redundant power configuration comply with EMI levels specified by the following regulations:

- FCC Docket No. 20780, Part 15J, Class B level
- CISPR22 Class A
- EN55022 Class B
- VCCI Class A ITE

Additionally, the 3534 Model F08 power supply has received a CE Mark for susceptibility and complies with the following Electro-Magnetic Compatibility (EMC) regulations:

- EN 61000-3-2 (Harmonics)
- EN 61000-3-3 (Voltage Fluctuations)
- EN 55024 (Immunity)

Immunity

The 3534 Model F08 switch provides immunity 50% greater than the levels specified by EN 55024 and complies with the following specifications:

- EN 61000-4-2, Severity Level 3 for ESD
- EN 61000-4-3, Severity Level 3 for RF Fields
- EN 61000-4-4, Severity Level 3 for EFT/Burst
- EN 61000-4-5, Severity Level 3 for Surge Voltage
- EN 61000 4-11, Power, Sag, Dip, and Variations

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
TotalStorage

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

Microsoft and Windows NT are trademarks of Microsoft 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.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

Electronic emission statements

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

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 non-recommended modification of the product, including the fitting of non-IBM option cards.

This product is in conformity with the EU council directive 73/23/EEC on the approximation of the laws of the Member States relating to electrical equipment designed for use within certain voltage limits. This conformity is based on compliance with the following harmonized standard: EN60950.

This product has been tested and found to comply with the limits for class A Information Technology Equipment according to European Standard EN 55022. The limits for class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

Attention: This is a class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

Where shielded or special cables (for example, cables fitted with ferrites) are used in the test to make the product comply with the limits:

Properly shielded and grounded cables and connectors must be used in order to reduce the potential for causing interference to radio and TV communications and to other electrical or electronic equipment. Such cables and connectors are available from IBM authorized dealers. IBM cannot accept responsibility for any interference caused by using other than recommended cables and connectors.

Germany compliance statement

Zulassungsbescheinigung laut Gesetz ueber die elektromagnetische

Vertraeglichkeit von Geraeten (EMVG) vom 30. August 1995.

Dieses Geraet ist berechtigt, in Uebereinstimmung mit dem deutschen EMVG das

EG-Konformitaetszeichen - CE - zu fuehren.

Der Aussteller der Konformitaetserklaeung ist die IBM Deutschland.

Informationen in Hinsicht EMVG Paragraph 3 Abs. (2) 2:

Das Geraet erfuellt die Schutzanforderungen nach EN 50082-1 und EN 55022 Klasse A.

EN 55022 Klasse A Geraete beduerfen folgender Hinweise:

Nach dem EMVG:_|t¹|

"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 entsprechenden

Kostenverordnung (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 that this is not suitable for your use, you may exchange it for one with a non-business use.

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。

IBM license agreement for Machine Code

Regardless of how you acquire (electronically, preloaded, on media or otherwise) BIOS, Utilities, Diagnostics, Device Drivers, firmware, 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.

Glossary

This glossary provides definitions for the fibre-channel and switch terminology used for the IBM 3534 Model F08.

This glossary defines technical terms and abbreviations used in this book. If you do not find the term you are looking for, see the *IBM Glossary of Computing Terms* located at www.ibm.com/networking/nsg/nsgmain.htm

This glossary also includes terms and definitions from:

- *Information Technology Vocabulary* by Subcommittee 1, Joint Technical Committee 1, of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC JTC1/SC1). Definitions are identified by the symbol (I) after the definition; definitions taken from draft international standards, committee drafts, and working papers by ISO/IEC JTC1/SC1 are identified by the symbol (T) after the definition, indicating that final agreement has not yet been reached among the participating National Bodies of SC1.
- *IBM Glossary of Computing Terms*. New York: McGraw-Hill, 1994.

The following cross-reference conventions are used in this glossary:

See Refers you to (a) a term that is the expanded form of an abbreviation or acronym, or (b) a synonym or more preferred term.

See also
Refers you to a related term.

8b/10b encoding. An encoding scheme that converts each 8-bit byte into 10 bits. Used to balance ones and zeros in high-speed transports

ACL. Access control list.

address identifier. A 24-bit or 8-bit value used to identify the source or destination of a frame.

alias address identifier. An address identifier recognized by a port in addition to its standard identifier. An alias address identifier may be shared by multiple ports.

alias AL_PA. An AL_PA value recognized by an L_port in addition to the AL_PA assigned to the port. See also *arbitrated loop physical address*.

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

AL_PA. See *arbitrated loop physical address*.

American National Standards Institute (ANSI). The governing body for fibre channel standards in the U.S.A.

ANSI. See *American National Standards Institute*.

API. See *application programming interface*.

application programming interface (API). A defined protocol that allows applications to interface with a set of services.

ARB. See *arbitrate primitive signal*.

arbitrate primitive signal. A primitive signal that is transmitted as the fill word by an L_port to indicate that the L_port is arbitrating to access to the loop. Applies only to the arbitrated loop topology.

arbitrated loop. A shared 100 MBps fibre-channel transport structured as a loop and supporting up to 126 devices and one fabric attachment. A port must successfully arbitrate before a circuit can be established.

arbitrated loop physical address (AL_PA). An 8-bit value used to uniquely identify an individual port within a loop. A loop may have one or multiple AL_PAs.

ARP. Address resolution protocol.

ASIC. Application-specific integrated circuit.

asynchronous transfer mode (ATM). A broadband technology for transmitting data over LANs or WANs, based on relaying cells of fixed size. Provides any-to-any connectivity, and nodes can transmit simultaneously.

ATM. See *asynchronous transfer mode*.

autoranging. A power supply that accommodates different input voltages and line frequencies.

arbitration wait timeout value (AW_TOV). The minimum time an arbitrating L_port waits for a response before beginning loop initialization.

AW_TOV. See *arbitration wait timeout value*.

bandwidth. The total transmission capacity of a cable, link, or system. Usually measured in bits per second (bps). May also refer to the range of transmission frequencies available to a network. See also *throughput*.

basic input/output system (BIOS). Code that controls basic hardware operations, such as interactions with diskette drives, hard disk drives, and the keyboard.

BB. Buffer-to-buffer.

BB_Credit. See *buffer-to-buffer credit*.

beginning running disparity. The disparity at the transmitter or receiver when the special character associated with an ordered set is encoded or decoded. See also *disparity*.

BER. See *bit error rate*.

BIOS. See *basic input/output system*.

BISR. Built-in self-repair.

bit error rate. The rate at which bits are expected to be received in error. Expressed as the ratio of error bits to total bits transmitted. See also *error*.

block. As applies to fibre channel, upper-level application data that is transferred in a single sequence.

bloom. Application-specific integrated circuit (ASIC) technology that the 3534 Model F08 is based on.

broadcast. The transmission of data from a single source to all devices in the fabric, regardless of zoning. See also *multicast* and *unicast*.

BTU. British thermal unit.

buffer-to-buffer credit. The number of frames that can be transmitted to a directly-connected recipient or within an arbitrated loop. Determined by the number of receive buffers available. See also *buffer-to-buffer flow control, end-to-end credit*.

buffer-to-buffer flow control. Management of the frame transmission rate in either a point-to-point topology or in an arbitrated loop. See also *buffer-to-buffer credit*.

CAM. Content addressable memories.

cascade. Two or more interconnected fibre-channel switches. Switches can be cascaded up to 239 switches, with a recommended maximum of seven inter-switch links (no path longer than eight switches). See also *fabric, inter-switch link*.

cascading switches. Switches that are interconnected to build large fabrics.

central processing unit (CPU). A part of a computer that includes the circuits that control the interpretation and execution of instructions. A CPU in the circuitry and storage that executes instructions. Traditionally, the complete processing unit was often regarded as the CPU, whereas today the CPU is often a microchip. In either case, the centrality of a processor or processing unit depends on the configuration of the system or network in which it is used.

chassis. The metal frame in which the switch and switch components are mounted.

circuit. An established communication path between two ports. Consists of two virtual circuits capable of transmitting in opposite directions. See also *link*.

class F. Connectionless service for inter-switch control traffic. Provides notification of delivery or nondelivery between two E_ports.

class 1. Service that provides a dedicated connection between two ports (also called connection-oriented service), with notification of delivery or nondelivery.

class 2. Connectionless service between ports with notification of delivery or nondelivery.

class 3. Connectionless service between ports without notification of delivery. Other than notification, the transmission and routing of class 3 frames is the same as class 2 frames.

class of service. A specified set of delivery characteristics and attributes for frame delivery.

CMI. Control message interface.

comma. A unique pattern (either 1100000 or 0011111) used in 8B/10B encoding to specify character alignment within a data stream. See also *K28.5*.

CPLD. Complex programmable logic device.

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

CPU. See *central processing unit*.

CRC. See *cyclic redundancy check*.

credit. When applied to a switch, 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 FL_port.

cut-through. A switching technique that allows the route for a frame to be selected as soon as the destination address is received. See also *route*.

cyclic redundancy check (CRC). A check for transmission errors included in every data frame.

data word. A type of transmission word that occurs within frames. The frame header, data field, and CRC all consist of data words. See also *frame, ordered set, transmission word*.

DDR. Double data rate.

defined zone configuration. The complete set of all zone objects that are defined in the fabric. The defined configuration may include multiple zone configurations. See also *enabled zone configuration, zone configuration*.

DID. The 3-byte destination ID of the destination device, in the 0xDomainAreaALPA format.

disparity. The relationship of ones and zeros in an encoded character. *Neutral disparity* means an equal number of each, *positive disparity* means a majority of ones, and *negative disparity* means a majority of zeros.

DLS. See *dynamic load sharing*.

DMA. Direct memory access.

DNS. Distributed name server.

domain_ID. Unique identifier for the switch in a fabric. Usually automatically assigned by the switch, but may also be assigned manually. May be any value between 1- 239.

DOS. Disk operating system.

DRAM. Dynamic random access memory.

DWDM. Dense wavelength digital multiplexing.

dynamic load sharing (DLS). Dynamic distribution of traffic over available paths. Allows for recomputing of routes when an Fx_port or E_port changes status.

E_D_TOV. See *error detect timeout value*.

EE_Credit. See *end-to-end credit*.

effective configuration. The particular zone configuration that is currently in effect. Only one configuration can be in effect at once. The effective configuration is built each time a zone configuration is enabled.

EIA. Electronic Industry Association.

EIA rack. A storage rack that meets the standards set by the Electronics Industry Association.

ELP. Extended link parameters.

EMC. Electro-magnetic compatibility.

EMI. Electromagnetic interference.

enabled zone configuration. The currently enabled configuration of zones. Only one configuration can be enabled at a time. See also *defined zone configuration, zone configuration*.

end-to-end credit (EE_Credit). The number of receive buffers allocated by a recipient port to an originating port. Used by class 1 and class 2 services to manage the exchange of frames across the fabric between source and destination. See also *end-to-end flow control, buffer-to-buffer credit*.

end-to-end flow control. Governs flow of class 1 and class 2 frames between N_ports. See also *end-to-end credit*.

E_port. See *expansion port*.

error. As applies to fibre channel, a missing or corrupted frame, timeout, loss of synchronization, or loss of signal (link errors). See also *loop failure*.

error detect timeout value (E_D_TOV). The time that the switch waits for an expected response before declaring an error condition. Adjustable in 1 microsecond increments from 2 - 10 seconds.

ESD. Electrostatic discharge.

EVPD. Enable Vital Product Data.

exchange. The highest level fibre-channel mechanism used for communication between N_ports. Composed of one or more related sequences, and can work in either one or both directions.

expansion port (E_port). A port is designated an E_port when it is used as an inter-switch expansion port to connect to the E_port of another switch, to build a larger switch fabric.

Extended Fabrics. A product that runs on Fabric OS and allows creation of a fibre-channel fabric interconnected over distances of up to 100 km (62.14 mi).

fabric. A network that uses high-speed fibre connections to connect switches, hosts, and devices. A fabric is an active, intelligent, nonshared interconnect scheme for nodes.

Fabric Assist. A feature that enables private and public hosts to access public targets anywhere on the fabric, provided they are in the same Fabric Assist zone. This feature is available only when both QuickLoop and zoning are installed on the switch.

fabric login (FLOGI). The process by which a device gains access to the fabric.

fabric loop port (FL_port). A fabric port that is loop capable. Used to connect NL_ports to the switch in a loop configuration.

fabric name. The unique identifier assigned to a fabric and communicated during login and port discovery.

fabric port (F_port). A port that is able to transmit under fabric protocol and interface over links. Can be used to connect an N_port to a switch. See also *fabric loop port, Fx_port*.

Fabric Watch. A product that runs on Fabric OS and allows monitoring and configuration of fabric and switch elements.

FAN. Fabric address notification.

FC. Fibre channel.

FCA. See *fibre-channel arbitrated loop*.

FC-AL. The Fibre Channel Arbitrated Loop standard. Defined on top of the FC-PH standard. Defines the arbitration on a loop where several FC nodes share a common medium.

FC-AL-3. The Fibre Channel Arbitrated Loop standard defined by ANSI. Defined on top of the FC-PH standards.

FCC. Federal Communications Commission.

FC-FLA. The Fibre Channel Fabric Loop Attach standard defined by ANSI.

FCP. See *fibre-channel protocol*.

FC-PH-1,2,3. The Fibre Channel Physical and Signaling Interface standards defined by ANSI.

FC-PI. The Fibre Channel Physical Interface standard defined by ANSI.

FC-PDLA. The Fibre Channel Private Loop Direct Attach standard defined by ANSI. Applies to the operation of peripheral devices on a private loop.

FC-SW-2. The second generation of the Fibre Channel Switch Fabric standard defined by ANSI. Specifies tools and algorithms for the interconnection and initialization of fibre-channel switches in order to create a multi-switch fibre-channel fabric.

fibre-channel arbitrated loop. 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.

fibre-channel protocol (FCP). The protocol for transmitting commands, data, and status using fibre-channel FC-FS exchanges and information units. Fibre channel is a high-speed serial architecture that allows either optical or electrical connections at data rates from 265 Mbps up to 4-Gbps.

fibre-channel service (FS). A service that is defined by fibre-channel standards and exists at a well-known address. For example, the Simple Name Server is a fibre-channel service. See also *fibre-channel service protocol*.

fibre-channel service protocol (FSP). The common protocol for all fabric services, transparent to the fabric type or topology. See also *fibre-channel service*.

fibre-channel shortest path first (FSPF). A routing protocol used by fibre-channel switches.

fibre-channel transport. A protocol service that supports communication between fibre-channel service providers. See also *fibre-channel service protocol*.

field replaceable unit (FRU). An assembly that is replaced in its entirety when any one of its components fails. In some cases, a field replaceable unit may contain other field replaceable units.

fill word. An IDLE or ARB ordered set that is transmitted during breaks between data frames to keep the fibre-channel link active.

firmware. The basic operating system provided with the hardware.

FLA. Fabric loop attach.

FLOGI. See *fabric login*.

FL_port. See *fabric loop port*.

F_port. See *fabric port*.

frame. The fibre-channel structure used to transmit data between ports. Consists of a start-of-frame delimiter, header, any optional headers, the data payload, a cyclic redundancy check (CRC), and an end-of-frame delimiter. There are two types of frames: Link control frames (transmission acknowledgements, and so on) and data frames.

FRU. See *field replaceable unit*.

FS. See *fibre-channel service*.

FSP. See *fibre-channel service protocol*.

FSPF. See *fibre-channel shortest path first*.

FTP. File transfer protocol.

full-duplex. A mode of communication that allows the same port to simultaneously transmit and receive frames. See also *half-duplex*.

Fx_port. A fabric port that can operate as either an F_port or FL_port. See also *fabric port, fabric loop port*.

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

GBIC. See *gigabit interface converter*.

GBps. Gigabytes per second.

Gbps. Gigabits per second.

generic port (G_port). A generic port that can operate as either an E_port or an F_port. A port is defined as a

G_port when it is not yet connected or has not yet assumed a specific function in the fabric.

gigabit interface converter (GBIC). A removable serial transceiver module designed to provide gigabaud capability for fibre channel (FC) and other products that use the same physical layer.

gigabit switch. A 16-port, fibre-channel gigabit switch.

G_port. See *generic port*.

half-duplex. A mode of communication that allows a port to either transmit or receive frames at any time, but not simultaneously (with the exception of link control frames, which can be transmitted at any time). See also *full-duplex*.

hard address. The AL_PA that an NL_port attempts to acquire during loop initialization.

hardware translative mode. Method for achieving address translation. The following two hardware translative modes are available to a QuickLoop-enabled switch:

- Standard Translative Mode: Allows public devices to communicate with private devices across the fabric.
- QuickLoop Mode: Allows private devices to communicate with other private devices across the fabric.

HBA. See *host bus adapter*.

host bus adapter (HBA). The interface card between a server or workstation bus and the fibre-channel network.

hub. A fibre-channel wiring concentrator that collapses a loop topology into a physical star topology. Nodes are automatically added to the loop when active and removed when inactive.

ID. Identification.

IDB. Interface descriptor block.

IDLE. Continuous transmission of an ordered set over a fibre-channel link when no data is being transmitted, to keep the link active and maintain bit, byte, and word synchronization.

IETF. Internet Engineering Task Force.

information unit (IU). A set of information as defined by either upper-level process protocol definition or upper-lever protocol mapping.

initiator. A server or workstation on a fibre-channel network that initiates communications with storage devices. See also *target*.

in-order delivery (IOD). A parameter that, when set, guarantees that frames are either delivered in order or dropped.

integrated fabric. The fabric created by six switches cabled together and configured to handle traffic as a seamless group.

internet protocol (IP). In the Internet suite of protocols, a connectionless protocol that routes data through a network or interconnected networks and acts as an intermediary between the higher protocol layers and the physical network.

inter-switch link (ISL). A fibre link between two switches.

IOD. See *in-order delivery*.

IP. See *internet protocol*.

IPA. Initial process associator.

ISL. See *inter-switch link*.

ISL Trunking. A feature that enables distribution of traffic over the combined bandwidth of up to four ISLs (between adjacent switches), while preserving in-order delivery. A set of trunked ISLs is called a trunking group; each port employed in a trunking group is called a trunking port. See also *master port*.

isolated E_port. An E_port that is online but not operational between switches due to overlapping domain ID or nonidentical parameters such as E_D_TOVs. See also *expansion port*.

IU. See *information unit*.

JBOD. See *just a bunch of disks*.

just a bunch of disks (JBOD). Indicates a number of disks connected in a single chassis to one or more controllers. See also *redundant array of independent disks*.

K28.5. A special 10-bit character used to indicate the beginning of a transmission word that performs fibre channel control and signaling functions. The first seven bits of the character are the comma pattern. See also *comma*.

LAN. See *local area network*.

latency. The period of time required to transmit a frame, from the time it is sent until it arrives.

LED. See *light-emitting diode*.

light-emitting diode (LED). A semiconductor chip that gives off visible or infrared light when activated.

link. As applies to fibre channel, a physical connection between two ports, consisting of both transmit and receive fibers. See also *circuit*.

link services. A protocol for link-related actions.

LIP. See *loop initialization primitive*.

LM_TOV. See *loop master timeout value*.

local area network (LAN). A computer network located on a user's premises within a limited geographical area. (T)

long wavelength (LWL). A type of fiber optic cabling that is based on 1300 mm lasers and supports link speeds of 1.0625 Gbps. May also refer to the type of GBIC or SFP. See also *short wavelength*.

loop. A configuration of devices (for example, JBODs) connected to the fabric by way of an FL_port interface card.

loop failure. Loss of signal within a loop for any period of time, or loss of synchronization for longer than the timeout value.

loop_ID. A hex value representing one of the 127 possible AL_PA values in an arbitrated loop.

loop initialization. The logical procedure used by an L_port to discover its environment. Can be used to assign AL_PA addresses, detect loop failure, or reset a node.

loop initialization primitive (LIP). The signal used to begin initialization in a loop. Indicates either loop failure or resetting of a node.

looplet. A set of devices connected in a loop to a port that is a member of another loop.

loop master timeout value (LM_TOV). The minimum time that the loop master waits for a loop initialization sequence to return.

L_port. See *loop port*.

loop port (L_port). A node port (NL_port) or fabric port (FL_port) that has arbitrated loop capabilities. An L_port can be in one of two modes:

- Fabric mode, connected to a port that is not loop capable, and using fabric protocol.
- Loop mode, in an arbitrated loop and using loop protocol. An L_port in loop mode can also be in participating mode or nonparticipating mode.

See also *non-participating mode, participating mode*.

loop port state machine (LPSM). The logical entity that performs arbitrated loop protocols and defines the behavior of L_ports when they require access to an arbitrated loop.

LPSM. See *loop port state machine*.

LSA. Link state acknowledgement.

LSR. Link state record.

LSU. Link state update.

LUN. Logical unit number.

LWL. See *long wavelength*.

MAC. Media access controller.

management information base (MIB). An SNMP structure to help with device management, providing configuration and device information.

MAP. Maintenance action plan.

master port. As relates to trunking, the port that determines the routing paths for all traffic flowing through the trunking group. One of the ports in the first ISL in the trunking group is designated as the master port for that group. See also *ISL Trunking*.

MIB. See *management information base*.

multicast. The transmission of data from a single source to multiple specified N_ports (as opposed to all the ports on the network). See also *broadcast*, *unicast*.

multimode. A fiber optic cabling specification that allows up to 500 m (1640.5 ft) between devices.

name server. Frequently used to indicate Simple Name Server. See also *simple name server*.

NL_port. See *node loop port*.

node. A fibre-channel device that contains an N_port or NL_port.

node loop port (NL_port). A node port that is loop capable. Used to connect an equipment port to the fabric in a loop configuration through an FL_port.

node name. The unique identifier for a node, communicated during login and port discovery.

node port (N_port). A node port that is not loop capable. Used to connect an equipment port to the fabric.

non-participating mode. A mode in which an L_port in a loop is inactive and cannot arbitrate or send frames, but can retransmit any received transmissions. This mode is entered if there are more than 127 devices in a loop and an AL_PA cannot be acquired. See also *participating mode*.

N_port. See *node port*.

NVRAM. Nonvolatile RAM.

Nx_port. A node port that can operate as either an N_port or NL_port. See also *node port, node loop port*.

OFC. Open fibre control.

ordered set. A transmission word that uses 8B/10B mapping and begins with the K28.5 character. Ordered sets occur outside of frames, and include the following items:

- *Frame delimiters* mark frame boundaries and describe frame contents.
- *Primitive signals* indicate events.
- *Primitive sequences* indicate or initiate port states.

Ordered sets are used to differentiate fibre-channel control information from data frames and to manage the transport of frames.

packet. A set of information transmitted across a network. See also *frame*.

participating mode. A mode in which an L_port in a loop has a valid AL_PA and can arbitrate, send frames, and retransmit received transmissions. See also *non-participating mode*.

path selection. The selection of a transmission path through the fabric. Switches use the FSPF protocol.

PCB. Printed circuit board.

PCI. Peripheral control interconnect.

Performance Monitoring. A product that provides error and performance information to the administrator and end user for use in storage management.

PCV. Page code valid.

PF. Page format.

phantom address. An AL_PA value that is assigned to a device that is not physically in the loop. Also known as phantom AL_PA.

phantom device. A device that is not physically in an arbitrated loop but is logically included through the use of a phantom address.

PLDA. See *private loop direct attach*.

PLOGI. See *port login*.

PMC. PCI mezzanine card.

P/N. Part number.

point-to-point. A fibre-channel topology that employs direct links between each pair of communicating entities. See also *topology*.

port login (PLOGI). The port-to-port login process by which initiators establish sessions with targets. See also *fabric login*.

port_name. The unique identifier assigned to a fibre-channel port. Communicated during login and port discovery.

POST. See *power-on self-test*.

power-on self-test (POST). A series of diagnostics that are automatically run by a device when the power is turned on.

private device. A device that supports arbitrated loop protocol and can interpret 8-bit addresses, but cannot log into the fabric.

private loop. An arbitrated loop that does not include a participating FL_port.

private loop direct attach (PLDA). A subset of fibre channel standards for the operation of peripheral devices.

private NL_port. An NL_port that communicates only with other private NL_ports in the same loop and does not log into the fabric.

protocol. A defined method and a set of standards for communication.

public device. A device that supports arbitrated loop protocol, can interpret 8-bit addresses, and can log into the fabric.

public loop. An arbitrated loop that includes a participating FL_port, and may contain both public and private NL_ports.

public NL_port. An NL_port that logs into the fabric, can function within either a public or a private loop, and can communicate with either private or public NL_ports.

QuickLoop. (1) A product that makes it possible to allow private devices within loops to communicate with public and private devices across the fabric through the creation of a larger loop. (2) The arbitrated loop created using this software. A QuickLoop can contain a number of devices or looplets; all devices in the same QuickLoop share a single AL_PA space.

RAID. See *redundant array of independent disks*.

RAM. See *random access memory*.

RAN. Remote Asynchronous Notification.

random access memory (RAM). A temporary storage location in which the CPU stores and executes its processes.

R_A_TOV. See *resource allocation timeout value*.

redundant array of independent disks (RAID). A collection of disk drives that appear as a single volume to the server and are fault tolerant through mirroring or parity checking. See also *just a bunch of disks*.

registered state change notification (RSCN). A switch function that allows notification of fabric changes to be sent from the switch to specified nodes.

remote procedure call (RPC). A facility that a client uses to request the execution of a procedure call from a server.

Remote Switch. A product that runs on Fabric OS and enables two fabric switches to be connected over an asynchronous transfer mode (ATM) connection. This requires a compatible fibre channel to ATM gateway, and can have a distance of up to 10 km (6.214 mi) between each switch and the respective ATM gateway.

request rate. The rate at which requests arrive at a servicing entity. See also *service rate*.

resource allocation timeout value (R_A_TOV). Used to time out operations that depend on the maximum possible time that a frame can be delayed in a fabric and still be delivered. This value is adjustable in one microsecond increments from 10 - 120 seconds.

resource recovery timeout value (RR_TOV). The minimum time a target device in a loop waits after a LIP before logging out a SCSI initiator. See also *error detect timeout value, resource allocation timeout value*.

RISC. Reduced Instruction Set Computer.

ro. Read only.

ROM. Read only memory.

route. As applies to a fabric, the communication path between two switches. May also apply to the specific path taken by an individual frame, from source to destination. See also *fibre-channel shortest path first*.

routing. The assignment of frames to specific switch ports, according to frame destination.

RPC. See *remote procedure call*.

RR_TOV. See *resource recovery timeout value*.

RSCN. See *registered state change notification*.

RSH. Remote shell.

rw. Read-write.

SAN. See *storage area network*.

SC. Standard connector.

SCSI. See *small computer systems interface*.

SCSI Enclosure Services (SES). A subset of the SCSI protocol used to monitor temperature, power, and fan status for enclosure devices.

SDR. Single data rate.

sequence. A group of related frames transmitted in the same direction between two N_ports.

SERDES. Serializer/deserializer.

service rate. The rate at which an entity can service requests. See also *request rate*.

SES. See *SCSI Enclosure Services*.

SESD. An SES device.

SFF. Bidirectional devices (transceivers) that can receive serial optical signals and convert them into electrical signals or receive electrical signals and retransmit them as optical signals.

SFP. See *small form-factor pluggable*.

short wavelength (SWL). A type of fiber optic cabling that is based on 850 mm lasers and supports 1.0625 Gbps link speeds. May also refer to the type of GBIC or SFP. See also *long wavelength*.

SI. Sequence initiative.

SID. The 3-byte source ID of the originator device, in the 0xDomainAreaALPA format.

SID-DID. Source identifier-destination identifier.

SIMMS. Single in-line modules.

simple name server (SNS). A switch service that stores names, addresses, and attributes for up to 15 minutes, and provides them as required to other devices in the fabric. SNS is defined by fibre channel standards and exists at a well-known address. May also be referred to as directory service. See also *fibre-channel service*.

simple network management protocol (SNMP). In the Internet suite of protocols, a network management protocol that is used to monitor routers and attached networks. SMNP is an application layer protocol. Information on devices managed is defined and stored in the application's Management Information Base (MIB).

single mode. The fiber optic cabling standard that corresponds to distances of up to 10 km (6.214 mi) between devices.

small computer systems interface (SCSI). A parallel bus architecture and a protocol for transmitting large data blocks up to a distance of 15 - 25 m (49 - 82 ft).

small form-factor pluggable (SFP). An optical transceiver used to convert signals between optical fiber cables and switches.

SMI. Special memory interface.

SNIA. Storage Network Industry Association.

SNMP. See *simple network management protocol*.

SNMPv1. The original standard for SNMP, now labeled v1.

SNS. See *simple name server*.

SOF. Start-of-frame.

SPC. SCSI-3 Primary Command.

storage area network. A network of systems and storage devices that communicate using fibre-channel protocols. See also *fabric*.

switch. Hardware that routes frames according to fibre-channel protocol and is controlled by software.

switch name. The arbitrary name assigned to a switch.

switch port. A port on a switch. Switch ports can be E_ports, F_ports, or FL_ports.

SWL. See *short wavelength*.

Tachyon. A type of host bus adapter.

target. A storage device on a fibre-channel network. See also *initiator*.

TCP. See *transmission control protocol*.

tenancy. The time from when a port wins arbitration in a loop until the same port returns to the monitoring state. Also referred to as loop tenancy.

topology. As applies to fibre channel, the configuration of the fibre-channel network and the resulting communication paths allowed. There are three possible topologies:

- **Point to point:** A direct link between two communication ports.
- **Switched fabric:** Multiple N_ports linked to a switch by F_ports.
- **Arbitrated loop:** Multiple NL_ports connected in a loop.

throughput. The rate of data flow achieved within a cable, link, or system. Usually measured in bits per second (bps). See also *bandwidth*.

translative mode. A mode in which private devices can communicate with public devices across the fabric.

transmission character. A 10-bit character encoded according to the rules of the 8B/10B algorithm.

transmission control protocol (TCP). A communications protocol used in the Internet and in any network that follows the Internet Engineering Task Force (IETF) standards for Internet protocol.

transmission word. A group of four transmission characters.

trap (SNMP). The message sent by an SNMP agent to inform the SNMP management station of a critical error. See also *simple network management protocol*.

tunneling. A technique for enabling two networks to treat a transport network as though it were a single communication link or LAN.

Tx. Transmitted.

U. Unit of measure for rack-mounted equipment.

UART. Universal Asynchronous Receiver Transmitter.

UDP. See *user datagram protocol*.

ULP. See *upper-level protocol*.

ULP_TOV. See *upper-level timeout value*.

unicast. The transmission of data from a single source to a single destination. See also *broadcast, multicast*.

universal port (U_port). A switch port that can operate as a G_port, E_port, F_port, or FL_port. A port is defined as a U_port when it is not connected or has not yet assumed a specific function in the fabric.

U_port. See *universal port*.

upper-level protocol (ULP). The protocol that runs on top of fibre channel. Typical upper-level protocols are SCSI, IP, HIPPI, and IPI.

upper-level timeout value (ULP_TOV). The minimum time that a SCSI ULP process waits for SCSI status before initiating ULP recovery.

user datagram protocol. A protocol that runs on top of IP and provides port multiplexing for upper-level protocols.

VCCI. Voluntary Control Council for Interference

WAN. See *wide area network*.

WDM. Wave division multiplexing.

well-known address. As pertaining to fibre channel, a logical address defined by the fibre channel standards as assigned to a specific function, and stored on the switch.

wide area network (WAN). A network that provides communication services to a geographic area larger than that served by a local area network or a metropolitan network, and that may use or provide public communications facilities. (T)

workstation. A computer used to access and manage the fabric. May also be referred to as a management station or host.

worldwide name (WWN). Uniquely identifies a switch on local and global networks.

World Wide Web (WWW). A network of servers that contain programs and files. Many of the files contain hypertext links to other documents available through the network.

WWN. See *worldwide name*.

WWW. See *World Wide Web*.

zone. A set of devices and hosts attached to the same fabric and configured as being in the same zone. Devices and hosts within the same zone have access permission to others in the zone, but are not visible to any outside the zone. See also *zoning*.

zone alias. An alias for a set of port numbers or WWNs. Zone aliases can be used to simplify the entry of port numbers and WWNs. For example, “host” could be used as an alias for a WWN of 110:00:00:60:69:00:00:8a.

zone configuration. A set of zones designated as belonging to the same zone configuration. When a zone configuration is in effect, all valid zones in that configuration are also in effect.

zoning. A product that runs on Fabric OS and allows partitioning of the fabric into logical groupings of devices. Devices in a zone can only access and be accessed by devices in the same zone. See also *zone*.

Index

D

E

F

J

K

L

M

Q

R

S

T

U

V

W

Z

Readers' comments — we would like to hear from you.

IBM TotalStorage™ SAN Fibre Channel Switch
3534 Model F08 User's Guide

Publication No. GC26-7454-00

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	☐	☐	☐	☐	☐

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	☐	☐	☐	☐	☐
Complete	☐	☐	☐	☐	☐
Easy to find	☐	☐	☐	☐	☐
Easy to understand	☐	☐	☐	☐	☐
Well organized	☐	☐	☐	☐	☐
Applicable to your tasks	☐	☐	☐	☐	☐

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? ☐ Yes ☐ No

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

Name ____________________ Address ____________________

Company or Organization ____________________

Phone No. ____________________

Readers' Comments — We'd Like to Hear from You
GC26-7454-00

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. M86/Bldg.050-3
5600 Cottle Road
San Jose, CA
U.S.A. 95193-0001

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

Cut or Fold
Along Line

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

GC26-7454-00

Spine information:

IBM TotalStorage™ SAN Fibre Channel Switch

3534 Model F08 User's Guide