McDATA®

Networking the world's business data™

SAN Routers

Eclipse™ 2640 SAN Router Administration and Configuration Manual

P/N 620-00203-020
REV A

Simplifying Storage Network Management

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

Record of Revisions and Updates

Revision	Date	Description
620-00203-000	12/2004	Initial release of Manual to support E/OSi Version 4.6
620-00203-010	2/2005	Revision of Manual to support E/OSi Version 4.6.1
620-00203-020	10/2005	Revision of Manual to support E/OSi Version 4.7

Printed October 2005

Third Edition

Contents

Figures

Tables

Preface

This manual provides the information required to configure and use the Eclipse 2640 SAN Router in an Ethernet/IP or Fibre Channel (FC) data network.

Who Should Use this Manual

The manual is designed for IT professionals, including experienced Data Networking Administrators and System Architects.

How to Use this Manual

This publication is organized as follows:

Chapter 1, *Overview*, provides an overview of the SAN Router features, configuring the SAN Router for your network.

Chapter 2, *Configuring System Basics*, provides steps for configuring the SAN Router's basic functions.

Chapter 3, *Configuring RADs and mSAN Connections*, provides steps for configuring the SAN Router's Fibre Channel ports for router-attached (Fibre Channel) devices or RADs and for connection to fabrics within the metro area SAN (mSAN).

Chapter 4, *Configuring iSAN Connections*, provides detailed steps for configuring the SAN Router ports for iFCP and to setup iFCP connections.

Chapter 5, *Configuring iSCSI Connections*, includes detailed steps to configure the Ethernet ports for iSCSI network connections.

Chapter 6, *Monitoring SAN Router Operation and Connections*, provides details on how to monitor SAN Router performance and operation in the network using Element Manager.

Chapter 7, *Configuration, Firmware, and System Log Maintenance*, includes information for upgrading E/OSi firmware, backing up and restoring configuration data, resetting the system, upgrading bootrom, and retrieving and clearing the system log.

Chapter 8, *Troubleshooting*, gives the troubleshooting procedures for the Element Manager and the SAN Router.

The *Glossary* defines terms, abbreviations, and acronyms used in this manual.

An *Index* is also provided.

Related Documentation

Other publications that provide additional information about this SAN Router include:

- *SAN Routing E_Port and iFCP, Concepts and Technologies, Configuration Options, Design Guidelines, Best Practices, Caveats* White Paper - by Prasad Pammidimukkala.
- E/OSi Command Line Interface (CLI) User Manual (620-000207-050).
- SANvergence Manager User Manual (620-000189).
- Eclipse 2640 SAN Router Installation and Service Manual (620-000202).
- E/OSi SNMP Support Manual (620-000228)
- McDATA Products in a SAN Environment Planning Manual (620-000124)
- *IP SANs*, Tom Clark, Addison-Wesley, ISBN 0-201-75277-8.
- *Designing Storage Area Networks* Second Edition, Tom Clark, Addison-Wesley, ISBN 0-321-13650-0.
- *Gigabit Ethernet: Technology and Applications for High-Speed LANs*, Addison-Wesley, ISBN 0-201-18553-9.
- *Fibre Channel: A Comprehensive Introduction*, NLA, ISBN 0-931836-84-0.
- *Basics of SCSI*, Fourth Edition, Ancot Corporation, ISBN 0-963-74398-8.

For the latest release information, refer to the software release note (SRN) for E/OSi, located under the support tab on www.mcdata.com.

Manual Conventions

The following notational conventions are used in this document.

Convention	Meaning
Italic	Outside book references, names of user interface windows, panels, buttons, and dialog boxes
Bold	Keyboard keys
Click. As in "click the icon on the navigation control panel."	Click with the left mouse button on the object to activate a function.
Right-click. As in "right click the product icon."	Click with the right mouse button on the object to activate a function.
Select. As in "select the log entry."	Click once on the object to select it.

Where to Get Help

For technical support, McDATA® end-user customers should call the phone number located on the service label attached to the front or rear of the hardware product.

McDATA's "Best in Class" Solution Center provides a single point of contact for customers seeking help. The Solution Center will research, explore, and resolve inquires or service requests regarding McDATA products and services. The Solution Center is staffed 24 hours a day, 7 days a week, including holidays.

NOTE: To expedite warranty entitlement, please have your product serial number available.

McDATA Corporation

380 Interlocken Crescent

Broomfield, CO 80021

Phone: **(800) 752-4572** or **(720) 566-3910**

Fax: (720) 558-3851

E-mail: support@mcdata.com

NOTE: Customers who purchased the hardware product from a company other than McDATA should contact that company's service representative for technical support.

Forwarding Publication Comments

We sincerely appreciate any comments about this publication. Did you find this manual easy or difficult to use? Did it lack necessary information? Were there any errors? Could its organization be improved?

Please send your comments via e-mail, our home page, or FAX. Identify the manual, and provide page numbers and details. Thank you.

E-mail:	pubsmgr@mcdata.com
Home Page:	http://www.mcdata.com
FAX:	Technical Communications Manager (763) 268-8818

Ordering Publications

To order a paper copy of this manual, submit a purchase order as described in Ordering McDATA Documentation Instructions, which is found on McDATA's web site at the following location:

www.mcdata.com/downloads/tpub/other/customer_ordering_instructions.pdf.

To obtain documentation CD-ROMs, contact your sales representative.

Trademarks

1 Overview

This chapter provides an introduction to the Eclipse™ 2640 SAN Router. Use the following links to move through this chapter.

Introduction

The Eclipse 2640 SAN Router (referred to as SAN Router in this manual) supports iSCSI, iFCP, and R_Port for trunking to both Internet Protocol (IP) backbones and legacy Fibre Channel (FC) fabrics. The SAN Routers connect to a wide range of end systems, including Fibre Channel, NAS, and iSCSI initiators and targets. SAN Routers support Ethernet and Fibre Channel switching over extended distances at wire speed.

The SAN Router can be deployed for multiple, concurrent applications, including SAN routing in the data center (mSAN routing), SAN routing over distance (iSAN routing) for disaster recovery, and iSCSI access to Fibre Channel storage.

mSAN routing enables you to build very large, stable fabrics where faults in one part of the network do not impact traffic in other parts. For disaster recovery, the backup site can be quite distant, thanks to McDATA's patent-pending FastWrite technology, which can sustain wire-speed throughput in spite of high-link latency. The TCP ports on the SAN Router can support iSCSI access to Fibre Channel storage.

SAN Routers offer:

- mSAN internetworking for scalable and fault-tolerant SANs.
- Compression for increased bandwidth.
- Support for full fabric, private and public loop Fibre Channel devices.
- Patent-pending FastWrite™ technology for maximizing throughput across long distances.
- Storage-optimized TCP to ensure high throughput in a dedicated network in enterprise environments typically used for storage traffic.

The Eclipse 2640 SAN Router, shown in Figure 1-1 on page 1-3, contains 16 ports.

- Twelve user-configurable small form factor port (SFP) connectors (ports 1-12) support Fibre Channel connections.
- Four multiService intelligent SFP port connectors (ports 13-16) support Internet Fibre Channel Protocol (iFCP) or Internet small computer systems interface (iSCSI) connections over TCP/IP.

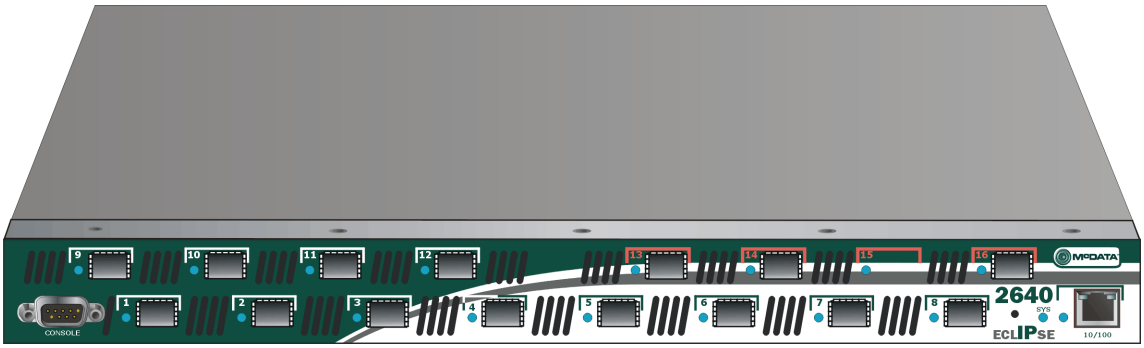


Figure 1-1 Eclipse 2640 SAN Router

Two management ports are located on the front of the SAN Router. An RS-232 serial port can connect to a VT100 or terminal emulator for access to the Command Line Interface (CLI), and an RJ45 port can connect to the LAN for out-of-band management through the SAN Router Element Manager and SANvergence Manager. The RJ45 management port can be accessed by any workstation on the LAN using http, Telnet, and SNMP for management.

The SAN Router has a modular design that enables quick removal and replacement of field replaceable units (FRUs), including:

- Redundant power supplies and cooling fans. The SAN Router has two power supplies, each with an AC power receptacle, and two cooling fans. Each power supply/fan unit is a field replaceable unit (FRU).
- Up to 16 duplex SFP fiber-optic port transceivers. Shortwave laser transceivers are available for transferring data over multimode fiber-optic cable. Longwave laser transceivers are available for transferring data over singlemode fiber-optic cable. Fiber-optic cables attach to SAN Router port transceivers with duplex LC connectors.

NOTE: Eclipse and IPS Switches have now been brought under one product family called Eclipse SAN Routers. During the transition from the Eclipse Switch to the Eclipse SAN Router name, the term “switch” and “SAN Router” may appear in software or product manuals and should be considered interchangeable.

SAN Router Features

The Eclipse 2640 SAN Router features are summarized in the following table.

Table 1-1 Eclipse 2640 SAN Router Features

Feature	Description
Intelligent Ports	The SAN Router supports two types of ports - standard ports and intelligent ports. A standard port can be configured for Fibre Channel traffic. An intelligent port can be configured for Ethernet port Internet Small Computer Systems Interface (iSCSI) or Internet Fibre Channel Protocol (iFCP).
iFCP standards track protocols	The SAN Router supports the IETF standard for the iFCP, which provides connectivity and networking for existing Fibre Channel devices over a TCP/IP network.
iSCSI	A TCP port can be configured for iFCP or iSCSI.
R_Port	Support for E_Port, or standard port, through the SAN Router R_Port, allows you to share devices between SANs while maintaining each SAN's independence.
FastWrite	The Fast-Write software feature available on intelligent ports improves the performance of write operations between Fibre Channel initiators and targets in a Wide Area Network (WAN). The improved speed depends on the WAN Round Trip Time (RTT), available buffer space on the target, number of concurrent I/Os supported by the application, and application I/O size.
Router Zoning	Using SANvergence Manager network management software or the CLI, you can create zones across networks. You can use zone sets for periodic reallocation of network resources. For example, you can have one set of zones for daytime data transactions and another set of zones for nighttime backups.

Table 1-1 Eclipse 2640 SAN Router Features (Continued)

Feature	Description
Real-time and historical system logs	The Element Manager and Log Viewer can be used to look at current system log messages from the connected SAN Router.
Compression	Compression technology available on intelligent ports identifies repetitive patterns in a data stream and represents the same information in a more compact and efficient manner. By compressing the data stream, more data can be sent across the network, even if slower link speeds are used. The Eclipse SAN Router supports both hardware and software compression.
Storage-optimized TCP	The storage-optimized TCP features supported by the SAN Router enhance performance in a dedicated network deployed in enterprise storage networks.

Scalability Metrics

For current scalability metrics on Fibre Channel, zoning, and iFCP/iSCSI for SAN Router products, such as maximum number of fabrics per mSAN, maximum imported Fibre Channel devices from a single fabric, maximum zones in a connected fabric, maximum number of SAN Routers in an mSAN, and other specifications, refer to the McDATA Fabric Guidelines (620-000208) on www.mcdata.com.

SAN Router Layout

The SAN Router front panel (Figure 1-2 on page 1-6) provides an Ethernet LAN connector (10/100), small form-factor pluggable (SFP) connectors port status LEDs, and a green system (SYS) LED. The panel also provides a 9-pin DSUB maintenance port (CONSOLE) for connection to a local terminal or remote terminal. The maintenance port provides an alternate way to configure the SAN Router in addition to the normal http scenario. Although this port is typically used by authorized maintenance personnel, operations personnel can use the port to configure SAN Router network addresses.

Sixteen user-configurable SFP connectors include:

- Ports 1-12, supporting Fibre Channel connections.
- Ports 13-16, supporting iFCP or iSCSI connections.

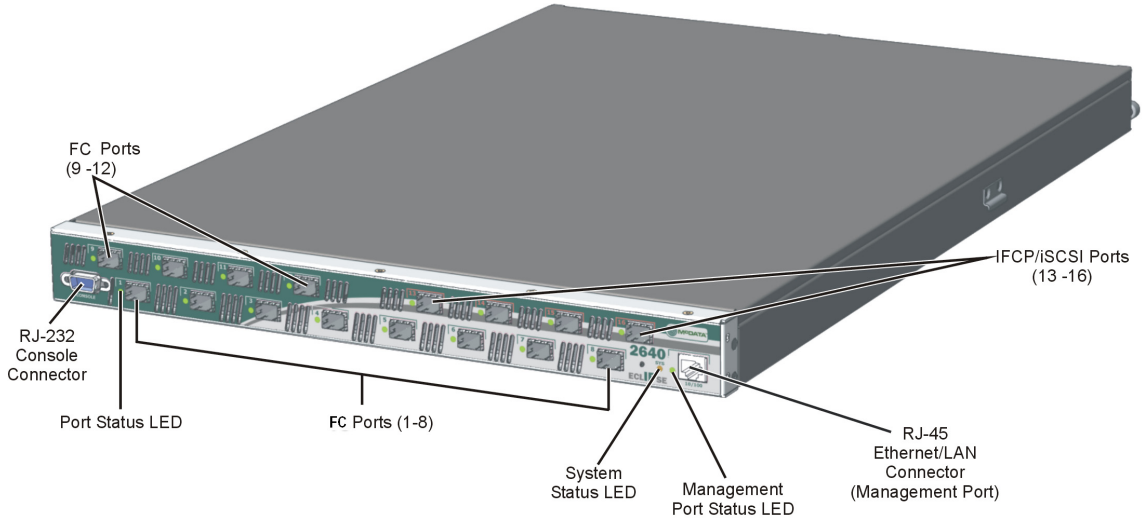


Figure 1-2 Eclipse 2640 LEDs, Ports, and Connectors

2

Configuring System Basics

This chapter provides steps for configuring the SAN Router's basic functions before performing specific configuration for various network connections.

Use the following links to move through the chapter.

Configuring the SAN Router

You can configure the SAN Router using any of the three options as follows:

- ***Command Line Interface (CLI).*** For this method a VT100 terminal or PC with terminal emulation software running must be connected to the RS-232 serial port on the SAN Router.
- ***SAN Router Element Manager.*** To use the Element Manger, you must configure the management port address for the SAN Router correctly so that you can access the SAN Router through the Element Manager and SANvergence Manger for configuration tasks.
- ***SANvergence Manager.*** Before configuring the SAN Router with SANvergence Manager, set up the correct management IP address and router IP address appropriate for your network.

For all these options, you must first set the management port address of the SAN Router. This address is set as a permanent one; it is retained even after the SAN Router is reset to factory results.

The following sections describe the steps required to set the basic parameters for the SAN Router before you can carry out advanced configuration.

Setting the Management IP Address

The 10/100 Ethernet port provides for out-of-band IP-based management, often used for enhanced security. This interface allows simple network management protocol (SNMP), Telnet, and web-based management traffic to be separated from storage traffic through the use of a separate LAN.

The management IP Address is used to receive and respond to SNMP-based management traffic from management workstations using the Element Manager and SANvergence Manager. Configure this IP address for the SAN Router management port through the Element Manager or CLI.

If the management workstation hosting the Element Manager and/or SANvergence Manager applications is on a different subnet from that configured in the *Management Port Configuration* dialog box, then a static route should be assigned to explicitly route the management traffic back to the management workstation. If there are multiple

management workstations in different networks, then multiple routes may need to be configured.

Unlike other configuration parameters, when the SAN Router is reset to factory defaults, the IP address of the management port is retained. This prevents administrators from locking themselves out of the SAN Router, requiring console connectivity to reset the management port IP address.

If the SAN Router is shipped in a cabinet, then the default IP address will be 10.xx.yy.zz where,

xx is the cabinet number (1, 2, 3, etc.)
yy is the product type identifier (16 for the Eclipse 2640 SAN Router)
zz is the position in the rack, bottom to top (1, 2, 3, etc.)

NOTE: The management port address must be configured correctly so that you can access the SAN Router through the Element Manager and SANvergence manager for further configuration tasks.

You can change the management port address using the CLI or the SAN Router's Element Manager.

Setting Parameters Through the CLI

The command line interface (CLI) provides options for out-of-band management of the SAN Router. You can use the commands described in the *McDATA E/OSi Command Line Interface (CLI) User Manual* (P/N 620-000207) for these operations.

CLI Procedure

To set the management port address using CLI and a serial port connection, use the following steps.

1. Use a null modem cable to connect a VT100 terminal or any standard PC running terminal emulation software to the RS-232 serial port on the SAN Router
2. Set the PC terminal emulator settings to the SAN Router default settings.

Parameter	Setting
Bits per second	9600
Data bits	8
Parity bits	None
Stop bits	1
Flow Control	None

3. Power up the terminal. Press the **Enter** key to display the CLI prompt.
4. Type *modify* at the Access Mode prompt. This is case-sensitive. Read is for read-only; modify is for read-write.
5. Type your password at the Password (community string) prompt. Use *private* as the password and press **Enter**.
6. Set the management port IP address with the following command:

```
set mgmt portadd <IP address><subnet mask>
```

   where:

   - IP address = IP address of the management port
   - subnet mask = subnet mask of the management port.

7. Enter a permanent route for a network management station using the command:

```
set mgmt permroute <addr><mask><gateway>
```

   where:

   - address = IP address of the network management subnet. This IP address is used to add a static route to the SAN Router's route table. This is required by the management station if its on a different subnet than the 10/100 interface.
   - mask = subnet mask of the network management subnet.
   - gateway = IP address of the next hop IP gateway. The gateway is a directly reachable IP router to which management traffic should be forwarded.

8. To save the configuration, at the command prompt enter:

```
save
```

9. Reset the system using the following command:

```
reset system
```

   The management IP address is now set and ready for normal operation.

10. If you require a terminal connection to the 10/100 port for out-of-band management, connect the standard RJ45 Cat 5 Ethernet cable from the LAN to the management port.

11. Ping the IP address that you entered for the SAN Router to verify network connectivity using the network management host.

    If there is no ping response, contact your network administrator to set up connectivity between the network management station and the SAN Router.

Using the Element Manager

The Element Manager is a web-based Java applet used to configure, monitor, and troubleshoot individual SAN Routers. The software is embedded in every SAN Router, so it does not need to be installed as a separate program on the management workstation for your mSAN.

Before you begin using the Element Manager, make sure that your workstation meets the requirements described in this section, that your browser is set up, and that you review the provided tips.

Workstation Requirements

Workstation requirements for the Element Manager are listed in the following table:

Table 2-1 Element Manager Workstation Requirements

	IBM Compatible Intel Pentium Class PC, 400 MHz or above with mouse, 32-bit	Sun Ultra 5 or better; 300 MHz or above, with mouse
Operating system	Windows 2003[a] Server Enterprise Edition Windows 2000 with SP4 Windows XP with SP2	Solaris 9.0 and Solaris 10.0. Refer to www.sun.com
Java Runtime Environment	JRE 1.5 and higher (provided with *SANvergence Manager*)	JRE 1.4 and later (not provided with *SANvergence Manager*)
Management Platform	None required	None required

Table 2-1 Element Manager Workstation Requirements(Continued)

	IBM Compatible Intel Pentium Class PC, 400 MHz or above with mouse, 32-bit	Sun Ultra 5 or better; 300 MHz or above, with mouse
Web Browser	Internet Explorer 6.0 or higher or Netscape 6.22 or higher	Mozilla 1.4
RAM	128 MB Minimum, 256 MB recommended	128 MB Minimum, 256 MB recommended
Monitor	SVGA (64K color) minimum, 1024 x 768 resolution	SVGA (64K color) minimum, 1024 x 768 resolution
Network Connection	TCP/IP Connection	TCP/IP Connection
Available Disk Space	50 MB for JRE v1.5 6MB for SANvergence Manager	50 MB for JRE v1.5 6MB for SANvergence Manager

a.DirectX 9.0b or later must be installed on the management workstation if additional software programs, such as EFCM or PC Anywhere, are coresident with SANvergence Manager.

Element Manager Overview

The Element Manager software configuration and monitoring functions are described in Chapters 2 through 8 of this manual.

Table 2-2 Element Manager Software Functions

Function	Configuration Options
Monitoring (Device View of SAN Router)	Device View LEDs and icons, system information icons Color indicators for operational status Message Log
SAN Router Operations (File menu)	Save Configuration Reset System Firmware Upgrade System Log Configuration Backup and Restore

Table 2-2 Element Manager Software Functions(Continued)

Function	Configuration Options
System Configuration (Configuration menu)	Operations Properties Inband Address SNMP Communities/Hosts SNMP Traps Date/Time New Device Zoning
Port Configuration (Configuration menu)	Management, FC/Ethernet (Fibre Channel, Ethernet and TCP Ports with iSCSI and/or iFCP) Advanced FC Port (E_D_TOV and R_A_TOV timeout values)
Static Routing (Configuration menu)	Static Routing
iSCSI Device Configuration (Configuration menu)	Devices RADIUS Server Configuration
iFCP Configuration (Configuration menu)	Setup Remote Connections Port Redundancy
Reports and Statistics (Statistics/Info menu)	Ping (iFCP/iSCSI) GE (Gigabit Ethernet Port statistics) Fibre Channel (Port Statistics and Device Properties) Port Traffic Statistics iFCP port Compression Rate Statistics MAC Forwarding Table Internet Protocol (IP) Forwarding Address Resolution Protocol (ARP) Table metro storage name server (mSNS) Report Remote Connection Statistics
Element Manager Operations (Options menu)	Get Write Permissions Polling Interval

Starting the Element Manager

To login to the SAN Router using the Element Manger, follow these instructions.

1. In the address field of your browser, enter the management IP address or DNS hostname of the target SAN Router (for example: 192.168.2.16), in the Address field. Some browsers may require "http://" before a hostname. The Element Manager login dialog box appears.

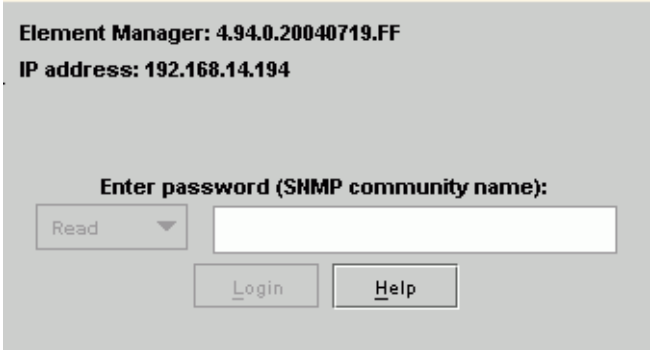


Figure 2-1 Element Manager Login Dialog Box

2. Type the access password for the SAN Router, then click *Login*.
   - The default passwords are *public* (read access) and *private* (read and write, or modify access).
   - When the password is verified, the *Element Manager Device View* appears.

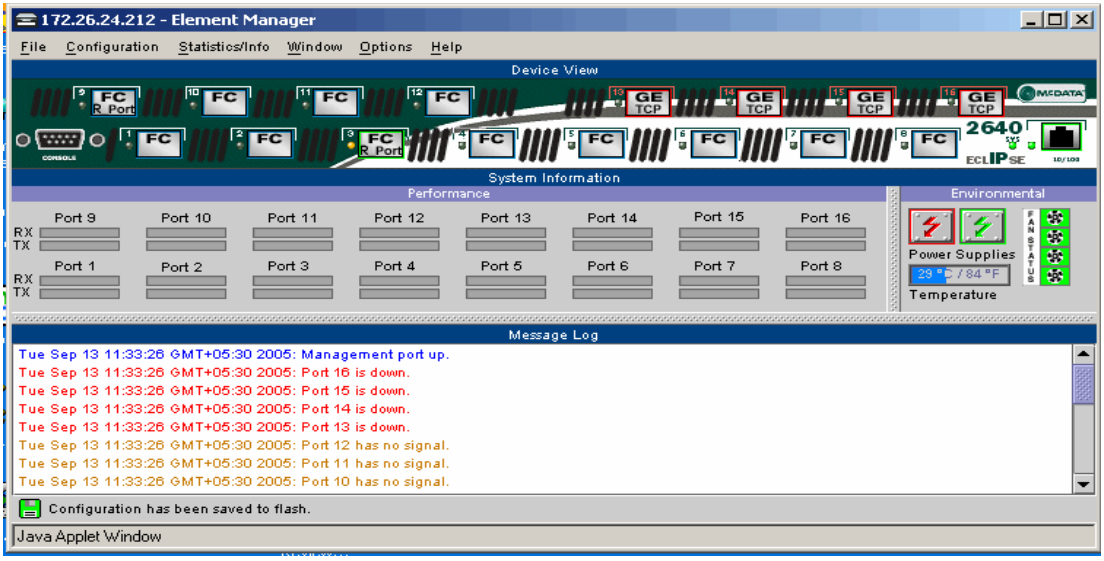


Figure 2-2 Element Manager window

You are now logged in and ready to use Element Manager.

If SANvergence Manager software is installed, click *Element Manager* button on the SANvergence screen.

Configuring the Management Port

To configure the out-of-band management port, follow these instructions:

1. Select *Configuration>Port >Management* to display the *Management Port Configuration* dialog box.

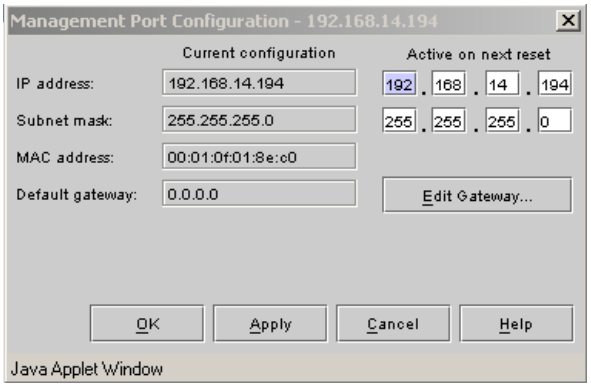


Figure 2-3 Management Port Configuration Dialog Box

2. Enter the IP address and subnet mask address for the management port.
3. Click *Edit Gateway* to add the IP address of the gateway router to the static route table if any of your management stations are on a different subnet than the one you are specifying for the management port.
4. Click *OK* or *Apply*.
5. Choose *Save Configuration to Flash* from the *File* tab to permanently save the new routing information.

Tips on using the Element Manager

Getting Help

An HTML-based help system is available with the Element Manager. You can search for text on a topic that interests you or browse help topics sequentially. To view help, choose *Index* from the *Help* menu. You can also click the *Help* button or press **F1** in a dialog box to view help customized for that dialog box.

To view version information about Element Manager, choose *About Element Manager* from the *Help* menu.

Keyboard Shortcuts

The following function keys provide keyboard shortcuts:

Table 2-3 Key Board Shortcuts

F1	Help - Displays help for the current window or dialog box.
F5	Refresh Window - Refresh main screen or a configuration dialog box.
Esc	Close the current dialog box

Getting Write Permission

You can login to Element Manager with the read-only password. However, if you attempt to configure the SAN Router from Element Manager, the following dialog box prompts you to type the modify (read/write) password.

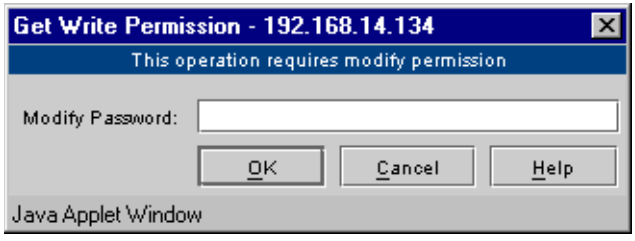


Figure 2-4 Get Write Permission Dialog box

CAUTION

Only one user at a time should be allowed to login with read and write privileges so as not to write over each other's changes.

Granting Clipboard Access for Copy and Paste

Element Manager is an unsigned Java™ applet. As such, default security settings prevent it from using the system clipboard. This means that you cannot copy and paste text between Element Manager text fields and other applications. For example, you cannot copy Element Manager's message log to another application or copy long file path names from one dialog box to another in another application.

However, you can grant clipboard access by editing the Java plug-in policy file. The policy file is named:

<plug-in-installation-directory>/lib/security/java.policy

On Microsoft Windows, the default installation directory is

- C:\Program Files\Javasoft\JRE\1.3.1 (for version 1.3.1)
- C:\Program Files\Java\j2re1.4.1 (for version 1.4.1)

So the full default file name is:

- C:\Program Files\Javasoft\JRE\1.3.1\lib\security\java.policy. (for version 1.3.1)
- C:\Program Files\Java\j2re1.4.1\lib\security\java.policy. (for version 1.4.1)

On Solaris, if the installation directory is (for example):

- /opt/JRE/1.3.1 (for version 1.3.1)
- /opt/JRE/1.4.1 (for version 1.4.1)

So the full file name would be (for example):

- /opt/JRE/1.3.1/lib/security/java.policy. (for version 1.3.1)
- /opt/JRE/1.4.1/lib/security/java.policy. (for version 1.4.1)

NOTE: Alternatively, for either operating system, you may instead edit the.*java.policy* file (note different name, with period in front) in the user's home directory. For Windows XP, the directory would be C:\Documents and Settings\<login-name>.

To grant clipboard access, follow these instructions:

1. Add the following lines at the beginning or end of the policy file to enable clipboard access for ALL Java applets:

   grant {permission java.awt.AWTPermission “accessClipboard”;};

CAUTION

The security risks in granting clipboard access to all applets are:

- **An applet could read the clipboard contents and send them to a remote server. If you have recently cut and pasted sensitive information, this could be a privacy risk.**
- **A malicious or malfunctioning applet could fill the system clipboard with very large amounts of data, consuming available disk space on your system.**

2. Add these lines to the policy file to limit clipboard access to Element Manager only:

   grant codeBase “http://<ip-address-or-hostname>/top/*” {permission java.awt.AWTPermission “accessClipboard”;};

   where <ip-address-or-hostname> is the address or DNS name used in the web browser for the SAN Router. You must repeat the lines above for each SAN Router in your network.

3. Restart your web browser to read the new policy file.

Using with Third-Party Browser Extensions

In some cases, the Element Manager cannot be started from a web browser when a third-party browser extension prevents the JRE plug-in from loading Element Manager.

If Element Manager cannot start, disable third-party extensions. Internet Explorer 6.0 allows you to enable or disable third-party extension support.

1. Select *Internet Options* under the *Tools* menu in Microsoft® Internet Explorer.
2. Click the *Advanced* tab.
3. Under *Browsing*, disable *Enable third-party browser extensions*, if enabled.
4. Restart your computer.

The Windows XP Service Pack 2 provides the ability to individually enable or disable an extension (now called an add-on) in Internet Explorer without entirely disabling third-party extension support. The FireFox 1.0 browser also supports this feature.

Using Configuration Dialog Boxes

Selecting an option displays a dialog box where you can modify configuration data. Click *OK*or *Apply* in each dialog box to save the changes.

Apply sets the changes to the SAN Router. The changes are stored in memory only on the SAN Router, not to flash. *OK* is similar to *Apply* but also dismisses the dialog box after setting the configuration parameters. Pressing **F5** will force a refresh of the dialog box. Any uncommitted changes will be lost.

To permanently save your changes to the runtime configuration, you must choose *Save Configuration* from the *File* tab.

This saves the currently running configuration to flash memory. Whenever you choose *Reset System* from the *File* tab, the configuration in flash is restored to the SAN Router.

NOTE: If the configuration has not been saved to flash, a red diskette icon appears in the bottom left corner of the Device View with a message that changes are not saved to flash (Figure 2-2 on page 2-9). A green icon indicates changes have been saved.

Configuring IP Addresses

SAN Routers use the iFCP and iSCSI protocols, which use IP addresses for all routing and forwarding of storage traffic. Using the iFCP/iSCSI protocol, all Fibre Channel addresses are mapped to one or more IP addresses.

You must configure two IP addresses with SAN Routers: the external iFCP/iSCSI network and the IP network. When sending storage traffic to the external network, SAN Routers uses the "external" IP addresses associated with the TCP ports. When sending storage traffic to the internal network, the SAN Routers use the *inband address* as the source address for the storage traffic.

Figure 2-5 shows external and internal storage networks. Traffic sent to the "external" network uses TCP ports, while traffic sent to the "internal" network uses Fibre Channel ports.

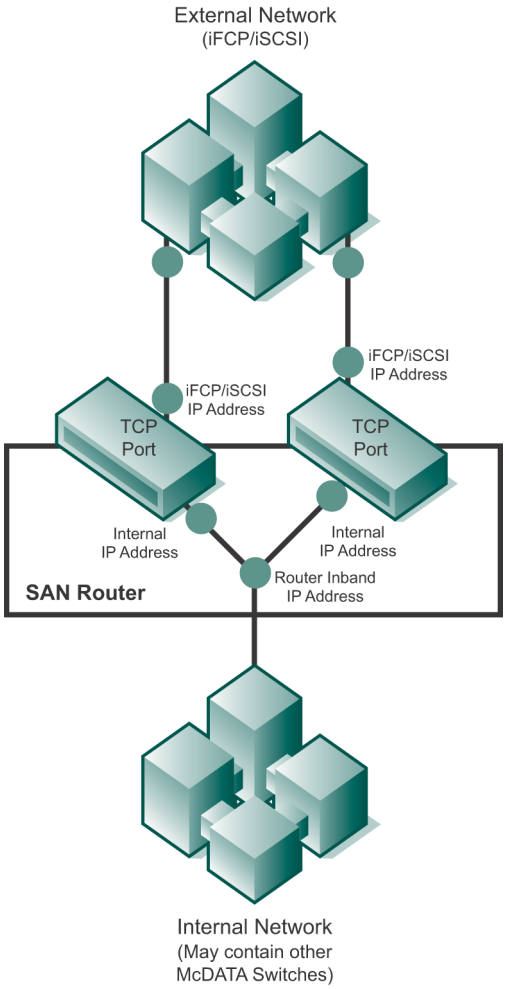


Figure 2-5 Internal and External IP Addresses

A SAN Router has iFCP/iSCSI ports that are connected to the external IP network, and one or more ports that are connected to the internal IP network. Each TCP port connects to each network (both the internal and external networks) as an independent device. The TCP port uses the iFCP/iSCSI IP address to talk to the external network and the internal IP network IP address to talk to the internal network.

The Figure 2-5 shows the role and position of each IP address relative to the internal and external IP networks.

The Router Inband IP Address

The router inband IP address is used for the internal delivery of storage traffic.

To configure the SAN Router inband address, use *Configuration>System>Inband Address* in the Element Manager.

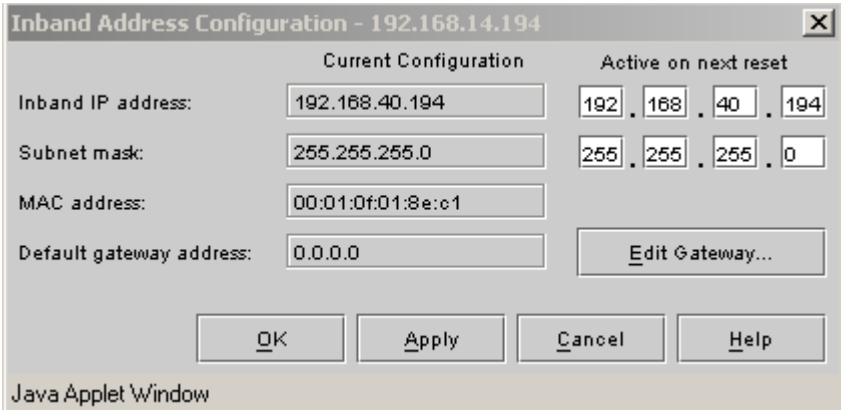


Figure 2-6 Inband Address Configuration Dialog Box

The iFCP/iSCSI Port IP Address

The "external" iFCP/iSCSI port IP address is used to open and terminate TCP connections that transport storage data over the external IP network. Storage traffic received at the iFCP/iSCSI port IP address can be either delivered to a device directly attached to the SAN Router or to another SAN Router somewhere in the internal network.

The iFCP/iSCSI port IP address is configured as the *IP address* in the *iSCSI/iFCP Parameters* section of the *Port Configuration* dialog box (Figure 2-7.)

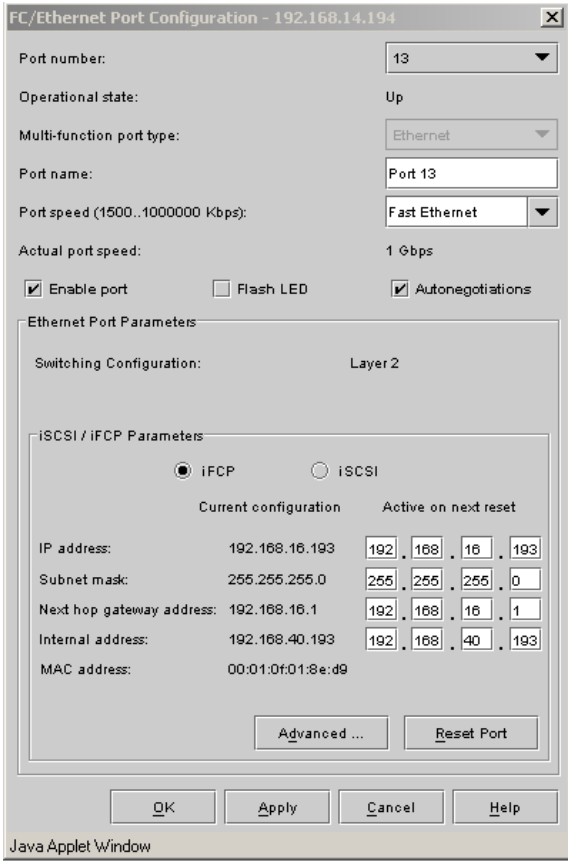


Figure 2-7 FC/Ethernet Port Configuration Dialog Box

The Next Hop Gateway IP Address

The iFCP/iSCSI ports interact with the external IP network as if they were independent IP hosts. Each iFCP/iSCSI port needs a gateway address of an external router that can forward the storage traffic to the remote iFCP/iSCSI port. This *Next Hop Gateway Address* is the first-hop gateway address. If the IP address of the remote iFCP/iSCSI port is in a different subnet from the local iFCP/iSCSI port, then you must configure the *Next Hop Gateway Address*. If the remote iFCP/iSCSI port is on the same subnet as the local iFCP/iSCSI port, then the *Next Hop Gateway Address* field is not used and does not need to be configured.

The Internal IP Address

Storage traffic that is to be transported through the external network by iFCP or iSCSI must first be delivered to the iFCP/iSCSI port that will perform the iFCP/iSCSI encapsulation. The internal IP address is used by the iFCP/iSCSI port to receive this storage traffic from the internal network. This traffic is then re-addressed and re-encapsulated into an iFCP/iSCSI connection that traverses the external network.

Because the internal IP address is local to the SAN Router, it *must* be on the same subnet as the router inband IP address. Storage traffic from devices directly connected to the SAN Router is delivered from the router inband IP address to the internal IP address through Ethernet, before it is re-encapsulated into iFCP/iSCSI for transport through the external network. Similarly, storage traffic received by the iFCP/iSCSI port from the external network will be re-encapsulated using the internal IP address as the source address. This traffic can then be addressed locally to the router inband IP address.

Figure 2-8 on page 2-20 shows an iFCP/iSCSI port IP address configuration, including the iFCP/iSCSI IP address, the *internal address*.

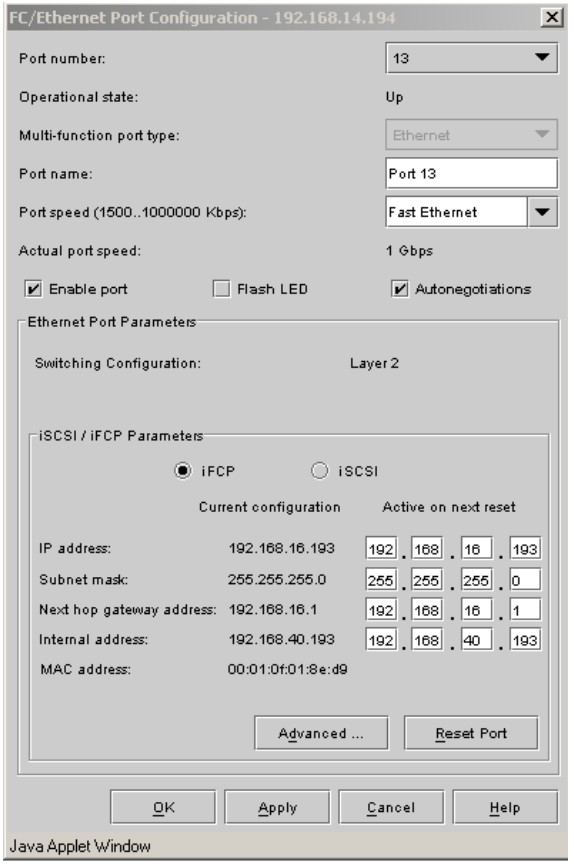


Figure 2-8 FC/Ethernet Port Configuration Dialog Box

Guidelines When Working with Firewalls

The iFCP and iSCSI protocols use TCP for transmission. TCP provides several benefits such as:

- Retransmission of any packets dropped by the network.
- Guaranteed in-order delivery.
- Fields that are leveraged by firewall devices for added security.

Prior to transmitting data, TCP must first establish a connection between the TCP sender and the TCP receiver. Only after a

connection is established are the TCP segments allowed to be transmitted from the sender to the receiver.

A firewall can be used to block the establishment of TCP for some applications while permitting other applications to transmit data. To accomplish this, firewalls frequently use a combination of TCP port numbers and IP addresses. Port numbers are used to identify the sending and receiving application. The port number, along with the source and destination IP addresses, uniquely identifies each connection. The TCP header contains two 16 bit fields for the source port number and the destination port number.

When firewalls are used, it is sometimes necessary to program the firewall with the port numbers used by iFCP or iSCSI; otherwise the firewall may block the traffic. The following are guidelines for iFCP and iSCSI TCP ports and firewalls:

Port Numbers Used by SAN Routers

- These iFCP TCP ports must be opened across the network when working with firewalls:

  E/OSi Firmware: 3.X and above
  Control Data -
  hex: 9101 decimal: 37121
  hex: 9102 decimal: 37122

  Data -
  hex: D5C decimal: 3420

- These iSCSI TCP ports must be opened across the network when working with firewalls:

  E/OSi Firmware: All
  Control and Data -
  hex: CBC decimal: 3260

Open Ports

The following datapath ports must be open if you want to manage across a firewall using Element Manager:

- HTTP (80)
- SNMP Protocol (161)
- SNMP Traps (162)
- iSCSI and iFCP information (37009)

- Ping operation results (37010)

The following datapath ports must be open if you want to manage across a firewall using SANvergence Manager:

- SNMP Protocol (161)
- SNMP Traps (162)

Configuring System Operations

Configuring the system operations of a SAN Router involves the following steps:

1. Configuring the system properties
2. Setting the system date and time
3. Setting the SAN Routing Cluster ID
4. Configuring SNMP
5. Configuring the system IP Addresses and static routes
6. Configuring System Metro Storage Name Server (mSNS)
7. Configuring new device zone settings

These steps are described in the following sections.

Configuring System Properties

To configure the system properties, follow these instructions:

1. Choose *Configuration>System>Properties* to display the *System Properties* dialog box (Figure 2-9 on page 2-24).

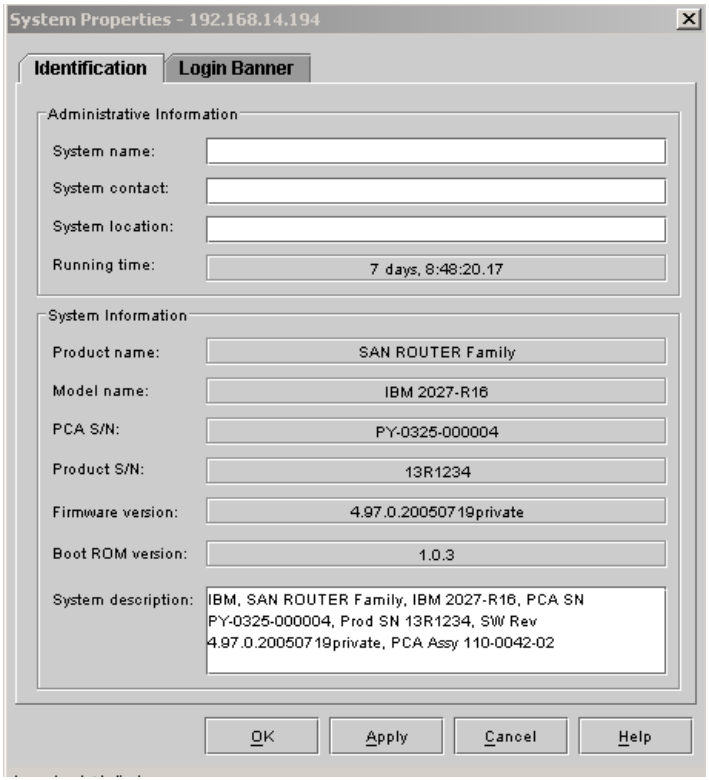


Figure 2-9 System Properties Dialog Box

2. Login banner lets you customize the banner which gets displayed in the HTML starting page above the login dialog box. The banner may be up to 25 lines long with up to 80 characters per line.

NOTE: The banner is also shown before the CLI and Telnet session login prompts.

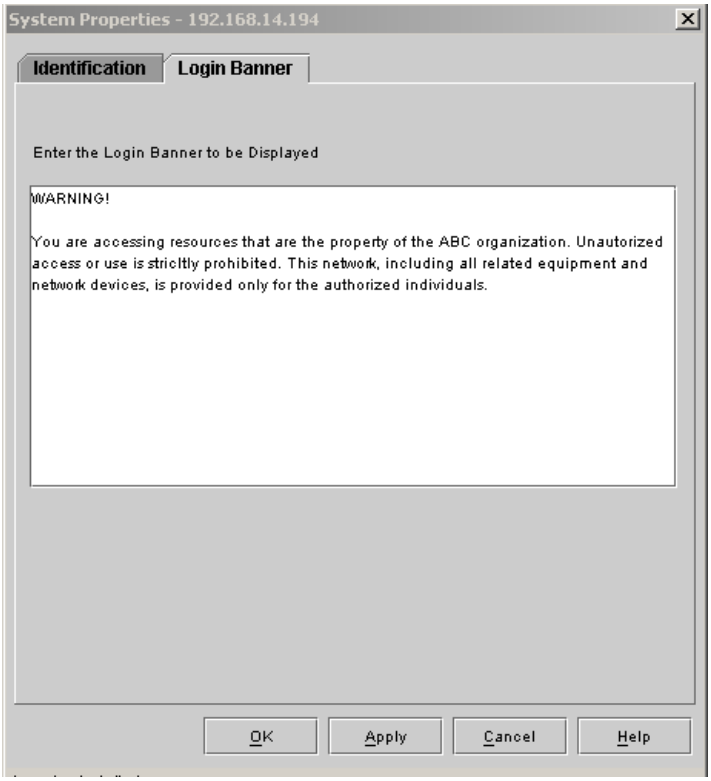


Figure 2-10 Login Banner

3. Click *OK* or *Apply*.
4. Choose *Save Configuration* from the *File* tab to permanently save your changes to the runtime configuration. This saves the currently running configuration to flash memory.

Setting the SAN Routing Cluster ID

The R_Port SAN Routing Cluster ID is used by the SAN Router R_Ports to register a unique virtual node WWN to the connected fabrics. Third-party management applications use this WWN to manage the SAN Router. Each SAN Router is its own single-member cluster. Each SAN Router connected to an mSAN must have a different cluster ID.

The values set take effect only after the SAN Router R_Ports are disabled and enabled (re-initialized).

NOTE: Changing the cluster ID changes the registered virtual switch node WWN. This may require the management applications to re-discover the SAN Router.

Procedure

To set the cluster ID, follow these instructions:

1. Select *Configuration>System>Operations* to display the *System Operations* dialog box.

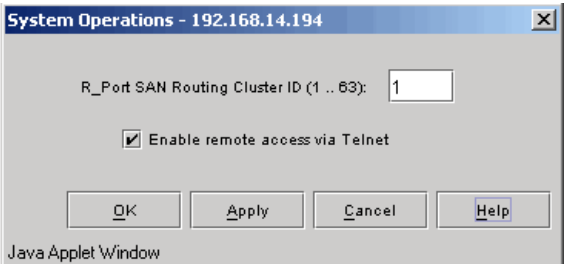


Figure 2-11 System Operations Dialog Box

2. Enter a number for the cluster ID, in the range 1-63.
3. If you want to enable remote access via Telnet, select the option.
4. Click *OK* or *Apply*.
5. Choose *Save Configuration* from the *File* tab to permanently save your changes to the runtime configuration. This saves the currently running configuration to flash memory.

Configuring System Date and Time

To configure the system date and time from the SAN Router's clock and configure Simple Network Time Protocol (SNTP), follow these instructions:

1. Select *Configuration>System>Date/Time* to display the *Date/Time* dialog box.

   The *Date/Time* dialog box displays the current date and time from the SAN Router's clock as shown in Figure 2-12.

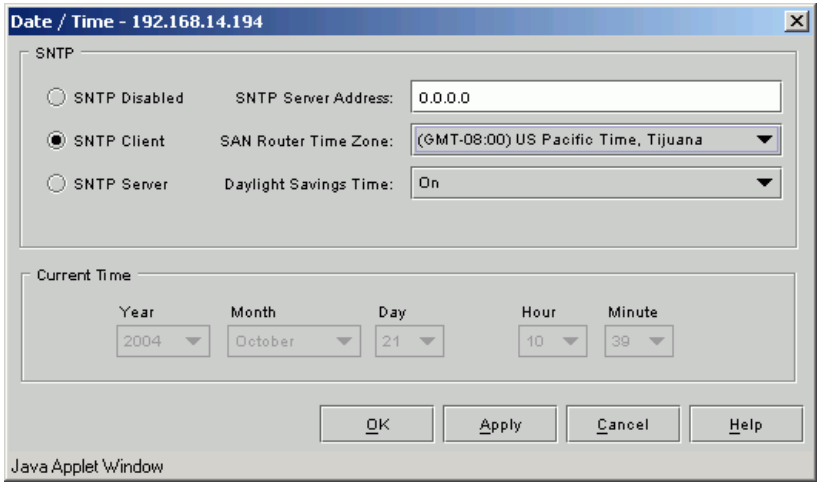


Figure 2-12 Date/Time Dialog Box

2. Select the SNTP operating mode for the SAN Router's internal clock.

   - *SNTP Disabled* - Select this mode to allow the SAN Router to keep time using its own internal clock. With this selected, you can set the time manually under the *Current Time* section, using GMT or local time.
   - *SNTP Client* - Select this mode to allow the SAN Router clock to resynchronize with an external SNTP server each minute. The SNTP server may be another SAN Router, corporate server, or even an internet sever if internet access is available.

     SNTP Server Address - Enter the IP address of the external sever.

SAN Router Time Zone - Select a time zone from the drop-down list.

Daylight Savings Time - Select *On* or *Off* from the drop-down list if daylight savings time pertains to your time zone. The SAN Router does not automatically change this setting when daylight savings time begins or ends. You must update this setting manually.

- *SNTP Server* - Select this mode to set the SAN Router as an SNTP server. In this mode, the SAN Router keeps time with its internal clock and provides this time to SNTP clients. Set the SAN Router's date and time manually using the drop-down lists in the *Current Time* section.

  SAN Router Time Zone - Select a time zone from the drop-down list. Specifying the SNTP server's time zone allows SNTP clients to adjust the time to their local time zone as needed.

  Daylight Savings Time - Select *On* or *Off* from the drop-down list if daylight savings time pertains to your time zone. The SAN Router does not automatically change this setting when daylight savings time begins or ends. You must update this setting manually.

3. Specify the correct date and time if you have selected *SNTP Disabled* or *SNTP Server*.
4. Click *OK* to apply.
5. Choose Save *Configuration to Flash* from the *File* tab to permanently save your changes to the runtime configuration. This saves the currently running configuration to flash memory.

Configuring the Router Inband and Gateway Address

NOTE: In Element Manager, the default gateway is represented as a "default route" in the routing table by specifying a destination address and a mask of "0.0.0.0". That is, all traffic not matching a more specific entry in the routing table will be sent to the "next hop" listed in the default route. The default route and the default gateway address are the same thing.

Configuring the Router Inband Address

To configure the SAN Router's internal "router inband" address through the Element Manager, follow these instructions:

1. Select *Configuration>System>Inband Address* to display the *Inband Address Configuration* dialog box (Figure 2-13).

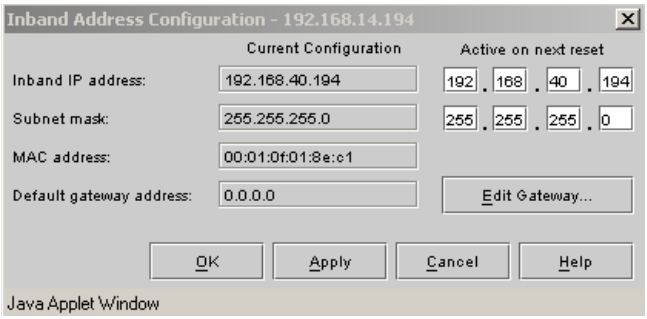


Figure 2-13 Inband Address Configuration Dialog Box

2. Type the new IP address.
3. Type the new subnet mask address. The subnet mask is the number of bits that defines the network address in a given IP address.

NOTE: The SAN Router "inband" address is different from the management port IP address and must be on a different subnet. Having them in the same subnet may cause the SAN Router to become isolated from the backbone network.

---

4. The default gateway address is shown for convenience. The gateway address is the IP address of a directly reachable SAN Router to which routed traffic should be forwarded. To change the default gateway, click the *Edit Gateway* button to display the *Static Route Configuration* dialog. For more information, refer to *Static Routes* on page 2-36.
5. Click *OK* or *Apply*. The new inband address takes effect after you reset the SAN Router. New default gateway addresses take effect immediately.
6. Choose *Save Configuration to Flash* from the *File* tab to permanently save your changes to the runtime configuration.

Configuring SNMP

To configure the SNMP communities and hosts, follow these instructions:

1. Select *Configuration>System>SNMP Communities/Hosts* to display the *SNMP Communities/Hosts* dialog box (Figure 2-14 on page 2-30).

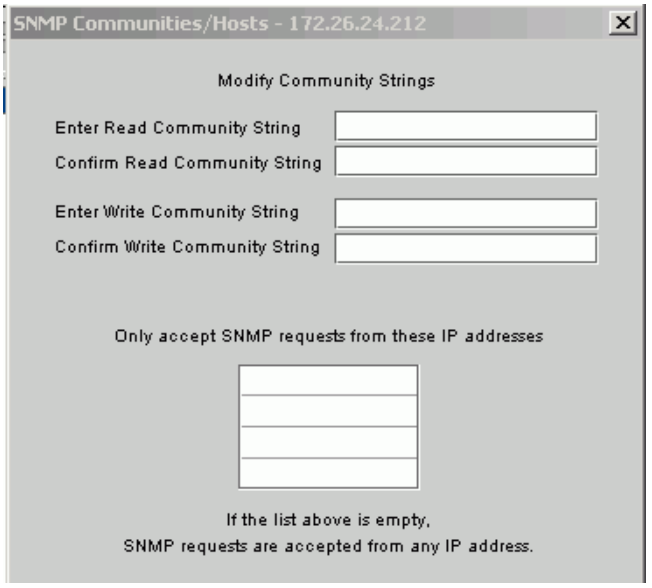


Figure 2-14 SNMP Communities/Hosts Dialog Box

2. Type the read-only password and read-modify password (community strings) for the SAN Router.
3. Optionally, enter a list of IP addresses from which the SAN Router is authorized to accept SNMP requests.
   - If you leave the list empty, SNMP requests are accepted from any management station.
   - If you make at least one entry in the table, SNMP requests are accepted only from addresses included in the table.
4. Click *OK* or *Apply*.

5. Choose *Save Configuration* from the *File* tab to permanently save your changes to the runtime configuration. This saves the currently running configuration to flash memory.

Configuring System SNMP Traps

The SAN Router sends SNMP traps to notify the management station of certain events. Traps can be triggered by one or more events.

Trap Types

The following tables describe SAN Router events that trigger specific SNMP traps. The SAN Router sends SNMPv1 format traps to inform management stations of certain events. Each trap sent by the SAN Router is assigned one of 3 severity levels: Info, Warning, or Critical. The SAN Router may be configured to filter generated traps by severity.

Table 2-4 Generic SNMP MIB-II traps, from RFC 1213

Trap	Name	Description	Severity
0	Cold Start	The SAN Router is powered on, or rebooted.	Critical
2	Link Down	An Fibre Channel port has lost an active link signal. This can also be caused by manually disabling an active port.	Critical
3	Link Up	An Fibre Channel port acquires an active link signal. The port must have been previously enabled to acquire an active link signal.	Info
4	Authentication	Authentication failure from receiving SNMP command with incorrect community string.	Warning

Table 2-5 RMON Traps, from RFC 1757, Enterprise 1.3.6.1.2.1.16

Trap	Name	Description	Severity
1	Rising Threshold	When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event will be generated.	Info
2	Falling Threshold	When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single event will be generated.	Info

Table 2-6 Fibre Alliance traps, enterprise 1.3.6.1.3.94

Trap	Name	Description	Severity
1	Conn Unit Status Change	Sent when the status of a power supply or fan changes.	Info
6	Port Status Change	A port status has changed. Sent when a port is enabled or disabled, or the link goes up or down.	Info (if port up) Critical if port disabled or down.

Table 2-7 McDATA Eclipse traps, enterprise 1.3.6.1.4.1.4369.3

Trap	Name	Description	Severity
1	SNS Server	The SAN Router has become the primary SNS server.	Info
3	Firmware Loaded	A new firmware image has completed a TFTP download to flash memory.	Info
5	Voltage Too High	A power supply voltage has exceeded its rated maximum value.	Critical
6	Voltage Too Low	A power supply voltage has dropped below its minimum allowed value.	Critical
7	Temperature	The SAN Router's internal temperature has exceeded the rated maximum.	Critical
8	Fan Failed	One or more fans have failed in the SAN Router.	Warning
9	Power Supply Changed State	A power supply has changed state from up to down or down to up.	Warning
14	iFCP Backup Not Ready Warning	Sent when a primary iFCP port cannot be backed up by its configured backup port. The backup port may be unreachable or not responding, or the backup port may be unable to act as backup due to its configuration. This trap may be sent after the SAN Router is reset, when the configuration is changed, or when an existing backup port becomes unreachable. This trap repeats when the backup connection is tried again unsuccessfully. There is no interruption of storage traffic, but the primary iFCP port is no longer protected from failure. The text message in the variable binding list includes the IP address of the primary iFCP port that cannot be backed up, and the IP address of the port configured to be the backup. The cause of the failure (such as timeout, rejected, or incorrect configuration) is not provided. There is no trap sent when the backup relationship is established successfully or re-established successfully.	Warning

Table 2-7 McDATA Eclipse traps, enterprise 1.3.6.1.4.1.4369.3 (Continued)

Trap	Name	Description	Severity
15	iFCP Backup Activated	Sent when a backup iFCP port begins to activate its backup connections. This may be caused by the primary port becoming unreachable or the primary port informing the backup port that the primary link has gone down. The backup port will attempt to establish all remote connections learned from the primary port. If there are any learned connections, this trap will be followed by traps, such as trap number 15 and 16, to indicate the success or failure of each remote connection. The text message in the variable binding list of this trap includes the IP address of the primary port that has failed and the IP address of the backup port that is reporting the primary port's failure. This trap is not generated in release 4.5.	Critical
16	iFCP Link Up	Sent when an iFCP port successfully establishes an iFCP connection to a remote mSAN. If the port makes multiple remote connections, one trap is sent for each connection. The connection may be a normal connection or a backup connection. The text message in the variable binding list includes the IP address of the iFCP port making the connection and the IP address of the remote end of the connection.	Info
17	iFCP Link Down	Sent when an existing remote connection is lost or terminated normally or when a connection attempt fails. If multiple connections are lost or terminated or multiple concurrent connection attempts fail, one trap is sent for each connection. This trap repeats when connection retries fail. The text message in the variable binding list includes the IP address of the local iFCP port making the connection and the IP address of the remote end of the connection. This trap does not specify the reason for the connection being down (such as timeout on existing connection, user configuration change, or remote end rejects connection).	Critical
18	R_Port Change	An R_Port's configuration has been changed by the user.	Info
19	FC Zone Change	An R_Port has applied zoning changes to fabric.	Warning
20	R_Port Down	An R_Port could not connect to its attached fabric.	Critical
21	R_Port Fabric Change	The fabric attached to an R_Port has been rebuilt. This may occur if an Fibre Channel switch or R_Port is added or removed from the fabric.	Warning

Configuring Trap Recipients

To configure the SNMP trap recipients, follow these instructions.

1. Select *Configuration>System>SNMP Traps* to display the *SNMP Traps* dialog box (Figure 2-15 on page 2-34).

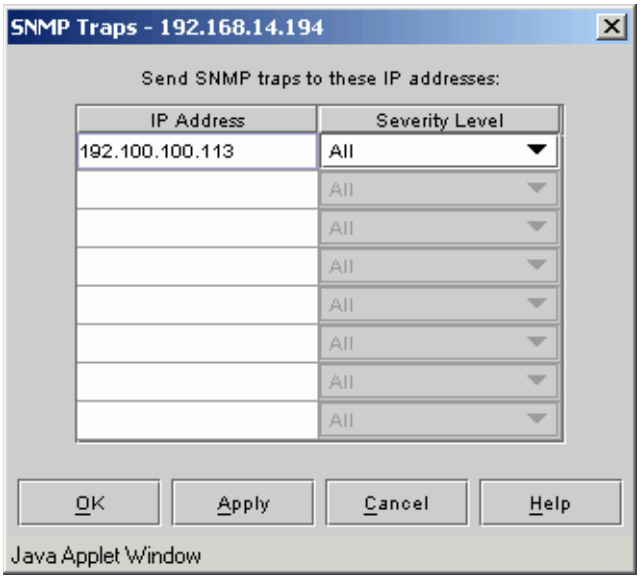


Figure 2-15 SNMP Traps Dialog Box

2. Configure up to eight (8) trap receivers, each with a severity filter. Use the severity level drop down list to specify the traps with specific severity levels that should be sent to each address.

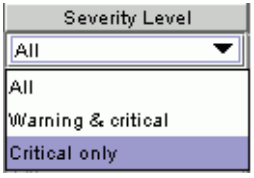


Figure 2-16 SNMP Traps Filter Pull Down Menu

3. Click *OK* or *Apply*.
4. Choose *Save Configuration* from the *File* tab to permanently save your changes to the runtime configuration. This saves the currently running configuration to flash memory.

Configuring mSNS

The SAN Router's metro storage name server (mSNS) stores the inventory of hosts and storage devices in the mSAN as well as zoning information, to specify which hosts can use which storage devices.

SAN Router discovers the Inventory information automatically. You can view inventory information for locally attached devices by selecting *Storage Name Server* from the *Statistics/Info* tab. For more information, refer to *Viewing Statistics* on page 6-14.

Configuring New Device Zoning

By default, all new devices attached to the SAN Router, including router-attached devices (RADs), are unzoned. They are not part of any zone and cannot talk to any other device. Initially, they are not even part of the default zone (zone 1). You must explicitly assign new devices to zones.

To change the default zone behavior:

1. Select *Configuration>System>New Device Zoning* to display the *New Device Zoning* dialog box (Figure 2-17 on page 2-35).

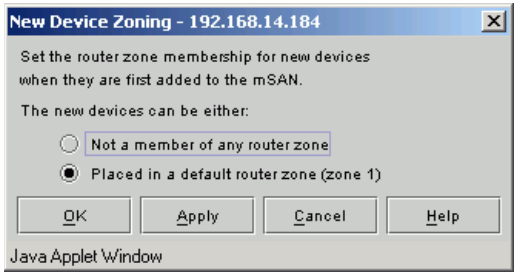


Figure 2-17 New Device Zoning Dialog Box

2. Click *Not a member of any zone* to reinstate the factory default.

   All new devices will be unzoned, isolated devices that do not have connectivity with any other zoned or unzoned devices. Some Fibre Channel HBAs do not interact well when placed in a common zone, due to vendor unique practices.

3. Click *Place in a default router zone (zone 1)* to place all new devices in the default zone (zone 1) where they can communicate with each other.
4. Click *OK*.
5. Choose *Save Configuration* from the *File* tab to permanently save your changes to the runtime configuration. This saves the currently running configuration to flash memory.

Static Routes

Static routes are used to route non-storage payload traffic, such as management traffic or RADIUS. A SAN Router contains several different IP subnets:

- The iFCP/iSCSI ports on a unique subnet, or subnets.
- The management port on a unique subnet (the management subnet can be the same subnet as an iFCP/iSCSI port, but this is not recommended).
- The internal IP network on a unique subnet.

NOTE: Changes to the permanent route are not active until after the next SAN Router restart, but changes to other static routes take effect immediately.

Refer to Figure 2-18.

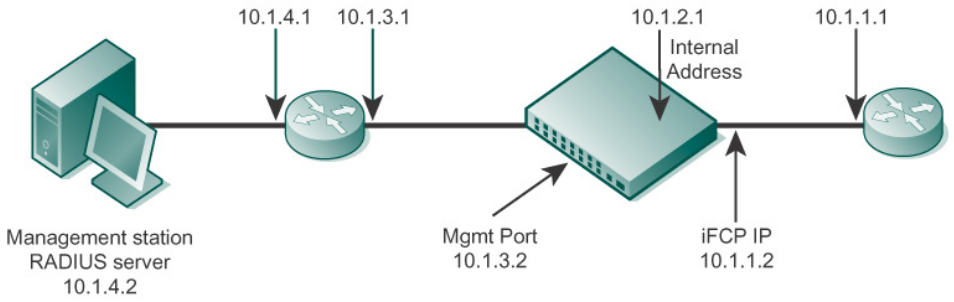


Figure 2-18 Static Route

If the SAN Router is responding to an IP packet that originated from, for example, the SNMP management station on 10.1.4.2, then it needs to be told to route the response over the management port to the SAN Router 10.1.3.1. Static routes are used for this purpose. An entry is made in the static route table telling the SAN Router to route all traffic destined to 10.1.4.1 (the IP mask is included to define a range of addresses) to the next hop SAN Router, 10.1.3.1.

The SAN Router supports three types of static route entries: a standard entry, a default gateway entry, and a permanent route entry. All of these entries are stored in flash memory and restored after the system is reset.

The permanent route is intended for management traffic and is listed separately on the bottom of the *Static Routing Configuration* dialog box (Figure 2-19 on page 2-38). A permanent route differs from a standard static route because it cannot be deleted and remains present even when the system is reset to the factory defaults. Use this route for traffic to your primary network management station to ensure management connectivity even when the system is reset to the factory defaults.

A default route is a static route with a mask of 0.0.0.0 (meaning all traffic). The default route is used if no other route matches the destination address. The default route is also called the "default gateway."

Traffic that matches more than one route entry will be routed using the entry with the longest (most specific) subnet mask. Therefore, the default route will only be used to route traffic that is not otherwise defined in the static route table.

To manually enter routes, follow these instructions:

1. Select *Configuration>Static Routing* to display the *Static Routing Configuration* dialog box.

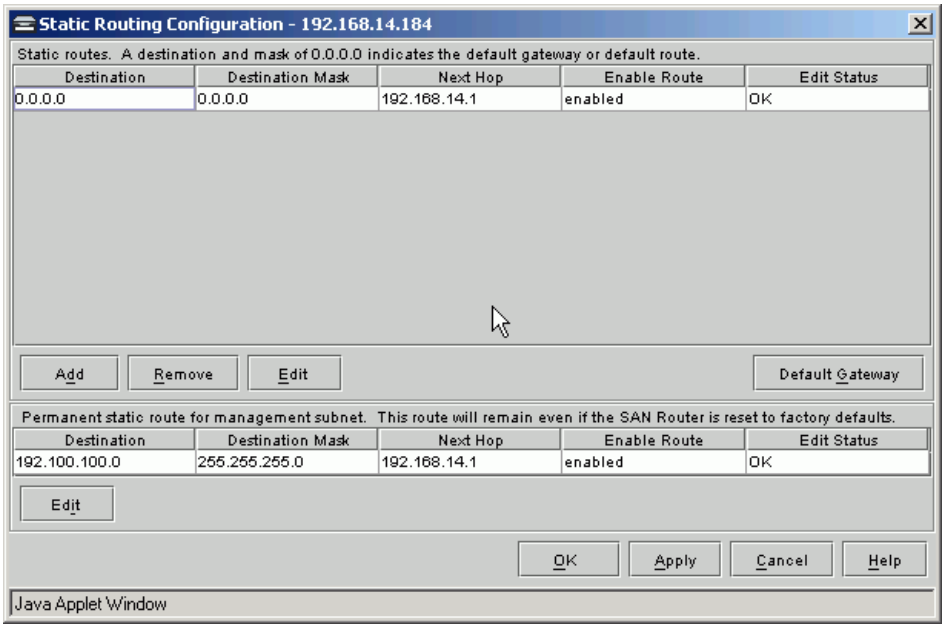


Figure 2-19 Static Routing Configuration Dialog Box

NOTE: Use the lower portion of this dialog box to create a permanent static route to the subnet where your management workstation(s) reside. For more information, refer to *Configuring the Management Port* on page 2-9.

- *Destination IP* is the IP address of the destination subnetwork.
- *Destination IP Mask* is the subnet mask of the destination subnetwork.
- *Next Hop* is the directly-reachable IP address to which the traffic should be forwarded.
- *Enable Route* is a field you can set to *Enabled* or *Disabled*. The default is *Enabled*. This allows you to create a route, disable it and enable it when needed.
- *Edit Status* (along with row color) defines the configuration state. In a table with multiple entries, a row may say edited, added or deleted. When you add a new static route, the entry

status is *Added Not Applied* and the row is green. If you select an entry to be removed, the entry status is *Removed Not Applied* and the row is red.

Important Notes for Static Routes

If the SAN Router is to be managed from a single external subnet, follow the directions under *Static Routes*.

There are two ways to manage an SAN Router if different management stations reside in different subnets.

1. Define static routes for each management subnet as described in *Static Routes*.
2. Add a default route by clicking on the *Default Gateway* in the *Static Routing Configuration* dialog box to add the route as the *Static route next hop*.

Adding a Route

1. Click *Add* to display the *Static Routing Parameters* dialog box.

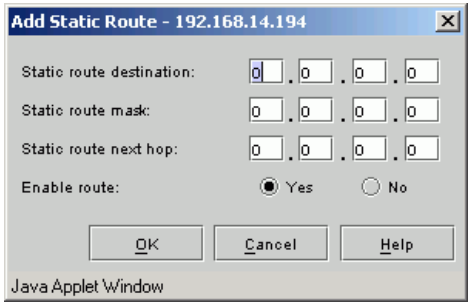


Figure 2-20 Add Static Route Dialog Box

2. Click *Yes* if you wish to enable the route.
3. Type values for the remaining parameters on the dialog box (refer to Table 2-8.:

Table 2-8 Static Routing Parameters

Item	Meaning
Static Route Destination	Defines the destination subnetwork of the traffic to be routed by the static route entry.
Static Route Mask	Coupled with the Static Route Destination, the Static Route Mask defines the destination subnetwork of the traffic to be routed by the static route entry.
Static Route Next Hop	The directly-reachable IP address where the traffic routed by the entry should be forwarded.

4. Set the *Default Gateway* or *Default Route* by entering a destination and mask of 0.0.0.0.
5. Click *Apply* or *OK*.
6. Choose *Save Configuration to Flash* from the *File* tab to permanently save your changes to the runtime configuration. This saves the currently running configuration to flash memory.

Editing a Route

1. Select an entry in the table.
2. Click *Edit*.
   - A non-default route may only be enabled or disabled. To change any other field, remove the old route and add a new one.
   - The default route cannot be disabled, but the next hop (default gateway) may be changed at any time.
   - Click the *Default Gateway* button as a shortcut method to add or edit the default route.
3. Click *Apply* or *OK*.

Removing a Route

1. Select an entry in the table.
2. Click *Remove*.
3. Click *Apply* or *OK*.

3

Configuring RADs and mSAN Connections

This chapter provides steps for configuring the SAN Router and its Fibre Channel ports for attaching directly to Fibre Channel devices, such as servers and storage.

Use the following links to move through the chapter.

Introduction

You can configure the SAN Router ports for connecting to Fibre Channel devices directly attached to the SAN Router. These devices, such as servers and storage devices, are called router-attached devices (RADs). You can also configure the R_Port to attach to fabrics that are interconnected by one or more SAN Routers.

R_Port is a fabric extension port used to establish inter-switch links (ISLs) between a SAN Router and Fibre Channel switches. R_Port allows you to interconnect, zone and manage existing fabrics with mSANs. Implementation of R_Port is FC-SW-2 compliant and can interoperate with other FC-SW-2 compliant fabrics. The Eclipse 2640 R_Port implementation also works with Brocade's pre-FC-SW-2 E_Port implementation.

When a SAN Router is connected to a fabric (Fibre Channel switches) through R_Ports, the SAN Router and Fibre Channel switches exchange standard Fibre Channel information, compliant with the standard FC-SW protocol. Additional device information is exchanged when other configuration steps are complete, as specified in the *SANvergence Manager User Manual*.

mSANs

An mSAN is a collection of one or more fabrics interconnected by a SAN router, where all the fabrics are within a data center or in different data centers that are within the metro area. An mSAN is characterized by low latency, high quality and high bandwidth ISLs such as those found within the data center or within the metro area using technologies such as dark fiber, xWDM, MAN services, etc.

Eclipse 2640 SAN routing done within an mSAN is referred to as mSAN Routing or SAN Routing within the data center. An mSAN may be referred to as a local mSAN within the context of its own mSAN, while all the other mSANs that it is communicating with are referred to as remote mSANs.

Port Configuration Tips

- To directly attach a SAN Router to an Fibre Channel device, such as a Fibre Channel server or storage, configure the ports 1-12 as Fibre Channel (FC) ports. For details, refer to the next section, *Configuring the FC Ports for Router-Attached Devices* on page 3-4.

- To directly attach a SAN Router to an Fibre Channel switch, configure the ports 1-12 as a R_Ports. For details, refer to *Configuring R_Ports for mSANs* on page 3-6.
- Configuring and Managing Zones in R_Port Connected Networks - SANvergence Manager Version 4.7 or higher is required to manage zones for R_Port connected networks. For detailed information on R_Port zone management, refer to the *SANvergence Manager User Manual*.

Configuring the FC Ports for Router-Attached Devices

This section describes how to configure the Fibre Channel ports on the SAN Router as R_Ports for attaching directly to an Fibre Channel device. To configure R_Ports for attaching to an Fibre Channel switch (mSAN), refer to *Configuring R_Ports for mSANs* on page 3-6.

1. Select *Configuration>Port>FC/Ethernet* to display the *FC/Ethernet Port Configuration* dialog box (Figure 3-1 on page 3-4).

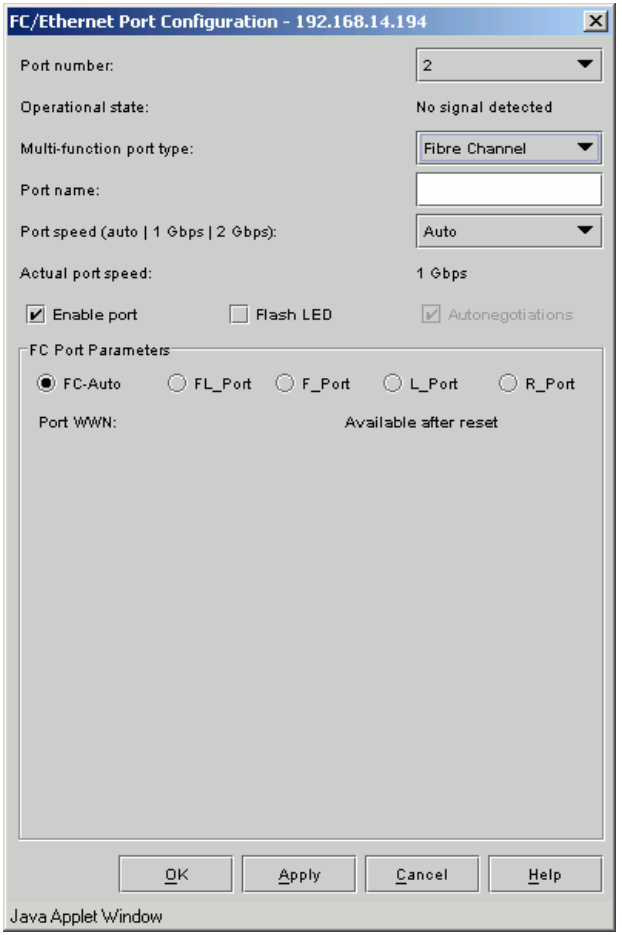


Figure 3-1 FC/Ethernet Port Configuration Dialog Box

2. Select an Fibre Channel port (1-12) from the *Port number* list.

3. Type a label for this port in the *Port Name* field. This label is displayed in the port tooltip, statistics, and other dialog boxes.
4. *Port Speed*: Click the *Port Speed* list and select either *1 Gigabit*, *2 Gigabit*, or *Auto*.

   For the SAN Router, default port speed is *Auto*. With this setting, the SAN Router automatically detects the speed supported by the connection and sets it appropriately. You can manually configure the port to 1 Gb/sec or 2 Gb/sec.
5. Select *Enable Port* to enable the selected port.
6. In the Fibre Channel Port Parameters, select one of the following types to register RADs.
   - FC Auto - Ports that automatically sense whether the type of connection is F_Port or FL_Port.
   - F_Port - A port to which non-loop N_Ports are attached.
   - FL_Port - A port to which one or more NL_Ports in an arbitrated loop are attached.
   - L_Port - Private loop or Filer mode. In this mode, the port will come up in loop mode without requesting devices to do FLOGI; in other words, the connecting device is forced to be a private device. Most NAS filers need the port to be configured in this mode.

   For Fibre Channel ports, the port WWN is displayed in a read-only field.

Configuring R_Ports for mSANs

The following procedure describes how to configure an Fibre Channel port as an R_Port to attach Fibre Channel devices and mSANs.

1. Perform steps 1 through 7 under *Configuring the FC Ports for Router-Attached Devices* on page 3-4.
2. In the *FC/Ethernet Port Configuration* dialog box, select R_Port in the *FC Port Parameters* section with the *Port type*.

   The configured R_Port parameters appear in the dialog box.

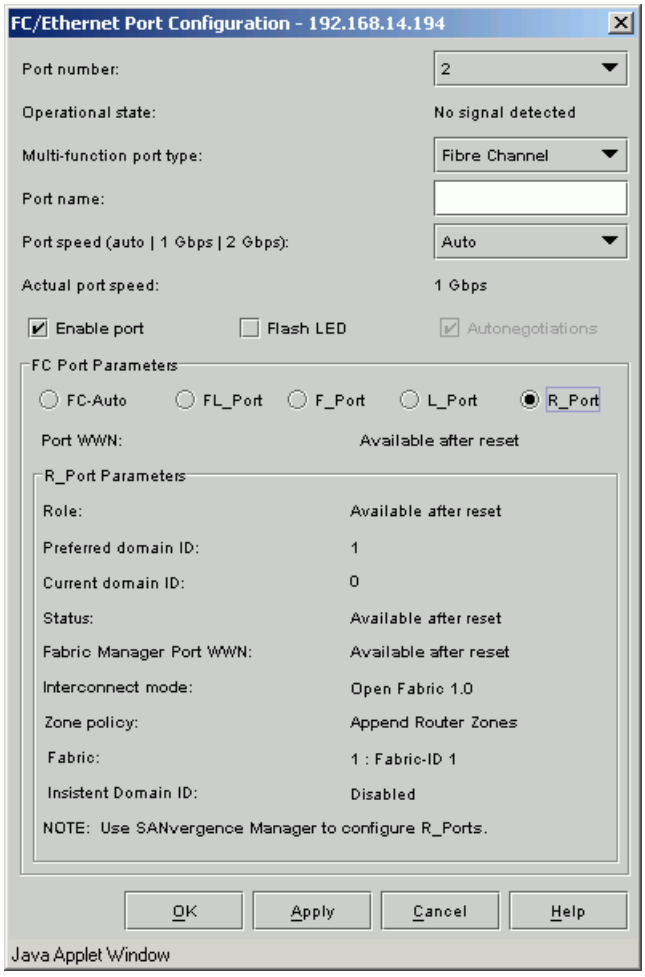


Figure 3-2 FC/Ethernet Port Configuration Dialog Box

Table 3-1 on page 3-8 describes the current R_Port parameters that may appear.

Table 3-1 R_Port Parameters

Parameter	Description
Role	The values are Fabric Manager or Non-principal. When a new Fibre Channel switch is connected and introduced to an existing fabric through use of the R_Port, an election process is initiated to determine which switch in the new fabric shall be the **principal switch**. To avoid duplicates, the principal switch is responsible for assigning and coordinating allocation of Domain IDs to every other switch in the fabric. The SAN Router will never become the principal switch. If switch needs to be rebooted, the role displays as "Available after reset."
Preferred domain ID	The Preferred Domain ID is the default domain ID for an R_Port on the SAN Router in question. An Eclipse 2640 SAN Router can have 12 R_Ports, each with its own unique Domain ID. The connected Fibre Channel switches would considers each R_Port as an individual Fibre Channel switch. The fabric may assign a different ID if necessary. This ID is a one-byte hexadecimal field used as part of the Fibre Channel Port ID address, which is maintained by the mSNS in the mSAN. The allowed range depends on the Interconnection Mode setting described below. • For Brocade mode: 1 to 239. 126 and 127 are reserved. • For Open Fabric1.0 mode: 1 to 29. 30 and 31 are reserved. • For McDATA Fabric 1.0 mode: 11 to 29. 30 and 31 are reserved. Use SANvergence Manager or the CLI to set this parameter. To avoid potential problems with certain fabric topologies, the following domain ids are not allowed:
Current domain ID	You cannot set this parameter. The current domain ID is the value that the domain ID is currently set to. The Current Domain ID is 0 for R_Ports that are not active.
Status	You cannot set this parameter. It indicates the status of this R_Port. For more detailed information on the Status parameter, refer to the R_Port status table in the *SANvergence Manager User Manual*.
Fabric Manager Port WWN	You can not set this parameter. This is the world wide name (WWN) of the Fabric Manager R_Port for the FC SAN.
Interconnect mode	Use SANvergence Manager to set this parameter. This is the interconnection mode to this fabric. Modes are: • Open Fabric 1.0 - Use for fabrics that are connected to third- party FC switches that support the FC-SW E_Port implementation. • McDATA Fabric 1.0 - Use for fabrics that are connected to McDATA switches that support this McDATA native mode. • Brocade - Use for fabrics that are connected to Brocade switches.

Table 3-1 R_Port Parameters (Continued)

Parameter	Description
Zone policy	Use SANvergence Manager to set this parameter. Options are Append Router Zones, and No Router Synch (Synchronization): **Append Router Zones -** The SAN Router Storage zone set is appended to the active zone set on the fabric connected by the R_Port. **No Zone Synch -** The zone set information between the mSAN and the fabric connected by the R_Port is not synchronized. The SAN Router Zone Policy specifies how zone information is synchronized between the mSAN and the connected fabrics. For more detailed information on the *set SAN Router Zone Policy* parameter, refer to the *SANvergence Manager User Guide.*
Fabric	Name used to create the FC ID (name) used by the SAN Router to identify the attached fabric.
Insistent Domain ID	This is a boolean (enable/disable) flag to make the preferred domain ID a required domain ID. If enabled, the value set for the preferred domain ID becomes the domain ID when the fabric initializes. If the preferred domain ID is not accepted by the principal switch in the fabric, the R_Port will be isolated from the fabric.

3. To configure the R_Port using different parameters that are displayed, use SANvergence Manager. Refer to instructions for configuring R_Port parameters in Chapter 4 of the *McDATA SANvergence Manager User Manual* (620-000189).
4. Note that the FC port timeouts, E_D_TOV and R_A_TOV, must be configured the same on the SAN Router and all Fibre Channel switches in an attached fabric. To configure these parameters, refer to *Configuring Advanced FC Port Parameters* on page 3-10.

Configuring Advanced FC Port Parameters

To configure FC port timeouts, follow these instructions:

1. *Select Configuration>Port >Advanced FC Port* to display the *Advanced FC Port Configuration* dialog box.

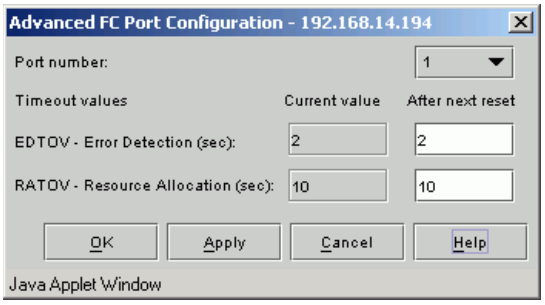


Figure 3-3 Advanced FC Port Configuration Dialog Box

2. Select the *Port number* from the list. The current timeout values are displayed and may not be changed.
   - *EDTOV* - (Error detection timeout value in seconds). This is a short timeout used to detect an error condition. The value EDTOV represents a reasonable timeout value for detection of a response to a timed event.
   - *RATOV* (Resource allocation timeout value in seconds) - A long timeout value used to determine when to reinstate a recovery qualifier. The value RATOV represents EDTOV plus twice the maximum time that a frame may be delayed within a fabric and still be delivered.
3. Enter the timeout values you wish to be in effect after the next system reset in the *After next reset* column.

Example Configuration and Procedures

This section provides a specific example of procedures to configure a SAN Router for a RAD, as well as an mSAN consisting of an Fibre Channel switch and attached storage (Figure 3-4).

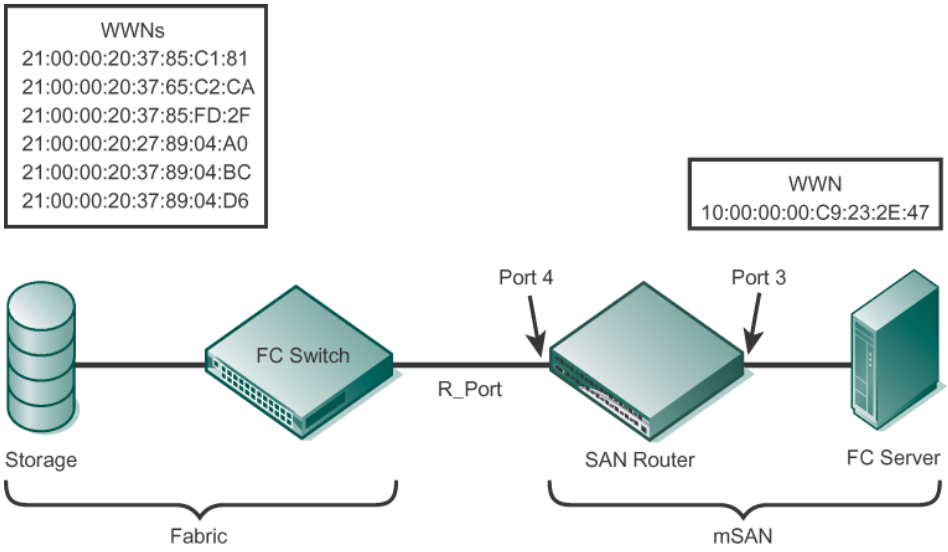


Figure 3-4 Connecting to Fabric and FC Device

The configuration in Figure 3-4 on page 3-11 shows both the SAN Router and the Fibre Channel switch with no pre-configured zones. Port 4 of a SAN Router will be connected to a port on the Fibre Channel switch. The FC server is connected to port 3. The FC WWN of the HBA in the server is 0x10000000C9232E47. There is a JBOD connected to the FC switch, which has six disks with WWNs as shown in the figure. This section describes this sample configuration using R_Ports.

To create the port configuration, follow these instructions:

1. Make sure the SAN Router is *not* connected to the FC switch.
2. Start the Element Manager for that SAN Router to configure an R_Port.

3. Follow steps under *Configuring the FC Ports for Router-Attached Devices* on page 3-4 to configure port 3 for connecting to the FC server. Make sure to select *FC-Auto* under *FC Port Parameters* on the *FC/Ethernet Port Configuration* dialog box.
4. Follow steps under *Configuring R_Ports for mSANs* on page 3-6 to configure port 4 as an R_Port.
5. Make sure that the fabric timeout values E_D_TOV, R_A_TOV for both the mSAN and the fabric match. Refer to *Configuring Advanced FC Port Parameters* on page 3-10.
6. Save the new configuration by choosing *File>Save Configuration*. Reset the SAN Router by choosing *File>Reset System* for the new configuration to take effect, if required.
7. Now that the R_Port configuration is complete, physically connect the ports on the SAN Router and the FC switch together.
8. On the *SANvergence Manager* main screen, select the mSAN in the *mSANs* pane where the SAN Router is located, then select *mSAN Configuration* to display the *mSAN Configuration* screen. Confirm that all the devices from the fabric are shown under the R_Port (port 4 that has the icon).
9. Select *Actions>Fabric Configuration* to display the *Fabric Configuration* window.
10. After you have established the physical connection, use the Selective Import option in the SANvergence Manager to import the devices from the FC switch into the mSNS. Importing the devices make the SAN Router and the FC switch register the new device information with their respective Name Servers. The FC switch registers with its simple name server (SNS) and the SAN Router with its metro storage name server (mSNS).
11. Select the *R_Ports* tab to set the *Preferred Domain ID* to a unique Domain ID on the fabric.

    If you are not using the default, set the interconnect mode for the FC switch.
12. Create a zone using SANvergence Manager.
13. Add the server attached to port 3 and the devices attached to port 4 to the newly created zone, while making sure that you are adding individual devices and not fabric ports into the zone.
14. Click *Commit* and save the configuration to flash when prompted.

As soon as the zone configuration is activated from SANvergence Manager (by clicking *Commit*), the zone set is also registered with the fabric zone server. Since you created the router zone set during the R_Port configuration process, the new zone set is also activated in the fabric.

Configuration Notes for All R_Ports on the Same Fabric

- E_D_TOV and R_A_TOV values must be the same.
- Domain IDs must be different. However, IDs can be the same on two different fabrics.
- World Wide Node Name (WWNN)-based zoning is not supported. In order to maintain interoperability between the McDATA fabric and third party fabrics, ensure that "soft" zoning on the fabric side is done using World Wide Port Names of devices instead of World Wide Node Names of devices.

Guidelines for Using Zone Policy

The following are guidelines for using zone policy:

- *Append Router Zones* is the default setting when an R_Port is first configured.
- *No Zone Synchronization* may be preferred if the native FC SAN management utility is used for configuring zoning. This is especially true if all the devices reside in the fabric (the devices are not directly attached to SAN Router ports).

  Any device zoned by SANvergence Manager is visible to all fabrics, whereas unzoned devices are invisible. With *No Zone Synchronization* in effect, it is only necessary to create one zone that contains all the devices that need to be shared between fabrics. There is no need to duplicate the actual zoning configuration present in each of the fabrics.
- In mixed mode environments, with some devices attached to SAN Router ports and others residing on fabrics, it is recommended that *Append Router Zones* be used instead of the *No Zone Synch* option as the configuration process is more involved.
- FC SAN management utilities from some FC switch vendors may not be capable of displaying devices outside the local fabric. In this case, use *Append Router Zones* zoning policy.

R_port Compatibility

The following R_Port compatibility table shows support for attaching Fibre Channel switches to the Eclipse 2640 SAN Router. The Fibre Channel switches must be operating in either McDATA Fabric 1.0 or Open Fabric 1.0 interoperating mode.

Table 3-2 R_Port Compatibility

		Connection Modes		
FC Switch	**Firmware Release**	**McDATA Fabric 1.0**	**Open Fabric 1.0**	**Brocade**
McDATA Sphereon 3016, 3032, 3216, 3232, 4500 and Intrepid 6064 and 6140	E/OS 5.2, 5.3, 6.1, 6.2, 7.0, 8.0	X	X	
McDATA Sphereon 4300	E/OS 6.1, 6.2, 7.0	X	X	
McDATA Intrepid 10,000	E/OSn 6.0	X	X	
Brocade 3900	4.1.2a,b		X	X
Brocade 3200 / 3800	3.1.1a,b,c		X	X
Brocade 2400	2.6.1a,b,c		X	X
Brocade 12000	4.1.2b		X	X
Qlogic SANBox2	1.3.64.00, 3.0, 4.0, 4.1		X	
IBM Blade server	IBM Qlogic 2.0.0.19		X	
Cisco 9509	1.3.5		X	

Table Notes

Since the SAN Router supports multiple fabrics in a seamless fashion, we recommend that the user **not** inter-mix switch vendors in the same fabric.

4

Configuring iSAN Connections

This chapter provides detailed steps for configuring the SAN Router ports for iFCP and setting up iFCP connections. Use the following links to move through the chapter.

Introduction

An iSAN (internetworked storage area network) is a collection of one or more fabrics interconnected using one or more SAN Routers, where at least one fabric is in a distant location outside the metro area. An iSAN is characterized by high latency and low bandwidth inter-switch links (T1, T3, OC3, etc.) such as those found in wide area networks. An iSAN has at least two SAN Routers that are interconnected using iFCP connections. An iSAN is also a collection of two or more mSANs. SAN routing done within an iSAN is referred to as iSAN Routing or SAN Routing over distance.

Figure 4-1, *iSAN Configuration Example* illustrates two mSANs interconnected through an iFCP link to create an iSAN. iFCP interswitch links (ISLs) can be used to overcome scalability limits of a single mSAN. iFCP is also recommended for connection across a WAN, as this provides higher performance when using features such as FastWrite and compression.

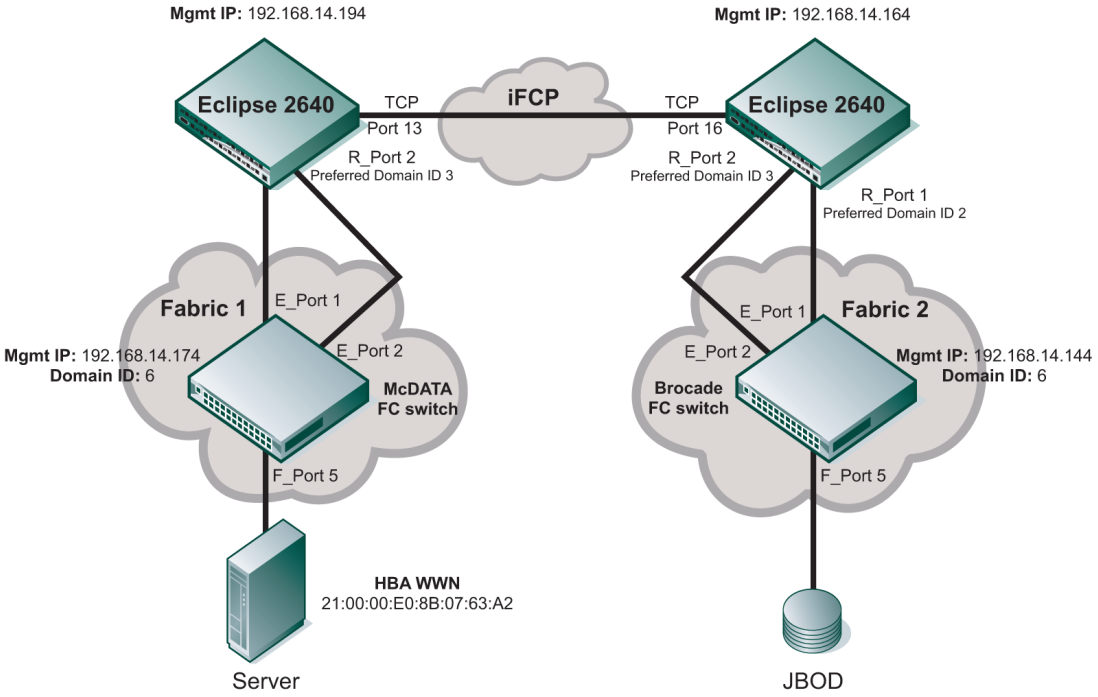


Figure 4-1 iSAN Configuration Example

Chapter 3 provides instructions for configuring the SAN Router to create an mSAN by attaching fabrics to the SAN Router R_Ports. Chapter 4 provides steps for interconnecting mSANs with remote mSANs over a WAN. Connections to the network are made through those SAN Router's TCP ports available for configuring FC Protocol (iFCP) connections.

Configuring TCP Ports for iFCP

This section describes how to configure the TCP ports (port numbers 13-16 on the Eclipse 2640 SAN Router) for iFCP connections.

This involves the following procedures:

- Setting the general port parameters
- Setting advanced TCP parameters
- Setting the iFCP parameters

Configuring the General Port Parameters

1. From the Element Manager, select *Configuration> Port> FC/Ethernet*

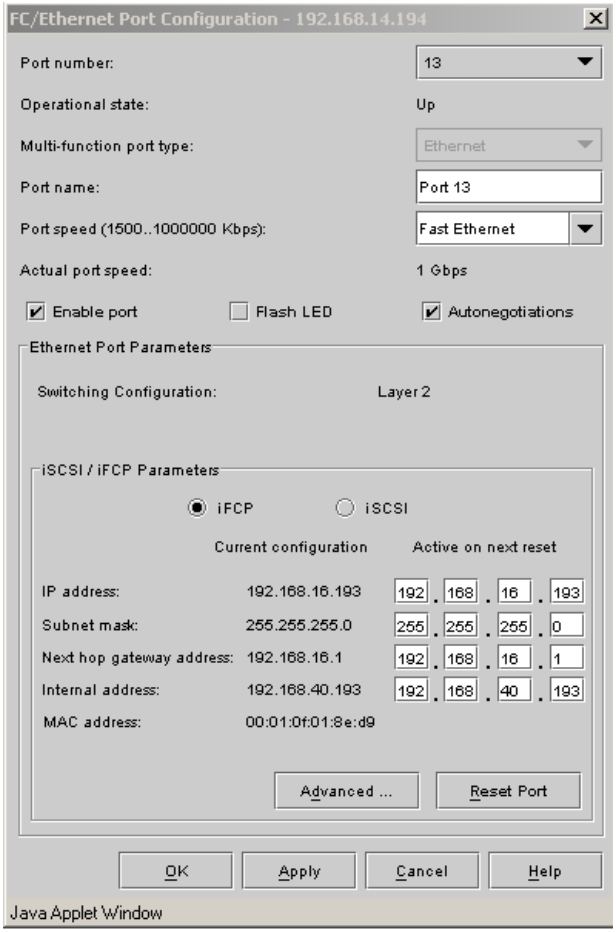


Figure 4-2 FC/Ethernet Port Configuration Dialog Box

2. Select a port. The screen is refreshed to show the operational state.
3. Type a label for this port in the *Port Name* field.
4. Set the port speed under the *Port Speed* list, if needed and select the *Enable Port* checkbox.
5. Select or clear the *Autonegotiations* check box as required. This option determines whether the port advertises its autonegotiation properties to a receiving device per the autonegotiation specified by IEEE standard 802.3.

6. Select the *Flash LED* option to blink the port LED. You can use this option to locate the physical port in a rack of SAN Routers.

Setting the Advanced TCP Parameters

The SAN Router provides options to optimize the TCP port behavior through a set of advanced parameters. Use the following procedure to configure the advanced TCP parameters.

1. Click the *Advanced* button. The *Advanced TCP Configuration* dialog box appears (Figure 4-3 on page 4-6).

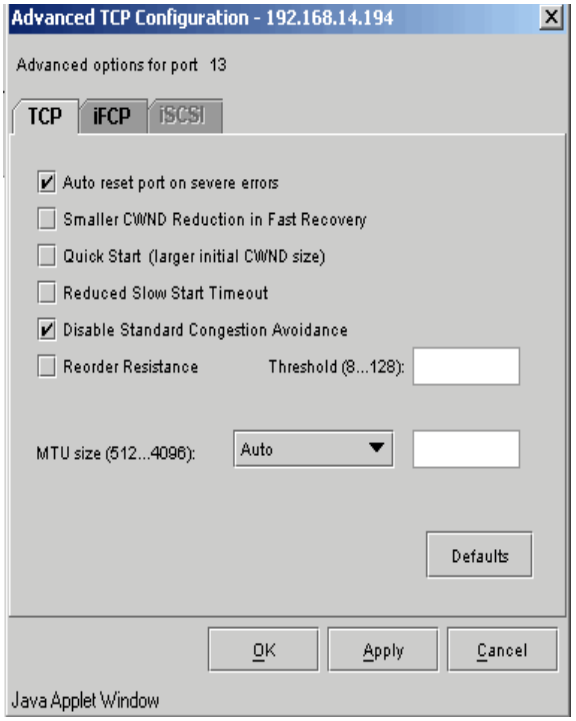


Figure 4-3 Advanced TCP Configuration

In the TCP section:

- Select *Auto-reset port on severe errors* especially when the port is a part of a mission-critical configuration.

Manual Reset: You may not want the auto-reset option to be on when you are troubleshooting unrecoverable errors. In this case, you can do a manual reset by clicking *Reset Port* in the *FC/Ethernet Port Configuration* dialog box.

2. Set the *MTU size*.

   The MTU (maximum transmission unit) size can be used to prevent accidental fragmentation when the path (discovered) MTU value, as returned by paths from/to this port, is incorrect. This can occur with some security/encryption appliances on the network, where the MTU size may not be correctly reported. The following options are available:

   - *Auto* - Use the discovered MTU size. This is the default setting.
   - *Manual* - Forces the system to use the configured value for MTU size and DOES NOT do auto-discovery. The range is from 512 to 4096, the default size is 1500.
   - *Min* (Auto, Manual) - Does auto -discovery and uses the minimum of the discovered and configured values.

Storage-optimized TCP Parameters:

Storage-optimized TCP is a set of enhancements made to the TCP behavior to ensure high throughput in a dedicated network in enterprise environments typically used for storage traffic. These enhancements are built on the inherent reliability of TCP by optimizing the traffic control features in a dedicated network. Following are the TCP feature enhancements that make up the storage-optimized TCP:

- Reorder resistance in case of out-of-order packet delivery.
- Quick start with higher initial value of congestion window.
- Smaller reduction in congestion window on slow start and fast retransmit.
- Disabling congestion avoidance phase in fast retransmit and fast recovery.
- Reduced slow start timeout.

You can implement these enhancements by selecting the checkboxes provided in the *Advanced TCP Configuration* on page 4-6.

1. Select *Smaller CWND Reduction in Fast Recovery* to improve the performance of the SAN Router when packet losses occur due to reordering or noise rather than congestion. When enabled, the SAN Router responds more slowly to congestion events because the send congestion window (CWND) is reduced to 7/8 of its previous value as compared to 1/2 in standard TCP.

NOTE: Do not select this option when other traffic sources sharing the same TCP link are bursty or intermittent.

2. Select *Quick Start* to improve the initial performance and error recovery performance on dedicated links with a lot of traffic. Enabling this increases the initial value for the congestion window at the beginning of TCP slow starts, and increase the congestion window size more rapidly.

   Standard TCP uses *Slow Start* to protect a network and the other traffic on it from a sudden burst that can cause congestion difficulties.

3. Select *Reduced Slow Start Timeout* to reduce the minimum *Slow Start* timeout from 500 msec to 150 msec. This improves responsiveness to congestion events that trigger *Slow Start*.

4. Disable *Standard Congestion Avoidance* to disable the slow growth mode of the SAN Router's congestion window that occurs in the standard TCP stack when a congestion event is detected.

   A congestion event occurs when there is either a transmission timeout (slowstart timeout) or sufficient duplicate acknowledgements trigger the fast recovery algorithm. The growth of the congestion window in congestion avoidance is normally at the rate of 1/cwnd bytes per ACK received.

5. Select *Reorder Resistance* for reliable links that reorder packets. Selecting this option will reduce unnecessary packet retransmission caused by packets being reordered in the TCP path.

   Selecting *Reorder Resistance* increases the number of duplicate ACKs required to trigger a *Fast Retransmit* or *Fast Recovery*. Use the next step to specify the number of ACKs.

NOTE: Enabling reorder resistance could slightly delay recovery from dropped packets in short data messages.

6. Specify the number of ACKs that trigger *Fast Retransmit* or *Fast Recovery* using the *Threshold* field. Valid values are between 8 to 128, with a default of 8. Larger values reduce retransmissions by causing the SAN Router to wait longer for retransmitted packets to arrive. This may delay the detection of dropped packets.

Setting the iFCP Parameters

1. To set the port as iFCP, select iFCP from the iFCP/iSCSI parameters field.
2. Specify the IP address. This is the iFCP/iSCSI IP address that will be used for this port after the next port reset or system reset.

   NOTE: This IP address must be in a subnet different from the SAN Router's inband subnet.

3. Specify the *Subnet mask*. This is the subnet mask to use for this port after the next port reset or system reset.
4. Specify the *Next Hop Gateway Address*.

   This is the gateway address to use for this port after the next system reset. TCP ports act as end nodes (hosts) attached to the WAN, and therefore may have a different gateway than the default gateway used by UDP ports connecting to the local mSAN.
5. Specify the internal IP address.

   The internal IP address is used with the SAN Router's inband IP address for internal control. The TCP port acts as a proxy between the SAN Router's internal network and the external WAN network.

   NOTE: The internal address must be in the same subnet as the SAN Router's inband IP address.

6. Select the iFCP tab from the *Advanced TCP Configuration* dialog box (refer to Figure 4-4) to specify the *iFCP* parameters:

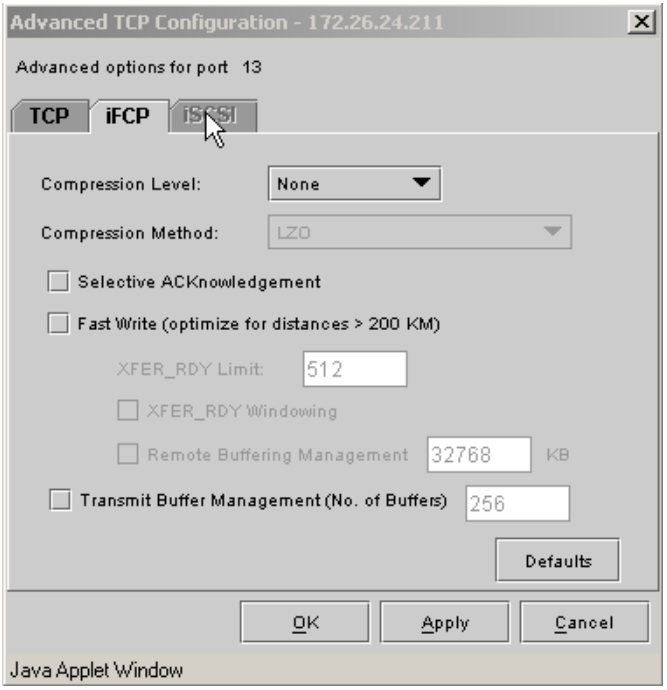


Figure 4-4 Advanced TCP Configuration iFCP Parameter

1. Select the compression behavior for the TCP/IP port using the *Compression Level* combo box. Compression is an optional software feature; the *Compression Level* field is disabled if compression is not included in your software version.

   Compression technology takes advantage of replicated characters or patterns being sent across a network port to effectively increase throughput on that port. Only the payload is compressed and not the TCP/IP header. Packets with a size less than 512 bytes are not compressed. Compression is especially useful when transmitting data over a slow link such as a T1 or 10 Mbps Ethernet. The following options are available for *Compression Level:*

   - *None* - Data that is going out of the port is not compressed. This is the default setting.

- *HW* - All transmitted data is compressed using the hardware feature in the SAN router. This is the recommended setting if the remote destination also supports HW compression.
- *SW* - All transmitted data is compressed, using the SAN router's CPU. Use this setting when you need to use as little bandwidth as possible and the remote destination does not support hardware compression. Note that effective throughput with the "SW" setting may be less than the effective throughput seen with the "SW as needed" setting, especially at link speeds greater than T3.
- *SW as needed* - Depending on the available bandwidth, decision are dynamically made whether or not to compress transmitted data. With *SW As Needed* setting *on*, the port keeps the egress data rate as close as possible to the port speed of the port.

2. Specify the compression algorithm by selecting the *Compression Method*. Compression is an optional software feature; the *Compression Method* field is enabled only if the *Compression Level* is *SW* or *SW as needed*.

   The multiple compression methods allow a trade-off between compression rate (speed) and compression ratio (amount of compression). The following options are available for *Compression Method*:

   - *LZO* - performs compression on a frame-by-frame basis. This method is best when there are many active initiator-target sessions. This is the default setting.
   - *Fast LZO with History* - performs compression two bytes at a time with eight kB of history. This works best with fewer active iFCP initiator-target sessions and a fast remote link.
   - *LZO with History* - performs compression one byte at a time with eight KB of history. LZO w/History gives the next best compression ratio, but has a compression rate of about 25 MB/s. For link Rates of 100 Mb/s or less use LZO w/History. This works best with fewer active iFCP initiator-target sessions and a medium speed remote link (for example, T3).
   - *Deflate* - provides the best compression ratio, but has the lowest compression rate. For link rates of 10 Mb/s or less use *Deflate* (may be called ZLIB). This is best for slow links, such at T1, with any number of active iFCP initiator-target sessions.

Select Hardware Compression from the Compression Level drop-down list. This has the lowest compression ratio, but it can run at link rate.

3. Select *Selective ACKnowledgement* (SACK) to acknowledge non-contiguous sequence numbers. This reduces the amount of retransmitted data when packets are lost. Enabling this provides better performance in congested networks (assuming the remote device also supports SACK).

Setting FastWrite Features

1. Select the *FastWrite* feature to improve performance for distance over 200 Km. The FastWrite feature can minimize the data transfer delay for write operations on long distance links by responding to *Initiator Write* commands with *TransferReadys*. This fills the WAN pipes and buffers the data at the SAN Router that is closest to the target. The SAN Router that is buffering the data then feeds it to the actual target at the rate that the target can handle. Therefore, FastWrite makes up for the round-trip delays typical of most WAN links. Note that FastWrite does not spoof Write Status commands, thus ensuring data integrity.

NOTE: Port reset is not required when changing FastWrite options in the TCP Advanced Options dialog box

---

When the FastWrite is enabled, several additional parameters are available to customize the FastWrite behavior:

- XFER_RDY Limit: The maximum number of XFER_RDY commands that may be issued early by the SAN Router to avoid round trip delays. The limit is applied to each Fabric Channel login session.
- XFER_RDY Windowing: When selected, the configurable XFER_RDY limit is treated as a moving “window” of consecutive XFER_RDYs that may be issued by the early SAN router. If not selected, the XFER_RDY limit is simply the total number of XFER_RDY commands that can be simultaneously outstanding for each login session.
- Remote Buffer Management: When selected, the local SAN Router limits the amount of buffer memory used in the remote SAN Router by limiting the amount of data requested by the local SAN Router and sent to remote SAN

Router without a XFER_RDY from the target device. Specify the maximum amount of buffered data, in kilobytes, in the text field. The memory limit is a single pool for all Fabric Channel login sessions.

- Selecting the *Transmit Buffer Management option* allows the user to manage the amount of Fabric Channel receive buffers that an iFCP port has for receiving the Fabric Channel frames forwarding from Fabric.

  In cases where ELSs are issued in the middle of large amount of data packets and the iFCP/TCP side is connected to a slow link (e.g. OC3 link), user may experience ELS timeout. ELS timeout occurs when ELSs have command timeout values shorter than normal Read / Write commands and when ELSs are queued behind the large amount of Read/Write data. Reducing the number of Fabric Channel receive buffers will cause congestion back into any attached device or fabric to occur sooner or for lower amounts of outstanding data, which then minimizes the ELSs timeout condition.

NOTE: Transmit buffer option may cause head of line blocking and congestion which might lower the performance of the system instead of helping it.

- Select the *Defaults* button to reset all options in the iFCP area to the following:
  - Compression Level - Off
  - Compression Method - LZO
  - Selective ACKnowledgement - enabled
  - FastWrite - disabled
  - Transmit Buffer Management - disabled

Configuring iFCP Connections

To configure an iFCP connection, configure a TCP port (13-16) as iFCP, as described in *Configuring TCP Ports for iFCP* on page 4-4. A pair of SAN Routers connects two mSANs. Each mSAN is identified by a unique mSAN ID and each has its own mSNS. Only configure a mSAN ID when iFCP is being used. Otherwise, there is only a single mSAN.

To configure the SAN Router for iFCP connections, select the following options from the *Configuration>iFCP* tab:

- Select *Setup* to configure the mSAN ID for the iFCP function.
- Select *Remote Connections* to configure connection-specific parameters. refer to *Configure Remote iFCP Connections* on page 4-15.

Configuring iFCP Setup

To configure the SAN Router for iFCP connection, follow these instructions:

1. Select *Configuration>iFCP>Setup* to display the *iFCP Setup* dialog box (Figure 4-5).

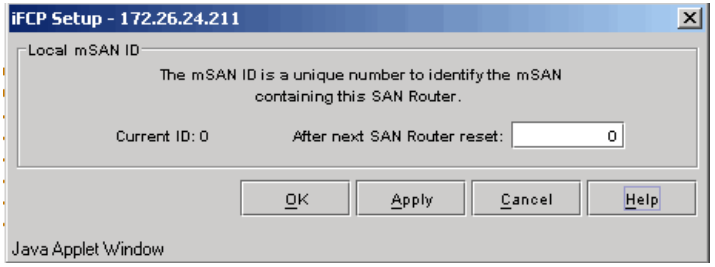


Figure 4-5 iFCP Setup Dialog Box

2. Optionally, change the *Active on next reset* mSAN ID.
   - A new mSAN ID takes effect when you reset the system. Thus, two IDs are shown: the ID currently in effect and the ID that will be used after you reset the system.

- Set the local mSAN ID when the SAN Router is installed. The default value is zero (0). The local mSAN ID is a number between 0 and 4,294,967,295 that uniquely identifies the local mSAN.

NOTE: The SAN Router at each end of the iFCP link (and thus the mSANs at each end) must have different mSAN IDs.

Configure Remote iFCP Connections

For each SAN Router, you must specify a list of the remote SAN Routers to which it should export zones.

To configure the remote connections, follow these instructions:

1. Select *Configuration>iFCP>Remote Connections* to display the *Remote Connections* dialog box (Figure 4-6).

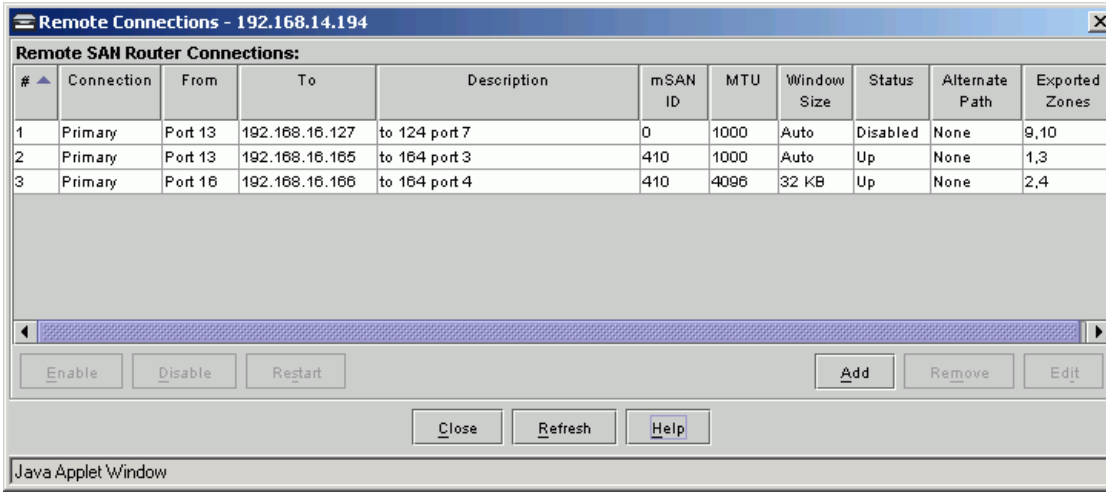


Figure 4-6 Remote Connections Dialog Box

Table 4-1 Read-Only Remote Connections Parameters

Column	Description
Connection	Indicates whether the connection is primary (manually configured on this SAN Router) or backup (automatically copied from this SAN Router or another SAN Router so the local SAN Router can back up the connection).
From	The connection port on the local SAN Router. If the port is not configured for iFCP, the remote connection will fail.
To	The connection destination in the remote SAN. This is the IP address of a port on a SAN Router in the remote SAN.
Description	A short note of up to 32 characters to describe this connection. This field is not used by the iFCP connection; it is just a convenience for the storage administrator. Descriptions are only shown for primary connections. For backup connections, the Description field indicates which connection this one is backing up.
mSAN ID	The numeric ID of the remote mSAN at this connection's destination. Every mSAN connected by iFCP through a SAN Router has a unique ID. The remote mSAN ID displayed here is the ID assigned to the remote mSAN, not the local mSAN. The remote mSAN ID may be 0 if the connection is not active.
MTU	The actual MTU size used by the connection. The actual MTU may be different than the discovered MTU if the port MTU is manually configured.
Window Size	The size for all TCP connections on this link. Auto means the window size is selected for each TCP connection depending on the round-trip time measurements. Any other user-defined value indicates a constant window size established in the parameters for this connection.
Status	This is the current status of this connection. Select **F5** to refresh the status table. Up indicates the connection is up and working and connected to the remote address shown in the To column. Down indicates the connection is enabled but is not operating for several reasons. Disabled indicates you have disabled the connection using the *Edit* button or the *Disable shortcut* button (this applies only to primary connections). Idle/Ready indicates a backup connection is ready to take over if the primary fails but is not currently in use (this applies only to backup connections).
Alternate Path	Shows the source and destination of the alternate link, if any. For primary connections, this field describes the backup connection. For backup connections, this field describes the primary connections.
Exported Zones	A list of zone IDs exported on this connection.

NOTE: Backup connections (identified by Backup in the Connection column) cannot be selected, even when the backup connection is active. Backup connections cannot be edited or removed. These connections inherit their settings from the corresponding primary connection.

CAUTION

When exporting zones across iFCP, make sure the zone members are device WWNs and not fabric ports, as fabric port zones are not supported across iFCP.

To configure an iFCP connection going to a remote SAN Router, follow these instructions:

1. Click *Add* on the *Remote Connections* dialog box to display the *Add Remote Connections* dialog box (Figure 4-7).

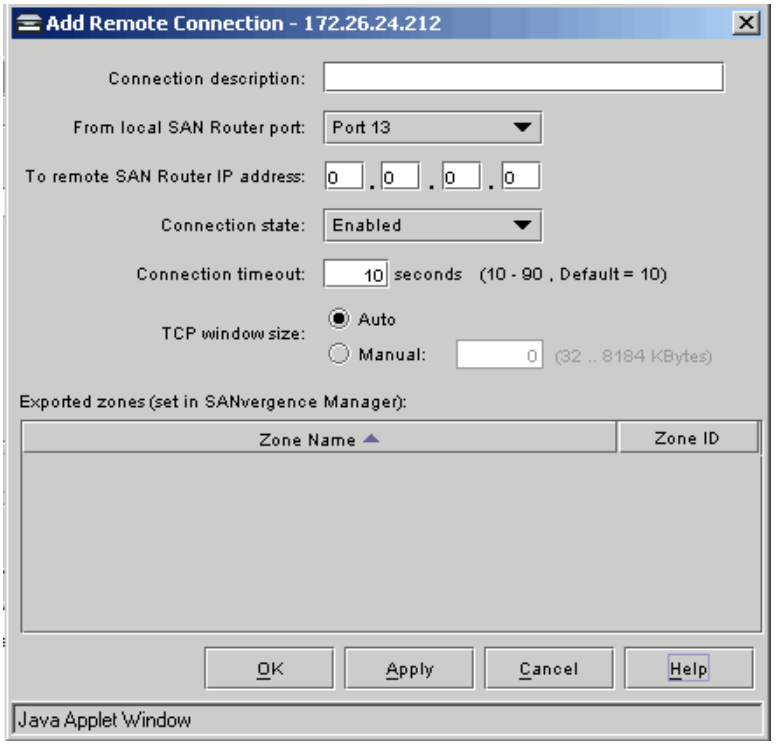


Figure 4-7 Add Remote Connection Dialog Box

Use this dialog box to add new remote iFCP connections or edit parameters for existing connections.

You can modify information in this dialog box as described in Table 4-2.

Table 4-2 Remote Connections Parameters

Setting	Description
Connection Description	Enter up to 32 characters of description to help remember the purpose of this connection.
Local SAN Router Port	Select the port on the local SAN Router from the drop-down list.
Remote SAN Router IP Address	IP address of the SAN Router that is providing TCP access to the remote SAN. Enter the remote SAN Routers WAN port address.
Connection State	Select Enabled from the drop-down list for normal sharing of devices between SANs. Select Disabled to prevent sharing of storage devices. While the connection is disabled, the connection acts as if it were not present in the list at all.
Connection timeout	The connection timeout is the maximum time that the remote SAN Router can remain unreachable before the connection is closed. The default is 10 seconds.
TCP Window Size	The size for TCP connection on this link. *Auto* indicates the window size is selected for each TCP connection depending on the round-trip time measurements. *Manual* indicates any other user-defined value entered in the text field next to the *Manual* button.
Exported zones	This table lists the zones exported over iFCP connections through the SANvergence Manager.

CAUTION

If you make zone changes using SANvergence Manager, do a refresh (press F5 or click *Refresh*) to update the list of available zones.

2. To edit existing remote connection information, select one or more rows in the table and click *Edit*. This displays the *Edit Remote Connections* dialog box (Figure 4-8 on page 4-20).

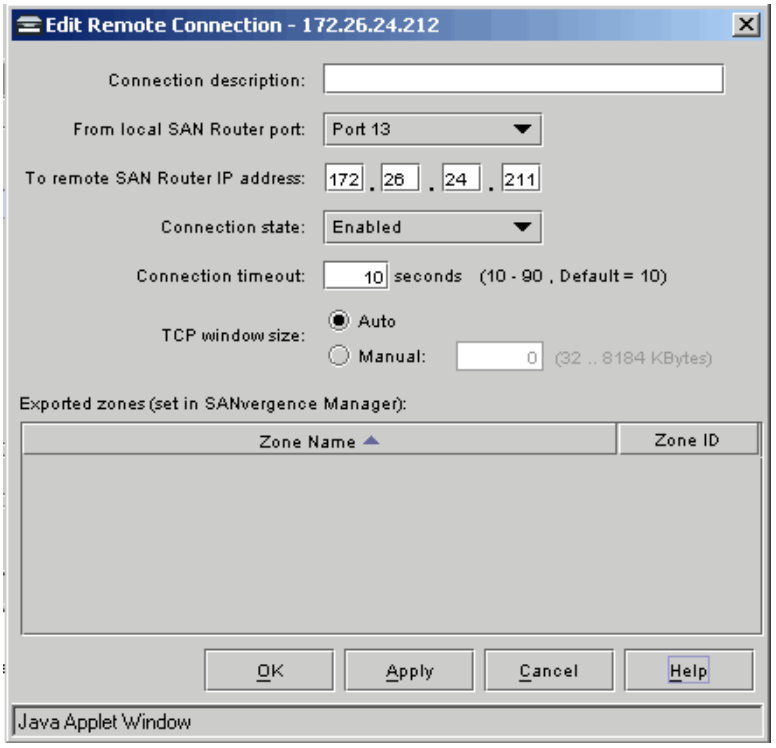


Figure 4-8 Edit Remote Connection Dialog Box

NOTE: To select a range of connections, select the first, then hold down the **Shift** key while selecting the last connection. To select a set of connections, hold down the **Ctrl** key while clicking on each connection.

3. To remove iFCP connections, select one or more rows in the table and click *Remove*. Removing a remote connection terminates all data sessions to that SAN Router. All devices in the remote mSAN are removed from the remote mSNS and are no longer available to the local mSAN.
4. Enable or disable remote connections, if needed (Refer to *Configure Remote iFCP Connections* on page 4-15).
   - Select the connections to be enabled or disabled and click the *Enable* or *Disable* button below the list of remote connections.

- A connection with a status of *Down* is enabled but inactive. The SAN Router periodically attempts to restore a failed connection. If you wish to initiate a reconnection attempt (for example, after you've corrected the cause of the connection failure), select the connection and click the *Restart* button.

5. Press **F5** or click the *Refresh* button to refresh the list of remote connections, including their status information.

NOTE: Restarting a connection is equivalent to disabling and then re-enabling the connection.

Configuring a Backup iFCP Connection

You can configure redundant fail-over for the iFCP connection so that one iFCP port backs up another iFCP port on the same SAN Router.

Redundant ports must be configured symmetrically; for example, each port must back up the other. A port can have both primary and backup connections, such as pair of ports having connections to a remote SAN, exporting different zones to split the load. If either port fails, the remaining port takes over the entire load.

To configure a backup for the SAN Router ports, follow these instructions:

1. Select *Configuration>iFCP>Port Redundancy* to display the *iFCP Port Redundancy Configuration* dialog box (Figure 4-9).

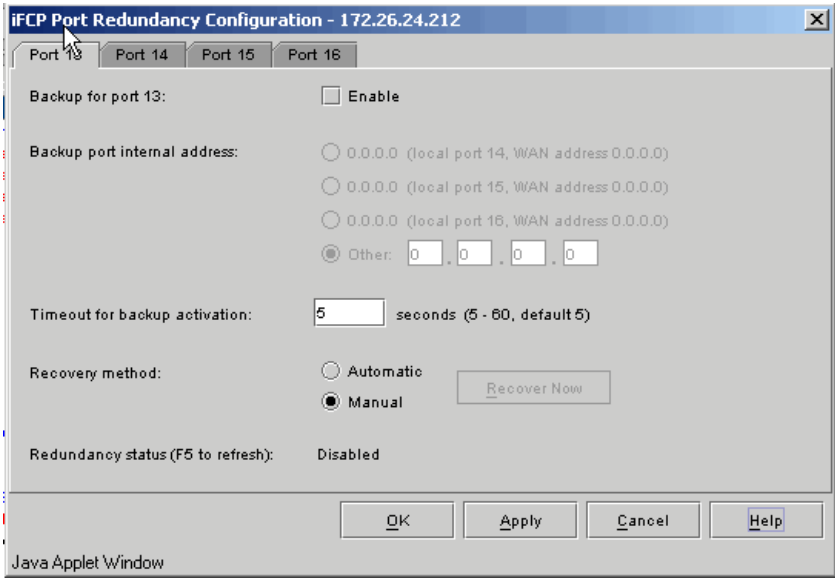


Figure 4-9 iFCP Port Redundancy Configuration Dialog Box

2. Select the tab for each port you wish to configure.
3. To enable backup operation, select the *Enable* box. To disable backup operation, clear this box.
4. Select the port that you want to backup for the port being configured.

5. Set the *Timeout for backup activation* to between 5 and 60 seconds (default is 5 seconds). If the backup port cannot reach the primary port through the local SAN for this period of time, the backup port assumes that the primary port has failed and activates the redundant connection. This timeout does not apply if the primary port is running but the WAN link to the primary port goes down. In that case the primary port notifies the backup port to activate the backup connections immediately.
6. Set the *Recovery method* to *Automatic* or *Manual*. This determines the primary port's behavior when the failure is corrected. When the port is restarted, it regains connection to the local SAN or a WAN link.
   - *Automatic* - The primary port takes over the connections from the backup port immediately. Switching the connections back to the primary port, like switching them to the backup port earlier, is disruptive. All data sessions to the affected devices are terminated. The remote devices are temporarily de-registered from the local SAN and then re-registered by the primary port.
   - *Manual* - The backup port continues to serve the transferred connections after the primary port is restored.

NOTE: Backup port is always on the same SAN Router as the primary port, it must be configured symmetrically before clicking *Apply* or *OK*. For example, if you select the *Port* 13 tab and specify Port 14 as a backup, then you must also select the *Port 14* tab and specify Port 13 as the backup.

7. Click *OK* or *Apply*.

   Redundancy status indicates whether the backup port is active and ready to take over in case of failure. Press **F5** to refresh this status information. If the backup configuration fails, the backup port cannot be reached. Verify that the backup port's IP address is the internal address of the port. If the backup configuration is rejected, the backup port is disabled, not configured for iFCP, not configured symmetrically as a backup pair or the local mSAN IDs differ.

Example Configurations and Procedures

This section provides procedures to configure the SAN Router for connecting remote SANs through iFCP. This section assumes that you have SANvergence Manager software installed.

Figure 4-10 illustrates two SAN Routers connecting two FC disks across a TCP/IP metropolitan area network (MAN) or wide area network (WAN).

NOTE: Although this example shows SAN Routers connected directly to storage devices, SAN Routers can also connect through FC switches.

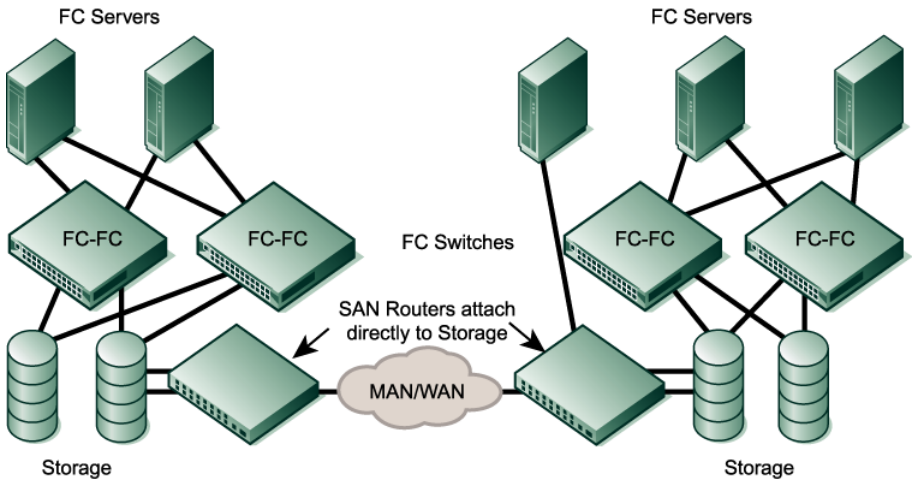


Figure 4-10 MAN/WAN Links

Since the WAN/MAN connection is a TCP-based iFCP link, TCP automatically restransmits any dropped packets. This configuration provides several benefits including:

- Very high performance including, data compression, FastWrite, and support for large TCP window sizes.
- High availability and scalability through state change notification (SCN), containment and separate mSNS, internet storage name services, and servers per site. Since SCN messages are contained, topology changes in the local site are not transmitted to all the switches in the remote site.

- If the WAN link is severed, separate mSNS servers allow continued undisturbed communication between initiators and targets within the local and remote sites.
- When the WAN link is reconnected, communication between the local and remote devices is automatic and no fabric resets are necessary to reconverge the network.

A simplified version of this is illustrated in Figure 4-11 on page 4-25.

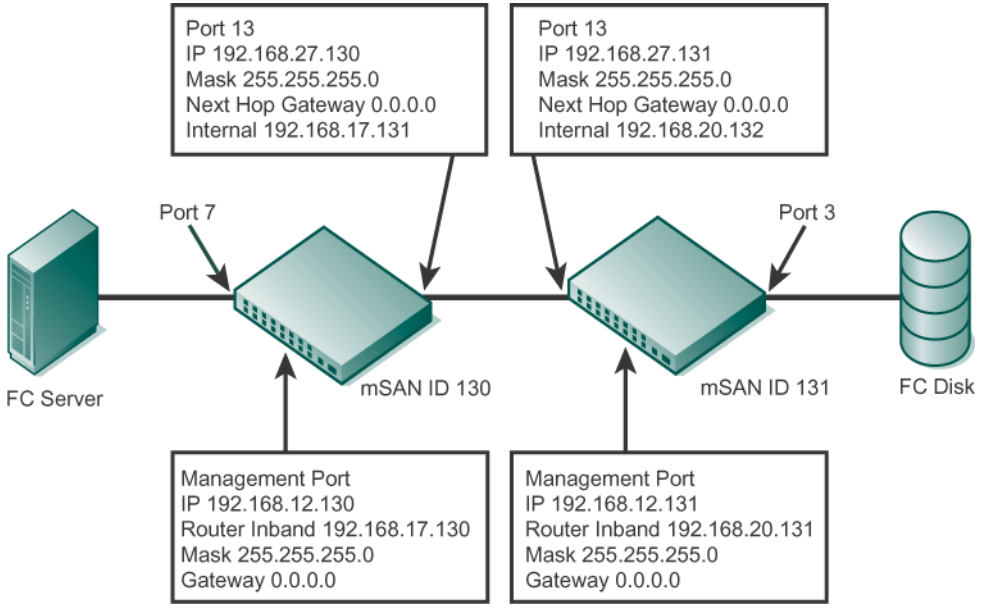


Figure 4-11 Automatic Communication

To configure this example, follow these steps.

Configuring Ports and Connections

1. Log in into Element Manager for the mSAN with management port address 192.168.12.131.

NOTE: You can log in through SANvergence Manager or by entering the IP address into an internet browser.

2. Enter the default *Modify* password (private) in the field provided and click *OK*.
3. When the Element Manager window appears, select *Configuration>System>Inband Address* to change the SAN Router's inband address parameters.
   - Set the inband address to 192.168.20.131.

   When you change the *Inband* IP *address*, you must reset the SAN Router before you can configure the iFCP port.
   - Leave the gateway at 0.0.0.0 and click *OK*.
4. Select *Configuration>Ports>FC/Ethernet* and select port 13 to configure the Remote SAN Router's iFCP port.
   - Select *iFCP* under *iSCSI/iFCP Parameters*, and enter the following:
     - Port IP- 192.168.27.131
     - Subnet Mask- 255.255.255.0
     - Next Hop Gateway Address: 0.0.0.0
     - Internal Address: 192.168.20.132
   - Click *OK*.
5. Select *Configuration>iFCP* to display the *iFCP Setup* dialog box.
   - Type *131* for the Local mSAN ID and click *OK*.
6. *Select File>Save Configuration* and click *OK*.
7. *Select File>Reset System* and click *OK*.
8. Verify in the Element Manager if the iFCP port is up and showing a TCP icon on the port, with a green port outline after the SAN Router comes up again.
9. Log into the Element Manager for the SAN Router with the 192.168.12.130 address.
10. Enter the default *Modify* password in the field provided (private) at the login prompt and click *Login*.
11. When the Element Manager appears, select *Configuration>System>Inband Address* to change the SAN Router's inband IP address.
    - Set the inband address to 192.168.17.130.

When you change the *Inband IP address*, you must reset the SAN Router before you can configure the iFCP port.

12. Select *Configuration>Ports>FC/Ethernet* when Element Manager displays the *FC/Ethernet Port Configuration* dialog box (Figure 4-12 on page 4-27).

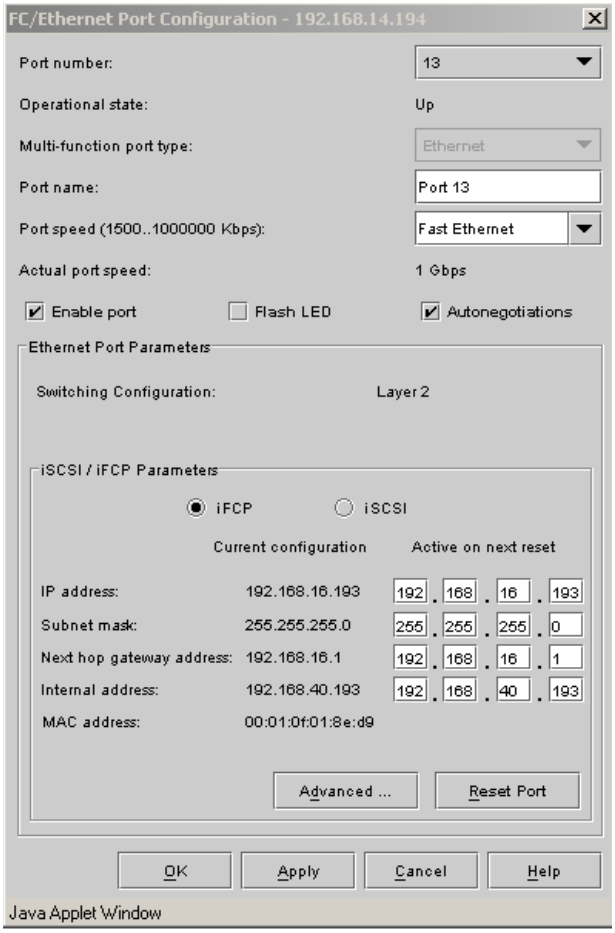


Figure 4-12 FC/Ethernet Port Configuration Dialog Box

- Select port 13 for configuring a remote SAN /iFCP connection.
- Select *Enable Port*.

- Select iFCP under *iSCSI/iFCP Parameters* and enter the following information:
  - Port IP- 192.168.27.130
  - Subnet Mask- 255.255.255.0
  - Next Hop Gateway Address: 0.0.0.0
  - Internal address: 192.168.17.131
- Select *OK*.

13. Select *Configuration>iFCP>Setup* to display the *iFCP Setup* dialog box, and enter *130* for the Local mSAN ID. Click *OK*.
14. Select *File>Save Configuration* and click *OK*.
15. Select *File>Reset the System* and click *OK*.
16. Verify in the Element Manager if the iFCP port is up and showing a TCP icon on the port, with a green port outline, after the SAN Router comes up again.

Setting up Remote and Exported Connections and Zones

1. Open the Element Manager for the SAN Router 192.168.12.130.
2. Select *Configuration>iFCP>Remote Connections* option.
   - Click *Add* to create a new remote connection and select port 13.
   - Enter the IP address for the other SAN Router iFCP port 13 (192.168.27.131).
3. Select *Configuration>iFCP>Remote Connections* for the remote SAN Router in the Element Manager.
   - Click *Add* to create a new remote connection and select port 13.
   - Enter the IP address for the opposite SAN Router's port 13 which is set as iFCP port (192.168.27.130).
4. Open a *SANvergence Manager* window for both SAN Routers and add two SANs, 192.168.12.130 and 192.168.12.131.
5. Select the *mSAN Configuration* window for the 192.168.12.130 SAN Router.

- Create a *New Zone* and name it "Remote Zone" (take note of the Zone ID for the zone).
- Right-click the HBA Port WWN located off the attached port under the right column and left click *Add* with the *Remote Zone* highlighted on the left.

CAUTION

When exporting zones across iFCP, make sure the zone members are device WWNs and not fabric ports, as fabric port zones are not supported across iFCP.

- Commit your changes and save to flash when prompted.

6. Open the *mSAN Configuration* window for the 192.168.12.131 SAN Router. Create a *New Zone* and name it "Remote Zone."

   Make sure the Zone ID is the same as the one noted for the other SAN Router.

   - Select the first FC disk port WWN (from the JBOD), located off the attached port under the right column.
   - Click *Add* with the *Remote Zone* highlighted on the left.
   - Repeat the previous two steps for each disk WWN.
   - Commit your changes and save to flash, when prompted.

7. Go to *Actions >Export Zones* window to export zones across iFCP.
8. Go to the SANvergence Manager *mSAN Configuration* window for each SAN Router, refresh the window, then confirm that the *Remote* devices (HBA, disks) display in their respective zones and have a blue "R" next to them.
9. Make sure the FCHBA driver is installed (if required).
10. Go to the Windows 2000 host and bring up the *Disk Manager* utility. You should see the drives that you zoned as local devices there (you may have to do a "Rescan" to discover the new disks).

The remote connection is set up.

5

Configuring iSCSI Connections

This chapter provides procedures to configure the SAN Router to support line-rate communication between iSCSI initiators and Fibre Channel targets.

Use the following links to move through the chapter.

Introduction

SAN Routers support true gigabit wire-speed iSCSI-FC gateway functionality, which means they can translate iSCSI traffic to Fibre Channel traffic and vice versa. Using SAN Routers, iSCSI initiators can access FC storage devices as shown in Figure 5-1. The initiators and targets (FC or iSCSI) can be either directly connected to the SAN Router or connected across an FC or IP network as shown.

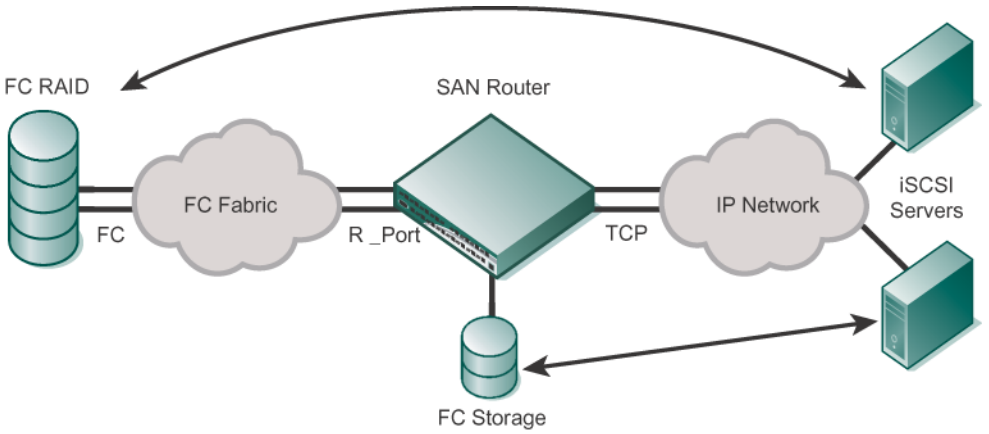


Figure 5-1 iSCSI Initiators Accessing FC Target

E/OSi supports the iSCSI specification RFC 3720.

Figure 5-2 illustrates an example of an iSCSI configuration. This configuration includes an iSCSI-enabled server (Web Server) through an iSCSI HBA or an iSCSI driver running on a traditional NIC (network interface card) or a TOE (TCP offload engine).

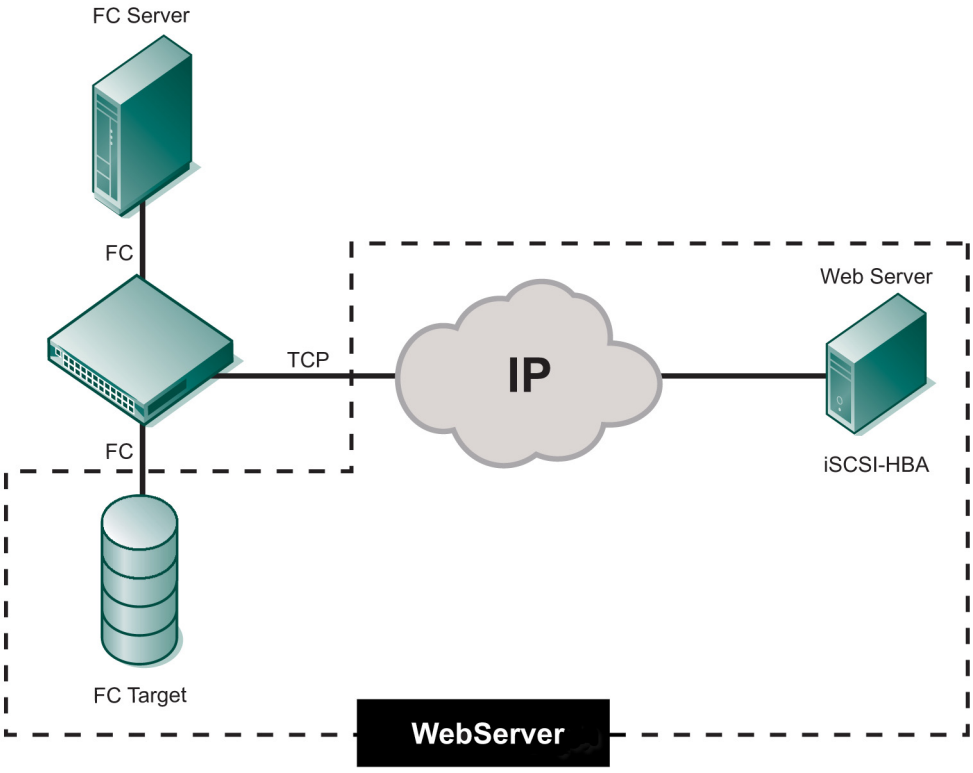


Figure 5-2 Example Configuration

The server in Figure 5-2 can either be directly connected to the SAN Router or indirectly connected via an intermediate IP network. For a direct-attached configuration, the server must be physically connected to the iSCSI-capable ports (13-16) on the SAN Router. When connected via an intermediate IP network, the server must have IP connectivity to one of the TCP ports on the SAN Router.

In the example configuration, the iSCSI server needs access to an FC disk that is directly connected to one of the FC ports on the SAN Router.

iSCSI Configuration Procedures

To configure iSCSI communication with fabrics, follow these steps:

1. Configure the TCP ports for iSCSI. Follow the procedures under *Configuring iSCSI Ports* on page 5-4.
2. Configure the iSCSI access control list. Follow procedures under *Configuring iSCSI Devices* on page 5-13.
3. Zone the iSCSI devices appropriately using SANvergence Manager, so the initiators can talk to the targets. Refer to *Zoning iSCSI Devices* on page 5-19.
4. Configure RADIUS server authentication of iSCSI initiators connected through the SAN Router. Refer to *Configuring iSCSI Authentication* on page 5-25.

Configuring iSCSI Ports

You can configure the TCP ports on the SAN Router (ports 13-16) to support iSCSI. Configuring the iSCSI ports involves the following procedures:

1. Configure the general port parameters of the Ethernet ports on the SAN Router using the procedure *Configuring the General Port Parameters* on page 5-4.
2. Configure the advanced TCP parameters using the procedure *Setting the Advanced TCP Parameters* on page 5-6.
3. Configure iSCSI ports on the SAN Router with the procedures under *Setting the iSCSI parameters* on page 5-9.
4. Configure the advanced parameters for the iSCSI ports with the procedures under *Setting Advanced iSCSI Parameters* on page 5-9.

Configuring the General Port Parameters

1. From the Element Manager, select *Configuration> Port> FC/Ethernet*.

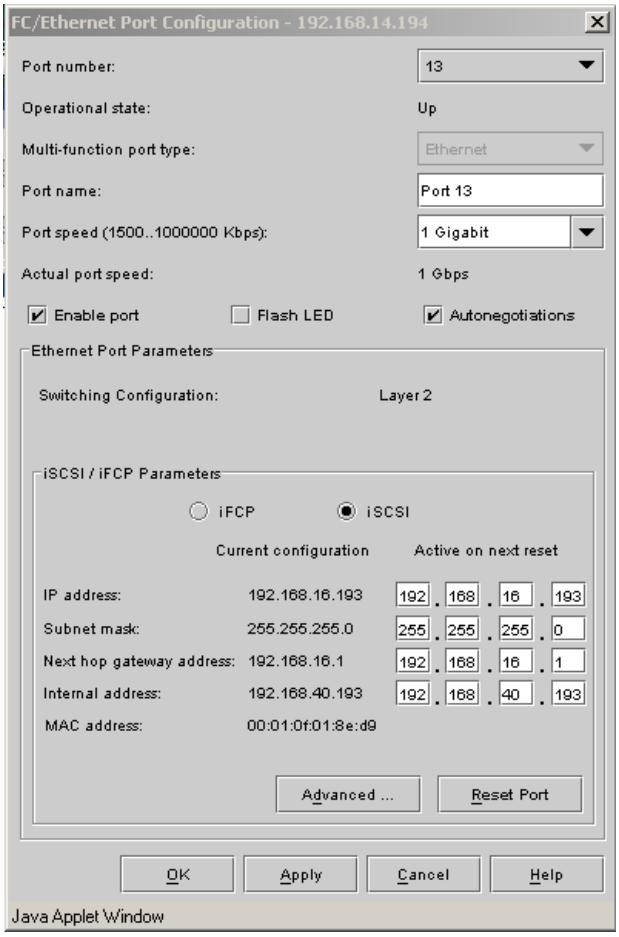


Figure 5-3 FC/Ethernet Port Configuration Dialog Box

2. Select a port. The screen is refreshed to show the operational state.
3. Type a label for this port in the *Port Name* field.
4. Set the port speed under the *Port Speed* list, if needed. Select the *Enable Port* checkbox.
5. Select or clear the *Autonegotiations* check box as required. This option determines whether the port advertises its autonegotiation properties to a receiving device per the autonegotiation specified by IEEE standard 802.3.

6. Select the *Flash LED* option to blink the port LED. You can use this option to locate the physical port in a rack of SAN Routers.
7. Select the type of the port as iSCSI.

Setting the Advanced TCP Parameters

The SAN Router provides options to optimize the TCP port behavior for storage traffic in a dedicated enterprise network through a set of advanced parameters. Use the following procedure to configure the advanced TCP parameters.

1. Click the *Advanced* button. The *Advanced TCP Configuration* dialog box appears (Figure 4-3 on page 4-6).

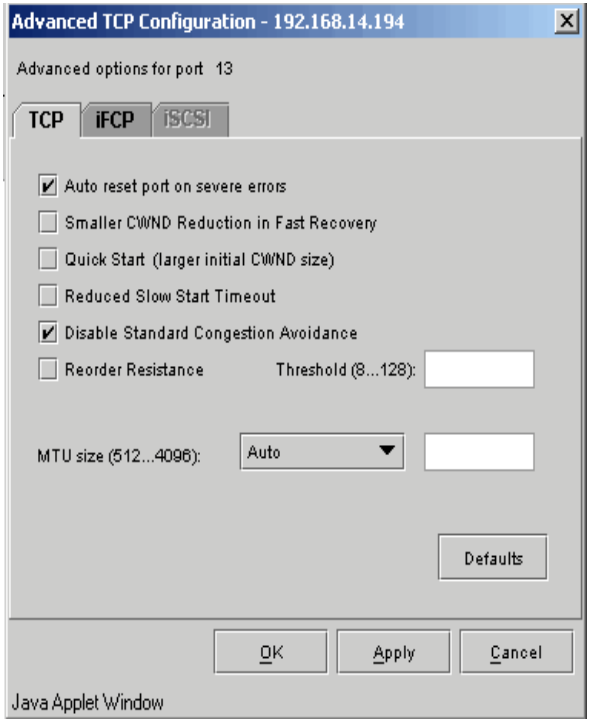


Figure 5-4 Advanced TCP Configuration

In the TCP section:

- Select *Auto-reset port on severe errors* especially when the port is a part of a mission-critical configuration.

  Manual Reset: You may not want the auto-reset option to be on when you are troubleshooting unrecoverable errors. In this case, you can do a manual reset by clicking *Reset Port* in the *FC/Ethernet Port Configuration* dialog box.

2. Set the *MTU size*.

   The MTU (maximum transmission unit) size can be used to prevent accidental fragmentation when the path (discovered) MTU value, as returned by paths from/to this port, is incorrect. This can occur with some security/encryption appliances on the network, where the MTU size may not be correctly reported. The following options are available:

   - *Auto* - Use the discovered MTU size. This is the default setting.
   - *Manual* - Forces the system to use the configured value for MTU size and DOES NOT do auto-discovery. The range is from 512 to 4096, the default size is 1500.
   - *Min* (Auto, Manual) - Does auto -discovery and uses the minimum of the discovered and configured values.

Storage-Optimized TCP Parameters:

Storage-optimized TCP is a set of enhancements made to the TCP behavior to ensure high throughput in a dedicated network in enterprise environments typically used for storage traffic. These enhancements are built on the inherent reliability of TCP by optimizing the traffic control features in a dedicated network. Following are the TCP feature enhancements that make up the storage-optimized TCP:

- Reorder resistance in case of out-of-order packet delivery.
- Quick start with higher initial value of congestion window.
- Smaller reduction in congestion window on slow start and fast retransmit.
- Disabling congestion avoidance phase in fast retransmit and fast recovery.
- Reduced slow start timeout.

You can implement these enhancements by selecting the checkboxes provided in the *Setting the Advanced TCP Parameters* on page 5-6.

1. Select *Smaller CWND Reduction in Fast Recovery* to improve the performance of the SAN Router when packet losses occur due to reordering or noise rather than congestion. When enabled, the SAN Router responds more slowly to congestion events because the send congestion window (CWND) is reduced to 7/8 of its previous value as compared to 1/2 in standard TCP.

NOTE: Do not select this option when other traffic sources sharing the same TCP link are bursty or intermittent.

2. Select *Quick Start* to improve the initial performance and error recovery performance on dedicated links with a lot of traffic. Enabling this increases the initial value for the congestion window at the beginning of TCP slow starts, and increase the congestion window size more rapidly.

   Standard TCP uses *Slow Start* to protect a network and the other traffic on it from a sudden burst that can cause congestion difficulties.

3. Select *Reduced Slow Start Timeout* to reduce the minimum *Slow Start* timeout from 500 msec to 150 msec. This improves responsiveness to congestion events that trigger *Slow Start*.

4. Disable *Standard Congestion Avoidance* to disable the slow growth mode of the SAN Router's congestion window that occurs in the standard TCP stack when a congestion event is detected.

   A congestion event occurs when there is either a transmission timeout (slowstart timeout) or sufficient duplicate acknowledgements trigger the fast recovery algorithm. The growth of the congestion window in congestion avoidance is normally at the rate of 1/cwnd bytes per ACK received. This option causes the CWND size to grow at a faster, linear rate. The SAN Router approximates this and puts a lower limit on the growth by increasing the cwnd by MIN (segement_size/8, 128) bytes per ack received.

5. Select *Reorder Resistance* for reliable links that reorder packets. Selecting this option will reduce unnecessary packet retransmission caused by packets being reordered in the TCP path.

   Selecting *Reorder Resistance* increases the number of duplicate ACKs required to trigger a *Fast Retransmit* or *Fast Recovery*. Use the next step to specify the number of ACKs.

NOTE: Enabling reorder resistance could slightly delay recovery from dropped packets in short data messages.

Specify the number of ACKs that trigger *Fast Retransmit* or *Fast Recovery* using the *Threshold* field. Valid values are between 8 to 128, with a default of 8. Larger values reduce retransmissions by causing the SAN Router to wait longer for retransmitted packets to arrive. This may delay the detection of dropped packets.

Setting the iSCSI parameters

After you have set the port as an iSCSI port, set the iSCSI parameters for the port:

1. Select the *iSCSI* check box under *iSCSI/iFCP Port Parameters*.
2. Specify the port's external IP address. This IP address will be used by the iSCSI devices to connect to the SAN Router. This is also the iSCSI Target address to configure for your iSCSI initiator. Refer to *The iFCP/iSCSI Port IP Address* on page 2-17.

   NOTE: This IP address must be in a subnet different from the SAN Router's inband subnet.

3. Specify the *Subnet mask*. This is the subnet mask to use for this port after the next port reset or system reset.
4. Configure the Next Hop Gateway address. This is the gateway address used for this port after the next system reset. TCP ports act as end nodes (hosts) attached to the WAN, and therefore may have a different gateway than the default gateway used by non-TCP ports connecting to the local SAN. Refer to *The Next Hop Gateway IP Address* on page 2-18.
5. Configure the internal address. The internal address is used by the SAN Router for its own internal operation and must be on the same subnet as the SAN Router inband IP address. Refer to *The Internal IP Address* on page 2-19

Setting Advanced iSCSI Parameters

Set the advanced iSCSI parameters to customize the iSCSI behavior of the port. Use the following steps to carry out these tasks.

1. Select the iSCSI tab from the *Advanced TCP Configuration* dialog box (refer to Figure 5-5) to specify the *iSCSI* parameters:

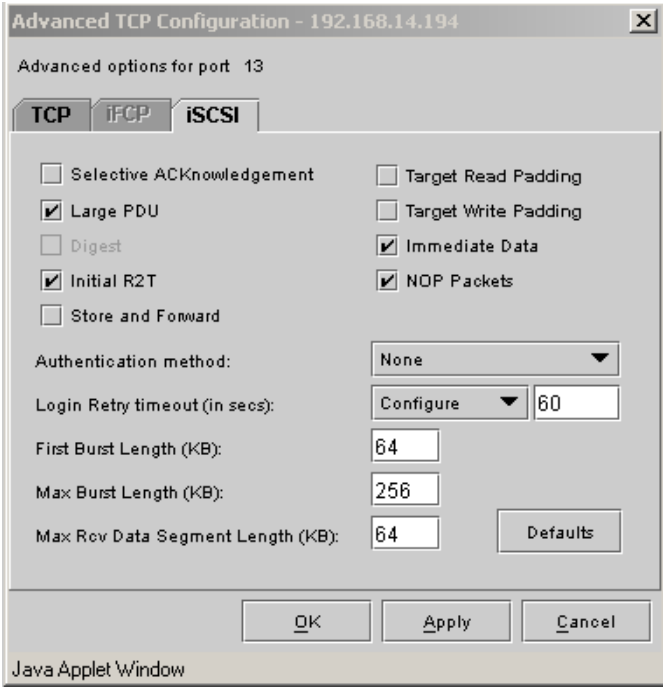


Figure 5-5 Advanced TCP Configuration iSCSI Parameters

- *Selective ACKnowledgement* - (SACK) allows acknowledgement of non-contiguous sequence numbers to reduce the amount of retransmitted data when packets are lost. Enable this for better performance in congested networks (assuming the remote device also supports SACK).
- *Large PDU* - When enabled, the SAN Router delivers data to iSCSI end nodes using maximum length iSCSI data PDUs, independent of how data is received from the FC device. The maximum length (MaxRecvDataSegmentLength) is negotiated at login.
- *Digest* - This adds a digest (extended checksum) to each payload for end-to-end integrity checking.

NOTE: Digest and large PDU cannot both be enabled at the same time.

- *Initial R2T* - (request to transfer). This skips the requirement for an initial R2T in unidirectional and the output part of bidirectional commands.
- *Store and Forward* - Enables the SAN Router to wait until all the data is received from a drive before delivering it to the initiator.
- *Target Read Padding* - Some earlier iSCSI initiators could not handle true data underrun cases, where the target returns less data than what the initiator requests. To accommodate those initiators a target read padding option is provided in the SAN Router. When enabled, the SAN Router (iSCSI target) will pad the data, if needed, to meet the iSCSI initiator's expected data length. The SCSI response indicates the actual data underrun details.
- *Target Write Padding* - Some earlier iSCSI initiators did not pad write data to 32-bit boundaries, as required by the iSCSI specification. To accommodate these initiators, the target write padding option is provided.

NOTE: If target write padding is enabled on a port, all initiators that login through that port must support it.

- *NOP packets* - This sends NOPs on idle connections to keep the iSCSI session active. The default setting is *On*.
- *Immediate Data* - Data sent along with an iSCSI command. The initiator and target negotiate support for immediate data. The default setting is *On*.
- *Authentication method* - This determines whether or not this intelligent port authenticates iSCSI initiators to determine access permission to iSCSI targets. Choices are *None*, *CHAP Preferred* (initiators are authenticated via CHAP, if the initiator supports CHAP, but other logins that do not support authentication are also accepted), and *CHAP Required* (initiators are always authenticated via CHAP).

- *Login Retry timeout (in seconds)* - This determines when the initiator can attempt to log into the SAN Router after a device is unzoned or disconnected.

— *Always Retry* - iSCSI initiators are not notified that the device is no longer available. This allows the initiator to retry indefinitely.

— *Configure* - Specify a value from 1 - 600 (secs). After this timeout expires, the SAN Router notifies the initiator that the device is no longer available.

NOTE: Change the Login Retry timeout to *Always Retry* for Windows environments. This will ensure that Windows iSCSI initiators automatically re-login. Otherwise initiators will only re-try logins for the specified time value set. This parameter has no effect on HP/UX.

- *First Burst Length (KB)* - The initiator and target negotiate maximum iSCSI data payload in bytes in a data-in or a solicited data-out iSCSI sequence. The default is *64 KB*. Other values are typically 8KB, 128KB, and 256KB.
- *Max Burst Length (KB)* - The initiator and target negotiate maximum iSCSI data payload in bytes in a data-in or a solicited data-out iSCSI sequence. The default is 256KB. Other values are typically 8KB, 64KB, and 128KB.
- *Max Rcv Data Segment Length (KB)* - The initiator or target declares the maximum data segment length in bytes it can receive in an iSCSI PDU. The default is *64 KB*. Other values are 8KB, 128KB, and 256KB.
- *Defaults* - Click to return the parameters to the default settings.

Configuring iSCSI Devices

There are two ways to configure a SAN Router with a list of iSCSI devices (access control list) allowed to connect - Automatic Addition and Manual Configuration.

To configure devices, select *Configuration>iSCSI>Devices*. The *iSCSI Devices* dialog box appears (Figure 5-7 on page 5-15).

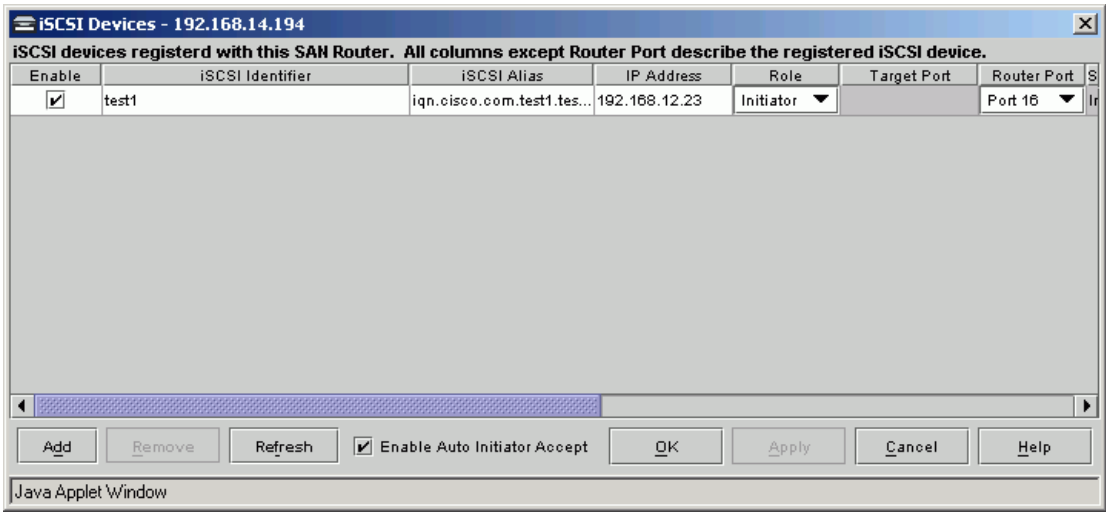


Figure 5-6 iSCSI Devices Dialog Box

Adding iSCSI Devices Automatically

A convenient way to configure the access control list (iSCSI initiators only) is to allow the SAN Router to add any iSCSI initiator that attempts to log in. Each newly discovered device appears in the *iSCSI Devices* dialog box (Figure 5-6 on page 5-13 and Figure 5-7 on page 5-15) without manual configuration.

To enable automatic configuration of the access control list, select the *Enable Auto Initiator Accept* checkbox in the *iSCSI Devices* dialog box. In addition, you can enable each iSCSI device registered with the SAN Router by clicking the checkbox in the *Enable* column for the device.

NOTE: This dialog box appears only if the software package supports iSCSI.

When an iSCSI initiator attempts a login, an entry automatically appears in this dialog box when you refresh the screen using the **F5** key. If the login from the Initiator includes an iSCSI Alias, it will overwrite any manually configured iSCSI alias.

After the initiator entry appears in the iSCSI Devices list, save the configuration from the *File* menu of Element Manager.

NOTE: Enabling the automatic configuration of iSCSI access control list does not compromise security. Even in the automatic mode, you can deny access to an initiator by disabling that entry in the Access List.

Adding iSCSI Devices Manually

To manually add devices to the access control list, follow these steps:

1. Obtain the iSCSI name of the device.

   Some initiators and targets allow the user to configure a name. Others use the method defined by the iSCSI standard to come up with a name. Refer to the documentation available with the iSCSI initiator for information on how you can configure iSCSI names.

   - If the iSCSI name is user-configurable, use this name in the *Add* dialog box later in this section. Go to step 6.
   - If the iSCSI name is not user-configurable, follow steps 5-7 to retrieve the iSCSI name of the device.

2. On the iSCSI Initiator configure the IP address of the target to be the SAN Router's TCP port.

3. Some iSCSI initiators require a fully qualified *eui* name of the target. The fully qualified *eui* name for FC targets accessed through a SAN Router can be obtained as follows:

   eui.<Port WWN of the FC target>
   Example:eui.22000020370e

   The WWN of the FC target can be obtained from the SANvergence Manager's *mSAN Configuration* window or Element Manager's *FC Device Properties* report.

4. On the iSCSI Initiator, start the iSCSI login process. Some initiators may provide a button to initiate a login; others may require a reboot of the initiator. Messages should appear in the Element Manager *Message Log*, indicating that the initiator has registered with the name server on the SAN Router.

   The string appearing after InitiatorName: and between the brackets ('[', ']') is the InitiatorName that the iSCSI initiator is attempting to login with.

5. Select this string and press ^c to copy it to the clipboard. Refer to the section titled *Granting Clipboard Access for Copy and Paste* on page 2-12 to allow copy and paste from a Java applet.

6. Select *Configuration>iSCSI>Devices*. The *iSCSI Devices* dialog box appears (Figure 5-7 on page 5-15).

NOTE: This dialog box appears only if the software package supports iSCSI.

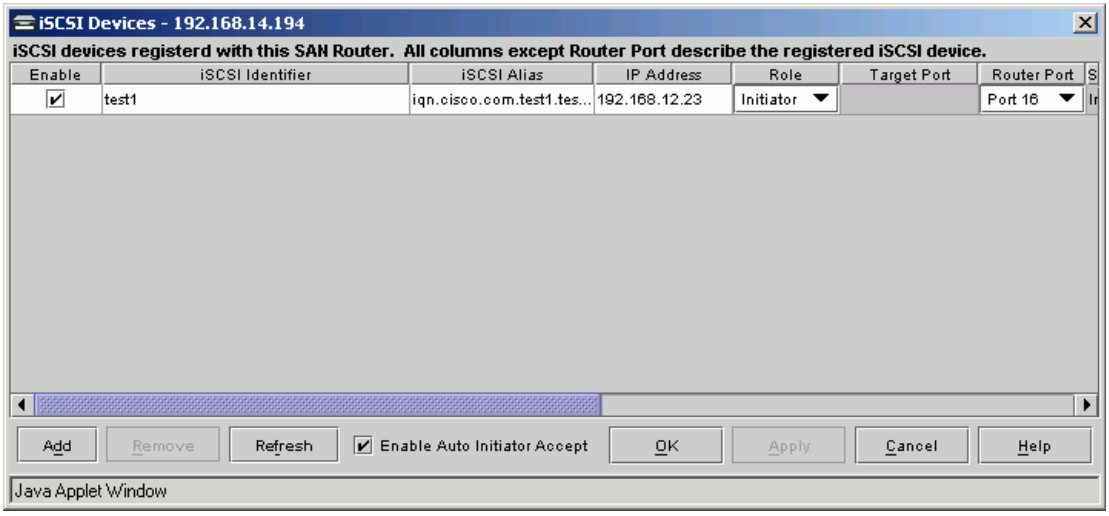


Figure 5-7 iSCSI Devices Dialog Box

7. To add a new iSCSI device, click the *Add* button. This adds a blank row to the table of devices, where you may enter the new device information.

8. Type in the iSCSI identifier, IP address of the iSCSI device, target port, SAN Router port, role and iSCSI alias (optional), and other information in the respective fields.

   iSCSI Identifier is the iSCSI Initiator Name that you copied in step 5. If it was user-configurable, make sure it matches the name configured on the server. If it was copied from the Message Log in the Element Manager to the clipboard, press ^v with the cursor in the *iSCSI Identifier* field.

NOTE: Refer to *iSCSI Devices Dialog Box Options and Data* on page 5-17 for details on these fields.

9. To edit previously-entered information, double-click the appropriate field and enter new text.
10. To remove an iSCSI device, select the row by single-clicking anywhere in the row, then click the *Remove* button. Select a range of rows by pressing **Shift** while clicking a row. You can select multiple rows by pressing **Ctrl** while clicking on each additional row.
11. To accept the input, click *OK* or *Apply*.

    To discard your changes, press **F5** to refresh the window with the current SAN Router configuration, or click *Cancel* to dismiss the window.

iSCSI Devices Dialog Box Options and Data

The following describes the fields in the *iSCSI Devices* dialog box where you can input information.

- *Enable* - Select this to register the iSCSI device with the name service.
- *iSCSI Identifier* - The unique textual name assigned to the iSCSI device by the device manufacturer.

  If the device is an FC device masquerading as an iSCSI device, it may have an identifier similar to eui.<16 hex digits>, where eui is the extended unique identifier and the hex digits are the FC WWN.
- *IP Address* - The IP address of the iSCSI device.
- *Target Port* - The TCP port for the iSCSI service. The typical iSCSI service port number is 3260. This field is not used for iSCSI initiators.
- *Router Port* - The port on the SAN Router to use for reaching the iSCSI device. The specific SAN Router port becomes the default route for traffic to the iSCSI device. The port must be one of the SAN Router's TCP ports.
- *Role* - The type of iSCSI device that this device can be : *Initiator*, *Target*, or *Both*.
- *iSCSI Alias* - A user-friendly name for the iSCSI device if it does not already have an alias (a factory-assigned alias overrides what you might enter here). The maximum length is 80 characters.

  Changing the iSCSI alias causes the SAN Router to close any active iSCSI sessions from this initiator, re-register with the mSNS, and reopen the sessions. This process takes a few seconds to complete.
- *Edit Status* - Status conditions include: *OK*, *Added not Applied*, *Edited not Applied*, and *Removed not Applied*. This clarifies which rows you've added, modified or marked for removal. All table changes are effective after you click *OK* or *Apply*. At that point, the requested changes are made on the SAN Router. *Added* and *Modified* rows will then show *OK* and removed rows will disappear. This column is read-only.

You cannot edit the remaining columns of the iSCSI device table. They show the SAN Router storage information associated with each iSCSI device. The iSCSI devices are registered in the mSNS as if they were FC devices. Each iSCSI device is registered as a different FC node. The iSCSI identifier becomes the FC *Node Symbolic Name*. The iSCSI alias becomes the *FC Port Symbolic Name*. These non-editable parameters include:

- *Session Status* - Session status is Active or Inactive. It indicates whether the iSCSI device is logged-in and communicating with another device via the SAN Router.
- *Port WWN* - 8-byte FC Port World-Wide Name registered in the storage name service for this iSCSI device. The *Port WWN* is made up by the SAN Router and is persistent across reboots.
- *Node WWN* - 8-byte FC Node World-Wide Name registered in the storage name service for this iSCSI device. The *Node WWN* is made up by the SAN Router and is persistent across reboots.
- *FCID* - 3-byte FC identification registered in the storage name service for this iSCSI device. The FCID is made up by the SAN Router and may change after a reboot.
- *Port IP Address* - IP address registered in the local storage name service for this external iSCSI device. This is the IP address for the SAN Router port used to reach the iSCSI device. Configure the address for each TCP port in the Element Manager's *FC/Ethernet Port Configuration* dialog box. mSAN traffic for the iSCSI device is sent to this address in the SAN Router so that the SAN Router can translate to iSCSI and forward the traffic to the real device's address.

Zoning iSCSI Devices

Zoning is the process of controlling which targets are accessible to the initiator. Targets could have one or multiple LUNs. SAN Routers support LUN mapping/masking capabilities within the SAN Router for iSCSI initiators. If you want to leverage the LUN Mapping/Masking feature, use the following procedure.

Zoning without LUN Mapping/Masking

1. Start SANvergence Manager
2. Select the proper mSAN from the list of mSANs in the *mSAN* pane.
3. Select *mSAN Configuration* to display the m*SAN Configuration* window.

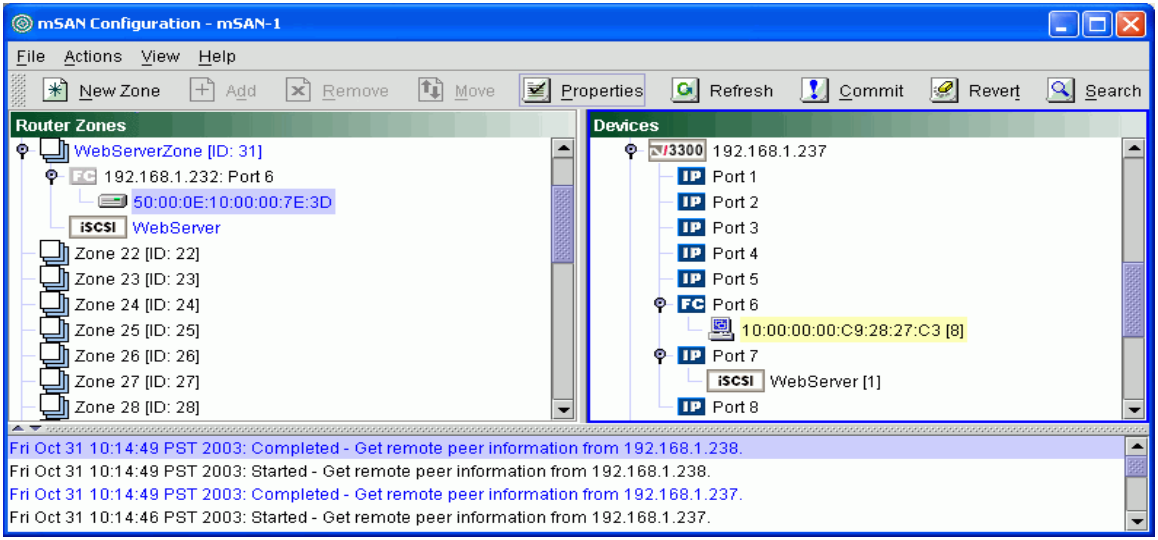


Figure 5-8 Zoning Configuration Window

4. Click *New Zone* to display the *New Zone* dialog box.
5. In the *New Zone* dialog box, type a zone name (WebServerZone).

6. Select the newly-created zone and the iSCSI initiator (WebServer) and click *Add*. With the newly-created zone selected, select each storage device you want the iSCSI initiator to access, and click *Add*.
7. Click *Commit* to save the changes to flash.

NOTE: The iSCSI device you added in Element Manager automatically appears in the *Devices* tree of the *mSAN Configuration* screen under the appropriate SAN Router port that it was configured for.

After zoning the iSCSI initiator, it will be able to login to the FC target. You may need to restart the iSCSI initiator before it can login to the target.

Zoning with LUN Mapping/Masking

NOTE: To use the LUN Mapping/Masking feature, the FC target needs to be directly connected to a port on the SAN Router. Also, LUN Mapping/Masking feature is applicable only to iSCSI initiators; FC initiators recognize the RAID in its native form.

FC targets can have their LUNs mapped and/or masked to an iSCSI initiator. The process of making visible certain LUNs and hiding certain others is referred to as LUN masking. Assigning the physical LUN (PLUN) to a new number (called the virtual LUN or VLUN) is called LUN mapping and provides for assigning sequential VLUN numbers that span non-contiguous PLUNs.

Configure LUN mapping/masking separately for each zone membership. You can add the same storage device to another zone, and expose different LUNs to the other zone.

Enabling the LUN Mapping and Masking Feature

Enable the LUN mapping and masking feature on the SAN Router from the *Actions* menu of the *mSAN Configuration* window in SANvergence Manager. Select *Enable LUN Mapping* to enable the feature. By default, this service is not enabled.

NOTE: If the feature is disabled, any previously created LUN maps and masks are deleted from the SAN Router.

Setting Up a LUN Map and Mask

1. In the *mSAN Configuration* window, click *New Zone* to display the *New Zone* dialog box.
2. In the *New Zone* dialog box, type a zone name.
3. Select the newly-created zone and the FC Target with multiple LUNs that you want the iSCSI Initiator to access, and click *Add*. The zone configuration at this point is shown in the Figure 5-9.

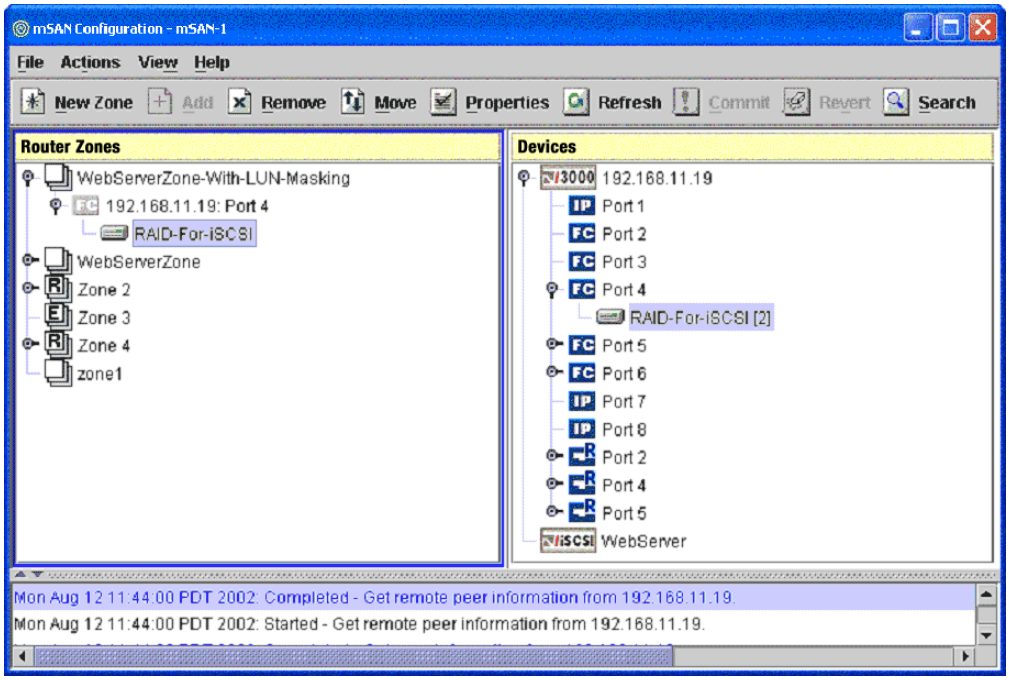


Figure 5-9 mSAN Configuration Window

4. Right-click the FC target in the Router Zones section and launch the *LUN Mapping/Masking* dialog box (Figure 5-10 on page 5-22). By default, all LUNs are selected (visible).
5. Select the LUNs that you want to provide access to the initiator. Set a selected LUN to a VLUN value of zero. You can change the VLUN value of other selected LUNs, but must ensure that one of the selected LUNs have VLUN set to zero. Click OK.

6. Add the iSCSI initiator to the new zone. The new changes are visible in the mSAN Configuration window, as shown in Figure 5-11 on page 5-23.

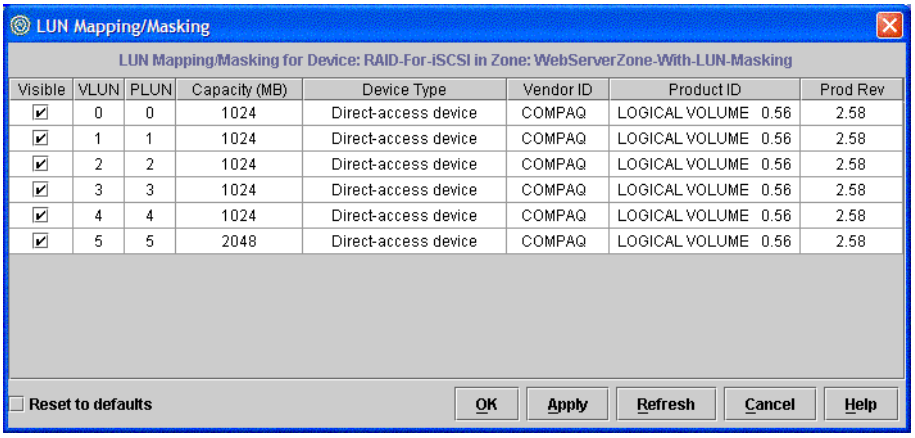


Figure 5-10 LUN Mapping/Masking Dialog Box

CAUTION

Adding a storage device with multiple LUNs to a zone that has initiators exposes all LUNs to the initiator. To selectively expose the LUNs to the initiators, carry out LUN Masking and Mapping first before you add a storage device to a zone with initiators in it.

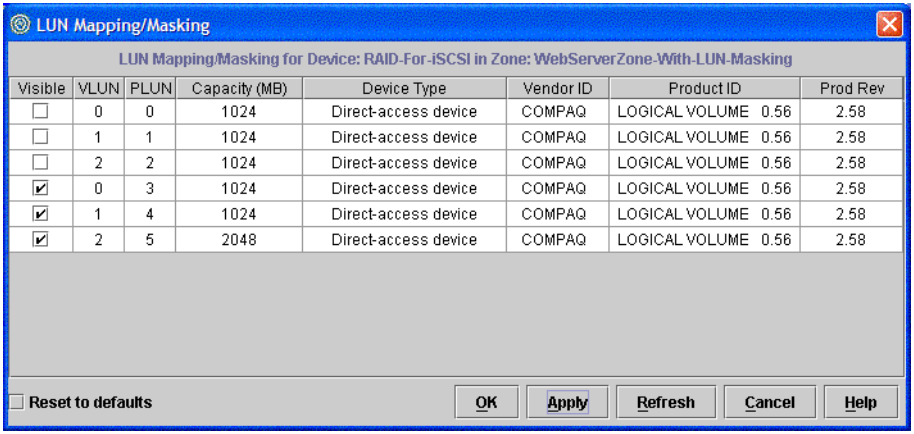


Figure 5-11 LUN Mapping/Masking Dialog Box

7. Click *Commit* to save the changes to flash. Now the iSCSI initiator will be able to login to the FC target and recognize the selected LUNs.

   Figure 5-12 on page 5-24 shows the three LUNs visible through the Windows 2000 disk management function.

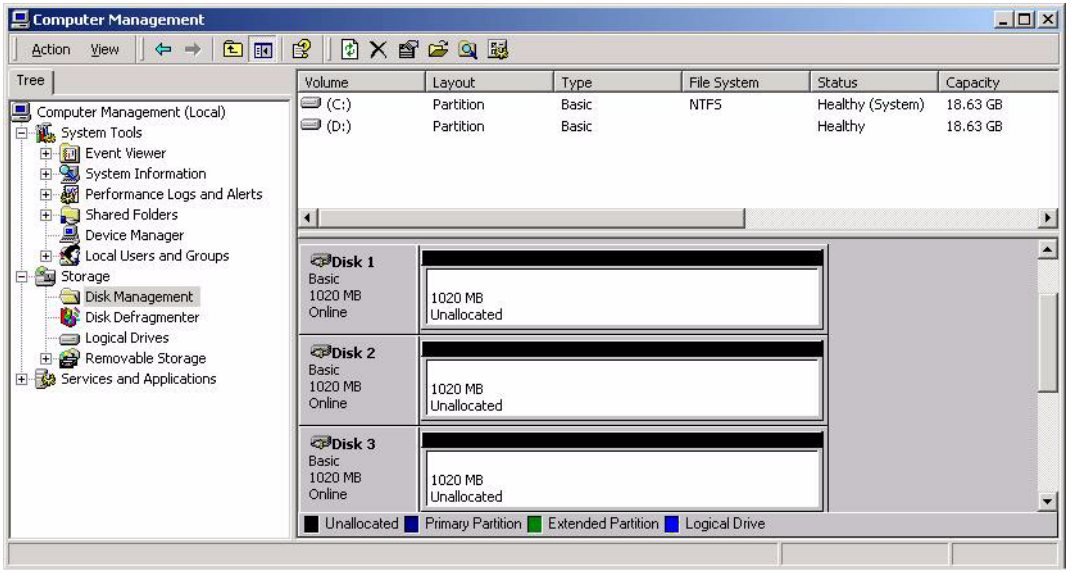


Figure 5-12 Computer Management Window

CAUTION

Changing the number of LUNs for a zoned target deletes the LUN map and forces the SAN Router to expose all LUNs to any initiators in the zone. To avoid this, remove the initiators from the zone before you change the number of LUNs on the target, and add the initiators back to the zone with appropriate permissions.

Configuring iSCSI Authentication

SAN Routers support CHAP-based authentication of iSCSI initiators in conjunction with an external RADIUS server.

Challenge Handshake Authentication Protocol (CHAP) provides a type of authentication between an agent (typically a network server) and the client program. Both share a predefined *secret*, which they verify during an authentication login sequence.

The RADIUS protocol is used for access authentication and accounting. The SAN Router supports a RADIUS client, which connects to a configured RADIUS server to authenticate logins from iSCSI initiators.

As part of the initial handshake between an initiator and the iSCSI port in the SAN Router, an authentication protocol is negotiated (either CHAP or none). If the protocol is CHAP, the SAN Router sends some random data (the "challenge") to the initiator. The initiator returns the challenge, encoded with the initiator's secret. The SAN Router's RADIUS client sends the encoded challenge to the RADIUS server. The RADIUS server uses its copy of the initiator's secret to confirm that the challenge was properly encoded. The iSCSI port sends an *Accept* or *Reject* to the iSCSI initiator based on the authentication response from the RADIUS server.

You can configure up to two RADIUS servers per SAN Router to authenticate iSCSI initiator logins. The primary RADIUS server is contacted first and, if no response is received within a timeout period, the secondary server is contacted.

The sample configuration in Figure 5-13 shows a SAN Router set up to use an external RADIUS server to authenticate iSCSI initiators.

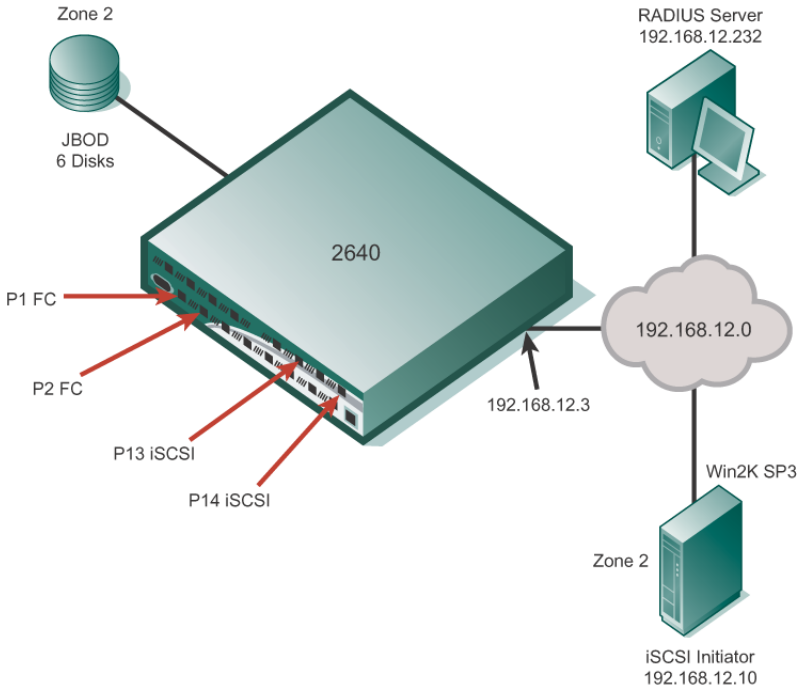


Figure 5-13 Sample Authentication Configuration

A typical interaction would be as follows:

1. The iSCSI initiator creates a "portal" session with the SAN Router.
2. The iSCSI initiator is configured to use CHAP authentication. The password and username have been configured in the iSCSI initiator.
3. The iSCSI initiator does not communicate with the RADIUS server directly. The SAN Router acts as a mediator between the iSCSI initiator and RADIUS server.
4. If the RADIUS server grants permission to the iSCSI port request, then the SAN Router will grant access to "zoned" FC targets to the iSCSI initiator.

The external RADIUS server can be anywhere on the network, as long as it is reachable from the out-of-band management port, or the iSCSI port used to reach the iSCSI initiator.

Using Static Routes

If your RADIUS server is attached via the SAN Router's management port, then you need to add a static route to the RADIUS server to reach the TCP port's internal address. Refer to Figure 5-14 on page 5-27.

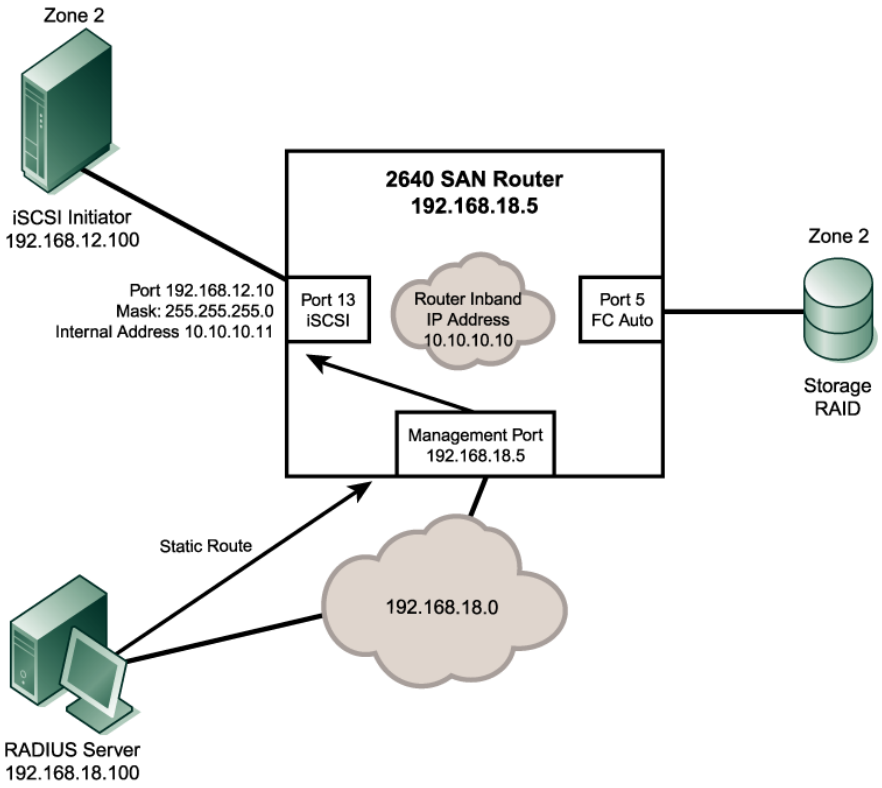


Figure 5-14 RADIUS Server on Management IP Subnet Static Routes

NOTE: The only way the RADIUS server can access the internal IP network is through a static route within the RADIUS Server. This allows the RADIUS server to send the authentication message to the management port which, in turn, passes the login request to the iSCSI initiator.

For details on setting up different configurations for RADIUS server access, refer to *Supported RADIUS Server Configurations* on page 5-32.

If you are having problems authenticating iSCSI login requests, make sure that the RADIUS server has logical connectivity to the iSCSI port address. You can confirm this with a ping to the internal address from the RADIUS server (ping 10.10.10.11). If the ping fails, iSCSI initiator will never receive the authentication grant. If the RADIUS server is not in a subnet attached directly to the SAN Router (not in the management port subnet, inband address subnet, or TCP port subnet), then you may need to add a static route to the SAN Router to reach the RADIUS server.

For more information and procedures on configuring static routes, refer to *Static Routes* on page 2-36.

Using RADIUS Authentication

Use the following steps to configure the SAN Router to use RADIUS authentication.

1. From Element Manager, select *Configuration>iSCSI>RADIUS Server Configuration*.

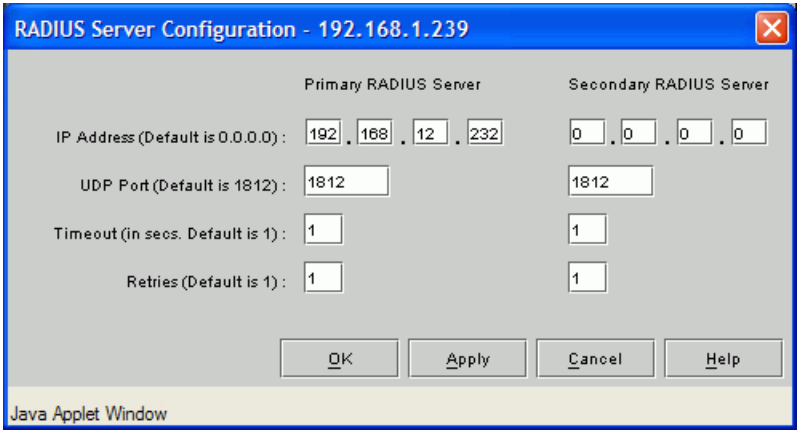


Figure 5-15 RADIUS Server Configuration Dialog Box

2. Enter the IP address of the primary and secondary RADIUS servers where this SAN Router will send device-login authentication requests. To indicate that this server is not in use, set the value to 0.0.0.0

3. Enter the UDP port on the RADIUS server to send the authentication requests. The RFC 2865 defaults this port to 1812, but can be different for other implementations.
4. Enter the timeout value in seconds. This is the timeout for each retry. If authentication does not occur and all retries have timed out, the secondary RADIUS server is contacted.
5. Enter the number of retries. If authentication does not occur after this number of retries, the next RADIUS server is contacted.
6. Use the *Advanced TCP Configuration* dialog box to set the iSCSI port to authenticate new initiators.
   - Select *Configuration>Port>FC/Ethernet* to display the *FC/Ethernet Port Configuration* dialog box.
   - Select the iSCSI port using the *Port number* drop-down list.
   - Click *Advanced* to display the *Advanced TCP Configuration* dialog box (refer to Figure 5-15).
   - Set the *Authentication Method* to *CHAP Required*.

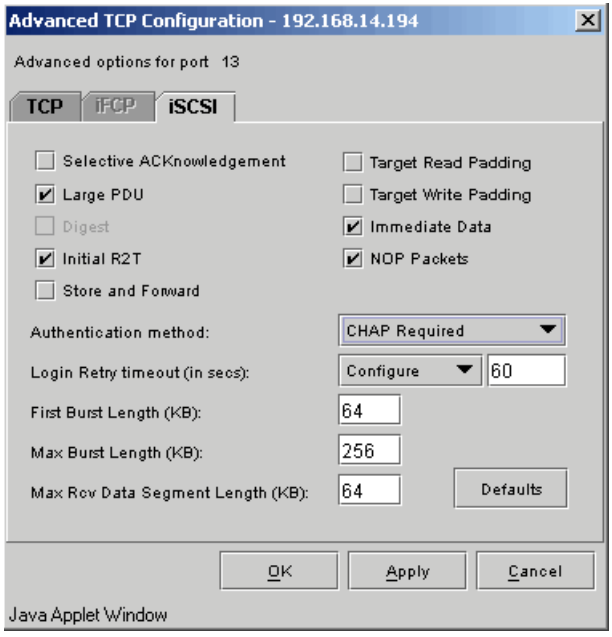


Figure 5-16 Advanced TCP Configuration Dialog Box

7. Choose *Save Configuration to Flash* from the *File* menu to permanently save the configuration to flash memory.

Configuring the iSCSI Initiator for Authentication

Refer to the documentation of your iSCSI initiator for instructions on setting up the initiator for CHAP authentication. Following is a procedure for using the Microsoft iSCSI initiator.

1. Start the Microsoft iSCSI initiator and enter the iSCSI port IP address on the SAN Router as the target portal address (Figure 5-17 on page 5-30).

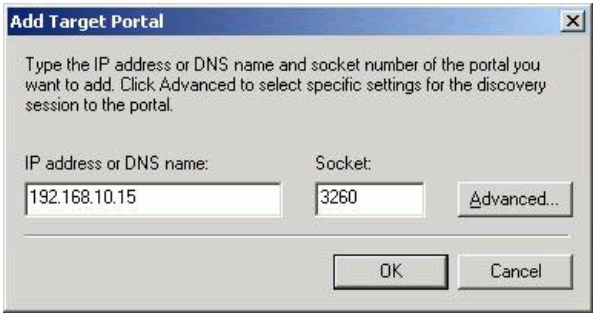


Figure 5-17 Add Target Portal Dialog Box

2. Click *Advanced* to display the *Advanced Settings* dialog box.

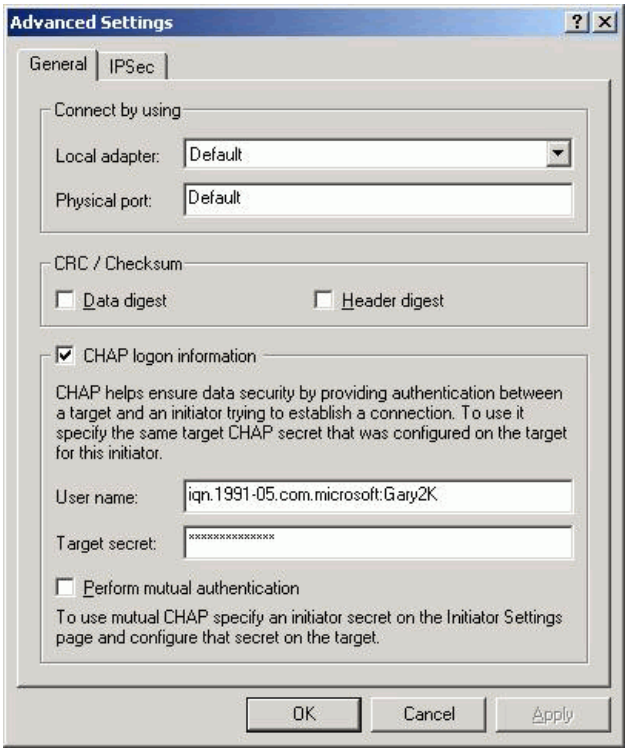


Figure 5-18 Add Target Portal Advanced Settings Dialog Box

3. Enter a user name. Make sure that the *Target secret* matches the Password and Secret in the user and clients.conf file, if you are using the freeRADIUS RADIUS server.
4. Click *OK* to close the dialog box.
5. Click *OK* on the *Add Target Portal* dialog box.
6. If devices have been zoned properly (refer to *Zoning iSCSI Devices* on page 5-19), verify login to the target portal and initiator function:
   - Select *Available Targets* in the initiator to display current targets and status.
   - Select the target name to display the *Log on to Target* dialog box.
   - Click *OK* to log on to the target.

- Verify that the target displays on the *iSCSI Initiator Properties* dialog box as "connected." If it doesn't, you must check the storage array for configuration problems.
- After you verify that an active session exists for the target, check the message log of the bottom of the Element Manager window on the SAN Router with the iSCSI port. A message should display that the iSCSI initiator is registering with the name server.
- Open the *iSCSI Devices* dialog box through the SAN Router's Element Manager, by selecting *Configuration>iSCSI>Devices*. The initiator should be visible in this screen.

Supported RADIUS Server Configurations

This section provides examples of supported RADIUS Server configurations and procedures for setting up these configurations.

Configuration 1 - RADIUS Server on the Same Subnet as the iSCSI Initiator

In this configuration, the RADIUS server is on the same subnet as the iSCSI initiator (refer to Figure 5-19). The RADIUS client on the SAN Router will communicate with the RADIUS server via the iSCSI port on the SAN Router.

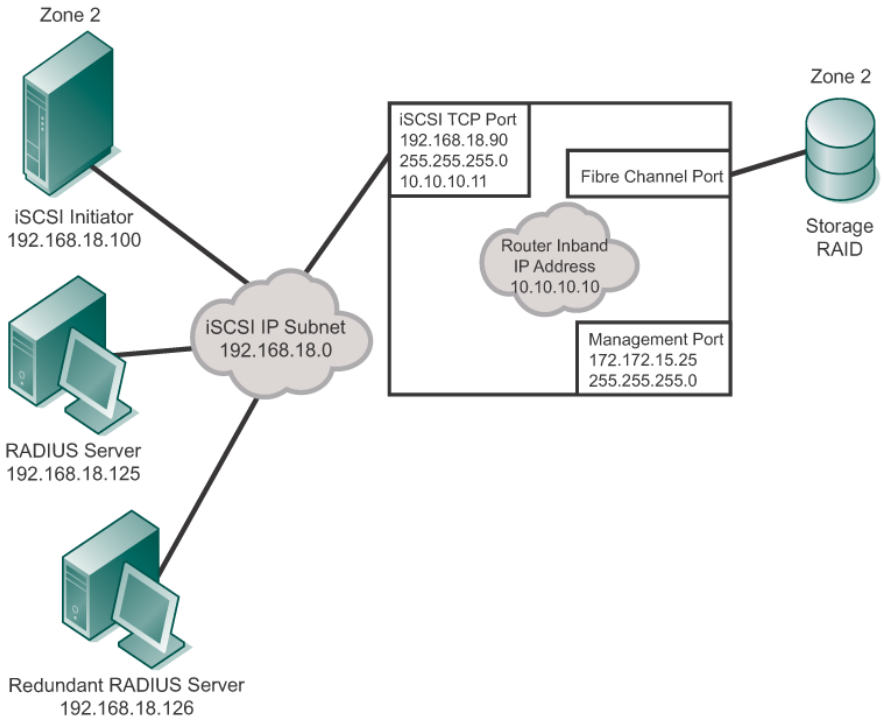


Figure 5-19 RADIUS Server Located on the iSCSI Subnet

Figure 5-20 shows an example of the associated *RADIUS Server Configuration* dialog box in the Element Manager. Display this dialog box by selecting *RADIUS Server Configuration* under the *Configuration* menu, *iSCSI* submenu.

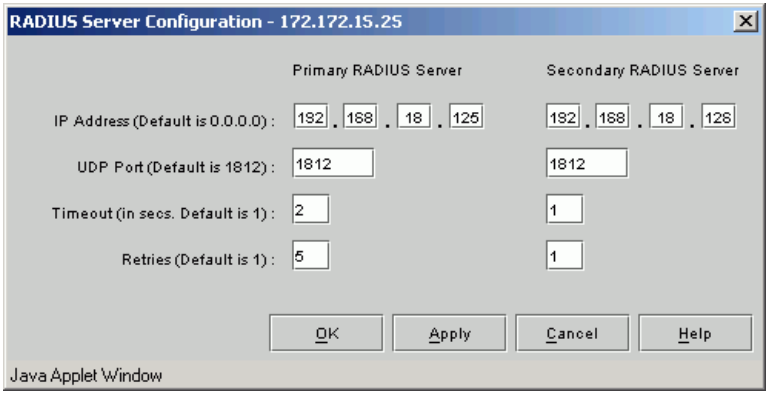


Figure 5-20 RADIUS Server Configuration Dialog Box

Configuration 3 - RADIUS Server Located on the Same Subnet as the Management Port

In this configuration, the RADIUS server is on the same subnet as the SAN Router's 10/100 management port (refer to Figure 5-21 on page 5-35). The RADIUS client on the SAN Router will communicate with the RADIUS server via the 10/100 management port on the SAN Router.

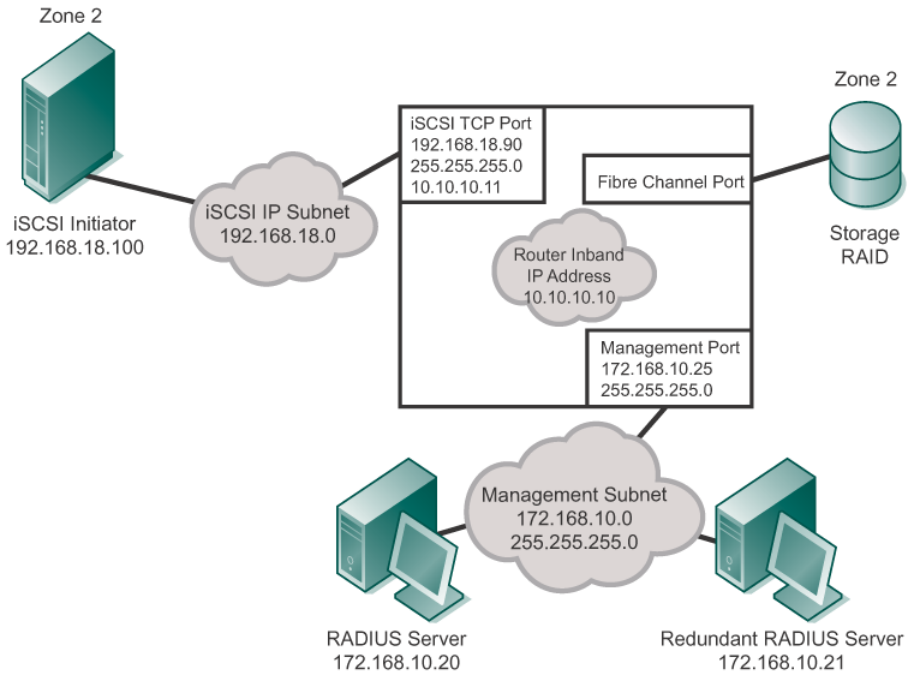


Figure 5-21 RADIUS Server Located on the Management Subnet

Note that you need to add a static route to the RADIUS server that tells the IP stack on the RADIUS server that the path to the iSCSI port of the SAN Router is through its management port IP address.

The RADIUS Server requires a static route logically pointing to SAN Router's internal address:
"route add 10.10.10.11 .255.255.255.255. 172.168.10.25."

Use the "ping" command to verify logical connectivity: "ping 10.10.10.11".

Figure 5-22 on page 5-36 shows an example of the associated *RADIUS Server Configuration* dialog box in the Element Manager. Display this dialog box by selecting *RADIUS Server Configuration* under the *Configuration* menu, *iSCSI* submenu.

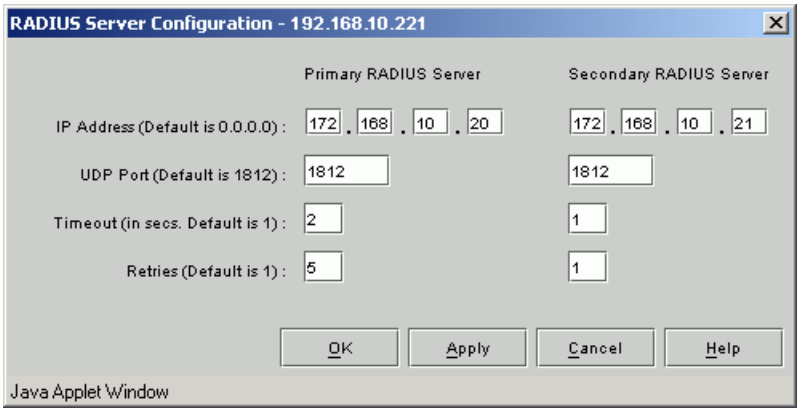


Figure 5-22 RADIUS Server Configuration Dialog Box

Configuration 4 - RADIUS Server Located One Hop from Management Subnet

In this configuration, the RADIUS server is on a subnet that is one hop away from the SAN Router's 10/100 management subnet (refer to Figure 5-23 on page 5-37). The RADIUS client on the SAN Router will communicate with the RADIUS server via the 10/100 management port on the SAN Router.

NOTE: You must add a static route to the RADIUS server and all the intermediate SAN Routers that tells them the path to the internal IP network of the SAN Router through its management port IP address.

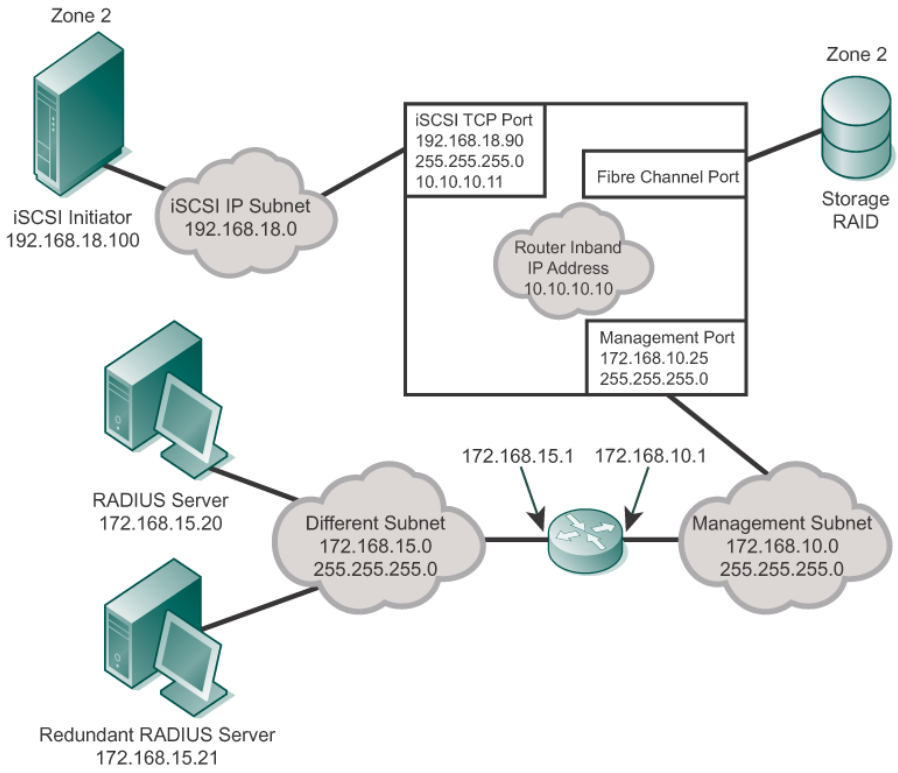


Figure 5-23 RADIUS Server Located One Hop from Management Port

Figure 5-24 on page 5-38 shows an example of the associated *RADIUS Server Configuration* dialog box in the Element Manager. Display this dialog box by selecting *RADIUS Server Configuration* under the *Configuration* menu, *iSCSI* submenu.

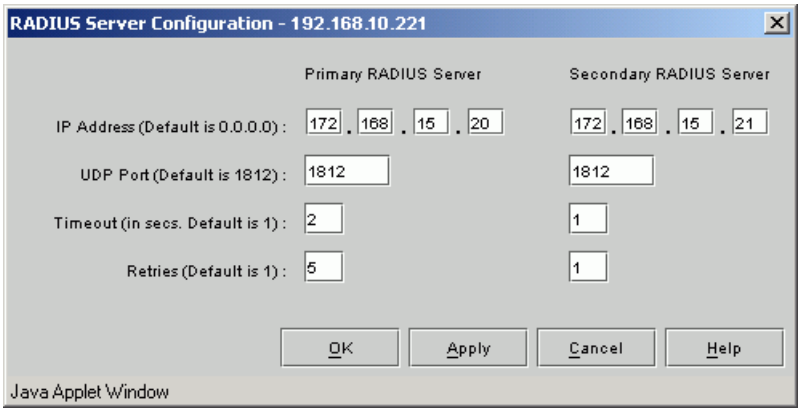


Figure 5-24 RADIUS Server Configuration Dialog Box

If the RADIUS Server resides on a subnet that cannot be directly accessed from the SAN Router, establish a static route path between the server and the SAN Router. The Static Route Table (Table 5-1) shows all necessary static routes in this example.

Table 5-1 Static Route

Static Route Source	Destination Address	Mask	Gateway Address
RADIUS Server	10.10.10.11	255.255.255.255	172.168.15.1
Redundant RADIUS Server	10.10.10.11	255.255.255.255	172.168.15.1
Router	10.10.10.0	255.0.0.0	172.168.10.25
SAN Router	172.168.15.0	255.255.255.0	172.168.10.1

Figure 5-25 on page 5-39 illustrates the *Add Static Route* dialog box in the Element Manager where you add static routes. Display the *Add Static Route* dialog box by selecting the *Add* button on the *Static Routing Configuration* dialog box. Display the *Static Routing Configuration* dialog box by selecting the *Static Routing* option from the *Configuration* menu.

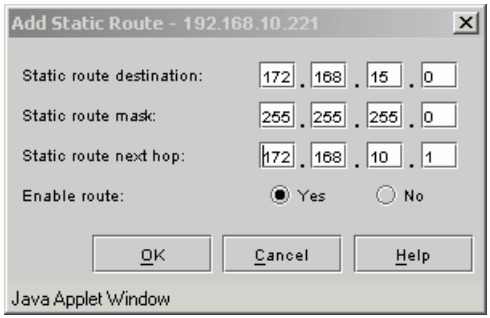


Figure 5-25 Add Static Route Dialog Box

Configuration 5 - Unsupported Case, RADIUS Server Located on Alternate TCP Port

In this configuration, the RADIUS server is on a subnet that is reachable *only* via a different iSCSI-capable port (refer to Figure 5-26 on page 5-40). This configuration is not supported. However, if there is an external route between the two ports provided by an external IP Router, the RADIUS server can be on a subnet that one of the other iSCSI-capable ports are on.

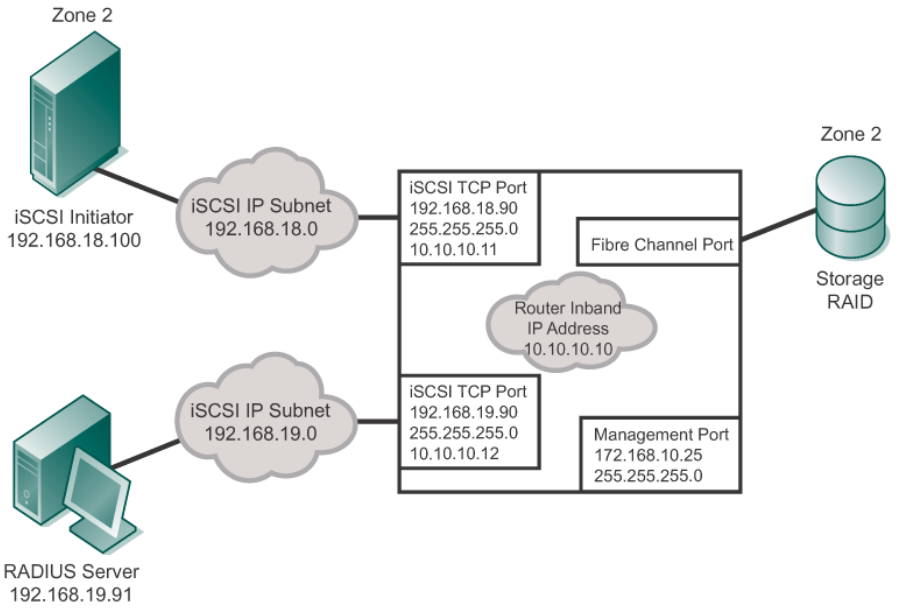


Figure 5-26 RADIUS Server Located on Alternate TCP Port

The primary and secondary RADIUS servers can be connected in any combination of the supported configurations. For example, the primary RADIUS server can be located on iSCSI port's subnet while the secondary RADIUS server can be located on iFCP subnet.

Use the “ping” command to verify logical connectivity from the RADIUS server to the iSCSI port (internal or external). When connecting the RADIUS server to the iSCSI external port subnet, the external iSCSI port IP address is used.

6

Monitoring SAN Router Operation and Connections

This chapter provides details on how to monitor SAN Router performance and operation in the network using Element Manager.

Use the following links to move through the chapter.

Using the Element Manager Tools

Device View

The device view in the *Element Manager* screen portrays the status of the SAN Router, current as of the most recent poll. Shown below is the *Device View*.

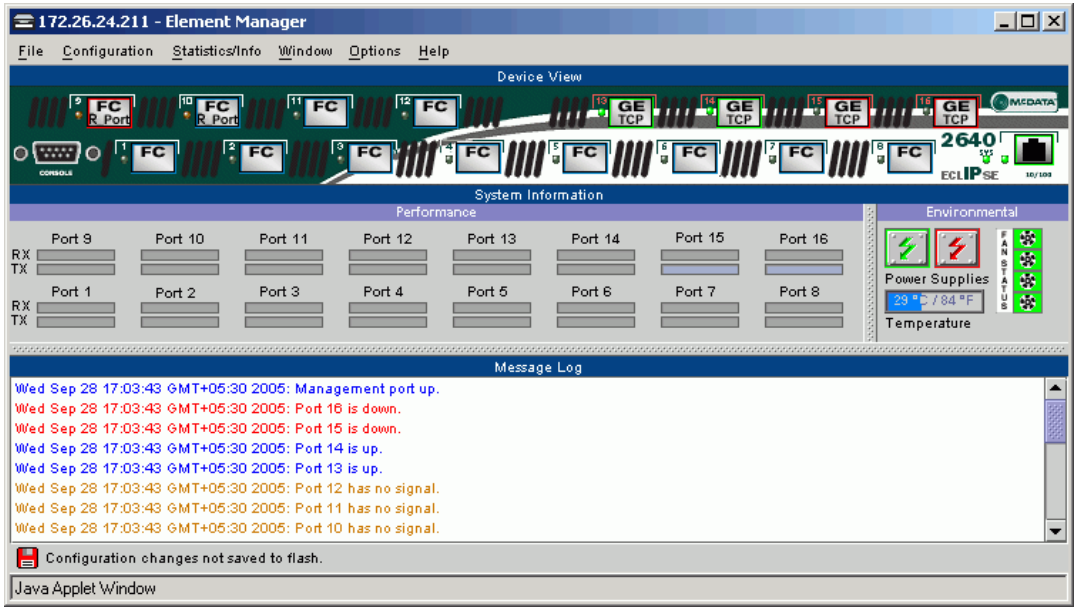


Figure 6-1 Device View for the SAN Router

Port Icons

Each port is represented by an icon that shows the port type, individual port LED, and a colored status border around the icon.

Port types may be:

- FC - Fibre Channel Port
- FC R_Port - Fibre Channel R_ Port
- TCP - TCP Port

The management and console ports have their own unique icons.

To determine what the colors in the *Device View* mean, choose *Color Legend* from the *Help* menu to display the *Color Legend*.

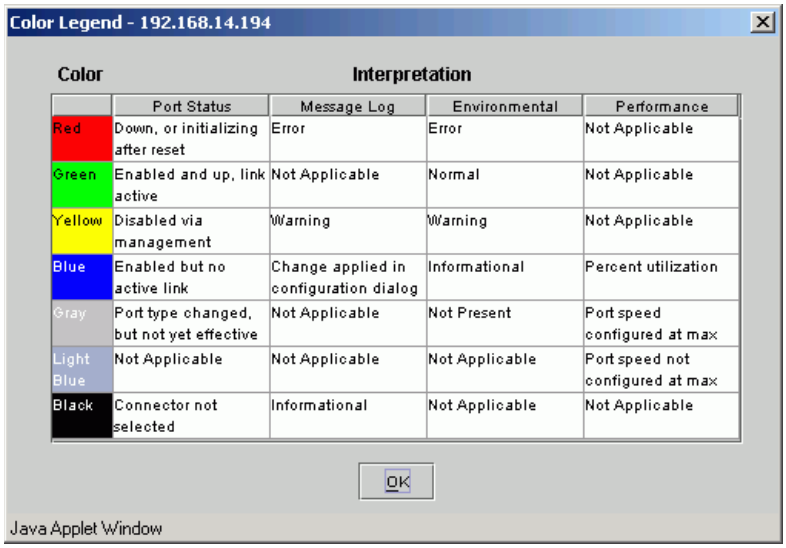


Figure 6-2 Color Legend window

LED and Icon Colors

Table 6-1 lists the meaning of the port LEDs, fan, and temperature icon colors in the *Device View*. A single LED by each port indicates port status.

Table 6-1 Port LED Colors

LED Label	Color	Meaning
Port LEDs	Green -	FC/R port link up.
	Amber - Yellow	FC port link up.
	Gray/ Off	Port type has changed and needs reset.
10/100 Mbps Management Port	Green -	FC/R port link up.
	Gray/ Off	The link is down.

Port Border Colors

The following table defines the meaning of the colored borders around the FC, TCP, and management port icons in the Device View.

Table 6-2 Eclipse 2640 Port Border Colors in the Device View

Port	Border Color	Meaning
FC/Ethernet	Green	Port is up.
	Yellow	Port disabled by user.
	White	Port type changed; waiting for reset to effect new type.
TCP	Red	Port is down or no link.
FC	Blue	Port is down or no link.
Management	Green	Port is up.
	Red	Port is down.

Port Tooltips

To view summary information for a port, position the pointer over the port icon and pause. The tooltip automatically appears. Figure 6-3, Figure 6-4, and Figure 6-5 on the following pages are tooltip examples for an FC port, FC R_Port, and an iFCP/iSCSI port.

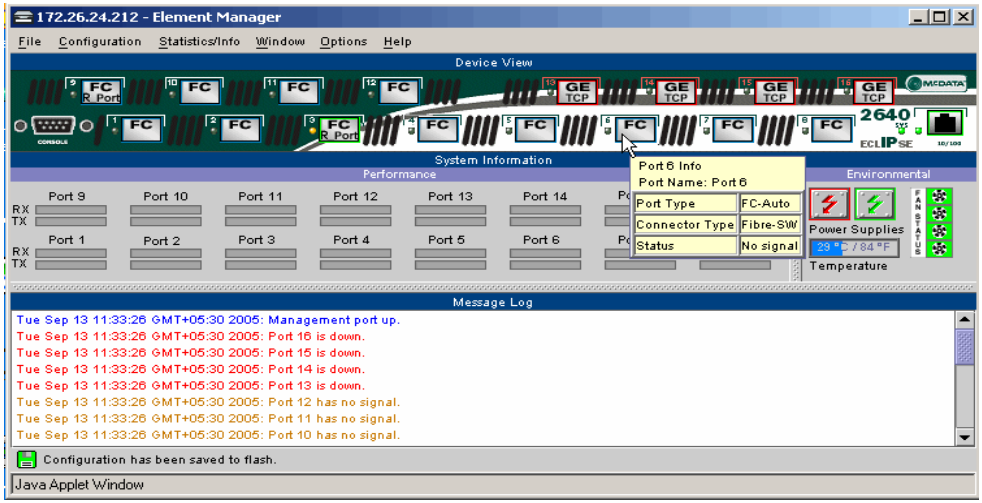


Figure 6-3 FC Port Tool Tip

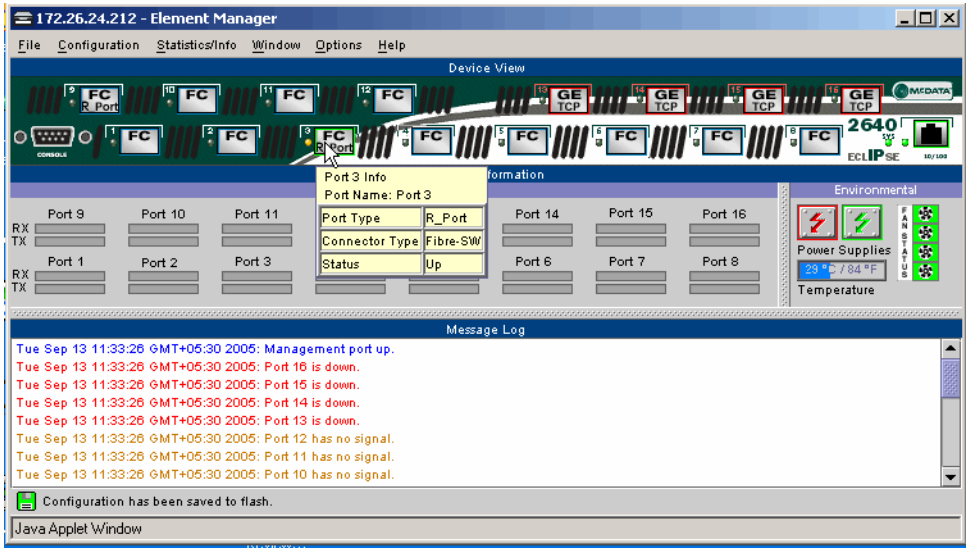


Figure 6-4 FC R_Port Tool Tip

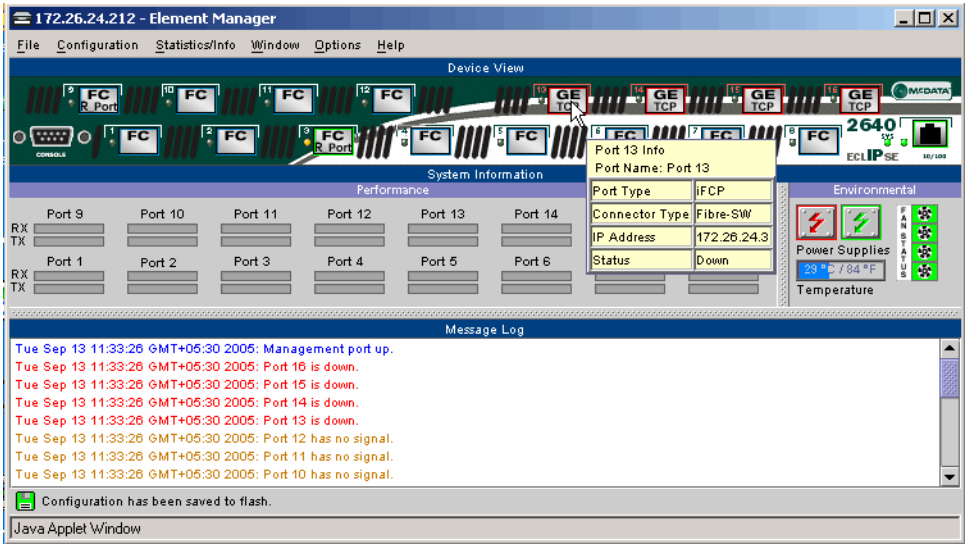


Figure 6-5 iFCP Tool Tip

System Information

The *System Information* panel in the *Device View* (Figure 6-6) displays the operating conditions of the SAN Router as of the most recent poll.

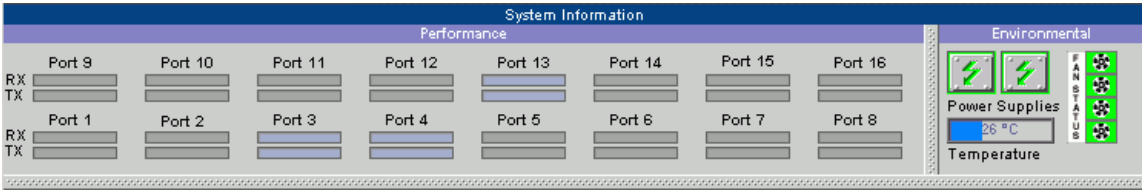


Figure 6-6 System Information Panel

Operational Status

LEDs on the Device View indicate status of system components.

Table 6-3 System Status LEDs

LED Label	Color	Meaning
Power Supplies		The colored borders around the two icons labeled Power Supplies monitor the two power supplies. If green, good DC power is being provided by the respective power supply. If a power supply icon border is red, the power supply has failed - check the power supply.
	Green	Green indicates normal operation.
	Amber	Amber indicates low power supply.
	Red	Red indicates failure.
Fans		The colored border around four stacked fan icons indicate the operating status of each fan.
	Green	Green indicates normal operation.
	Amber	Amber indicates low fan speed.
	Red	Red indicates failure.
Temperature Bar	Blue	Indicates the internal temperature of router chassis.The temperature bar turns yellow when the temperature approaches the recommended maximum and turns red when the temperature exceeds the recommended maximum.
System	Green	Indicates that the system is operational.

Performance

The bars below each port number indicate the average percentage of port bandwidth used on the previous poll cycle. The top bar represents packets received (RX); the bottom bar represents packets transmitted (TX). To view the performance bar tooltip, just position your pointer over the bar and pause (Figure 6-7).

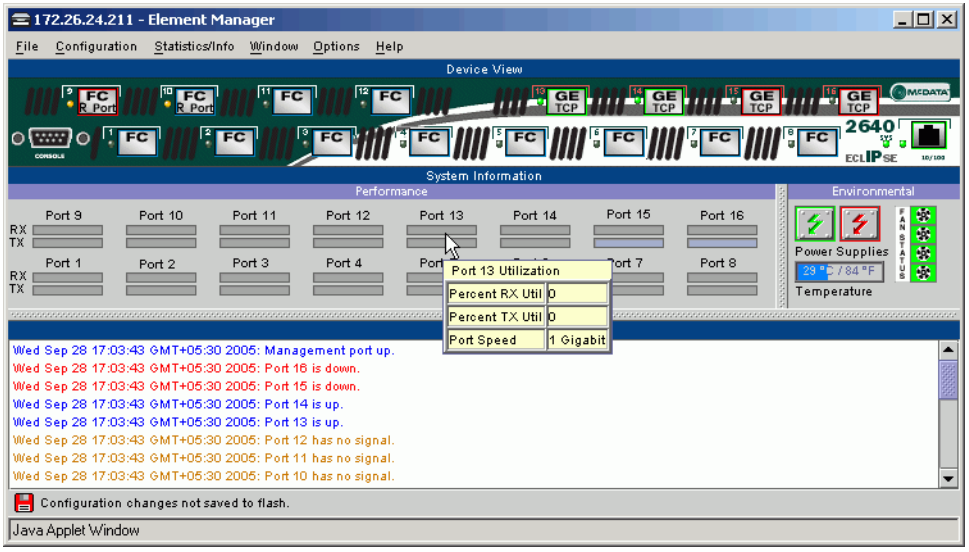


Figure 6-7 Performance Bar Tool Tip

The background color of the bar is dark gray if rate limiting is not configured and lighter gray when configured to limit bandwidth usage. Likewise, if a TCP port is configured to limit traffic to a T3 state, the background color is light gray. The blue color represents the percentage of port bandwidth.

The green (receive) or yellow (transmit) bar represents the percentage of port bandwidth used.

Environmental

Each power supply icon is surrounded by a colored border indicating status. Red indicates failure, green indicates normal operation.

The *Temperature* bar indicates internal temperature of the router chassis.

Four stacked *Fan Status* icons reflect the four chassis cooling fans. A green border indicates normal operation, yellow means low RPM, and red indicates failure.

To display a tooltip on environmental data, position the pointer over the icon. Figure 6-8 is an example for the SAN Router's system temperature, power supplies, and fans.

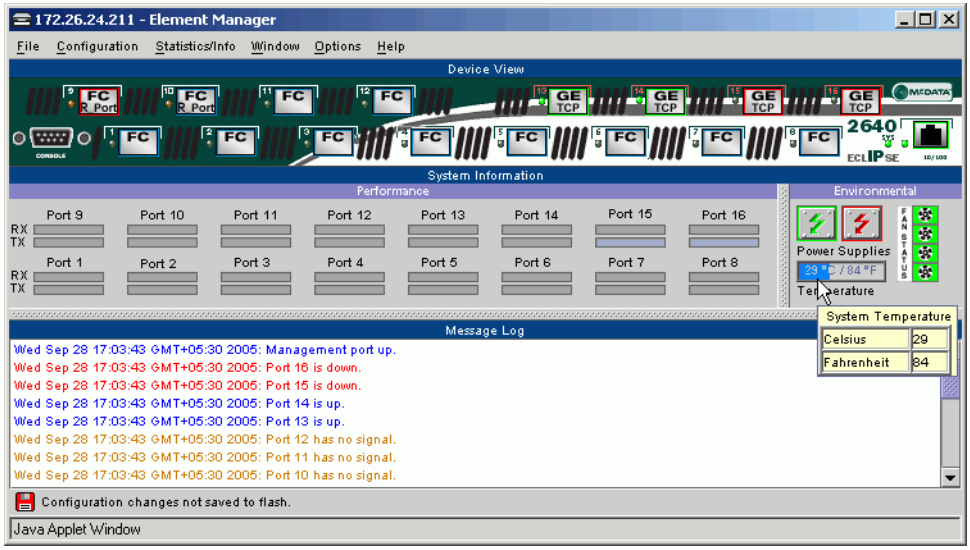


Figure 6-8 System Temperature Tool Tip

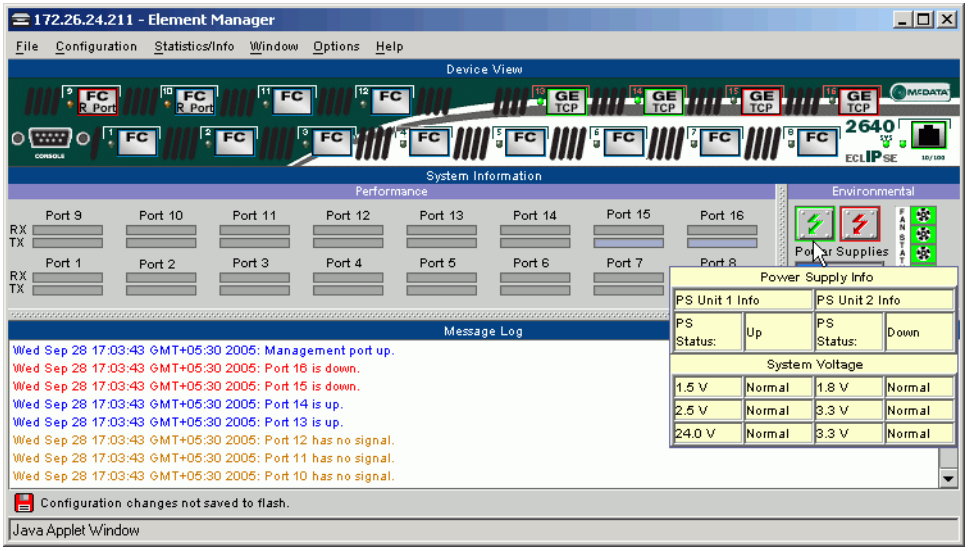


Figure 6-9 Power Supply Tool Tip

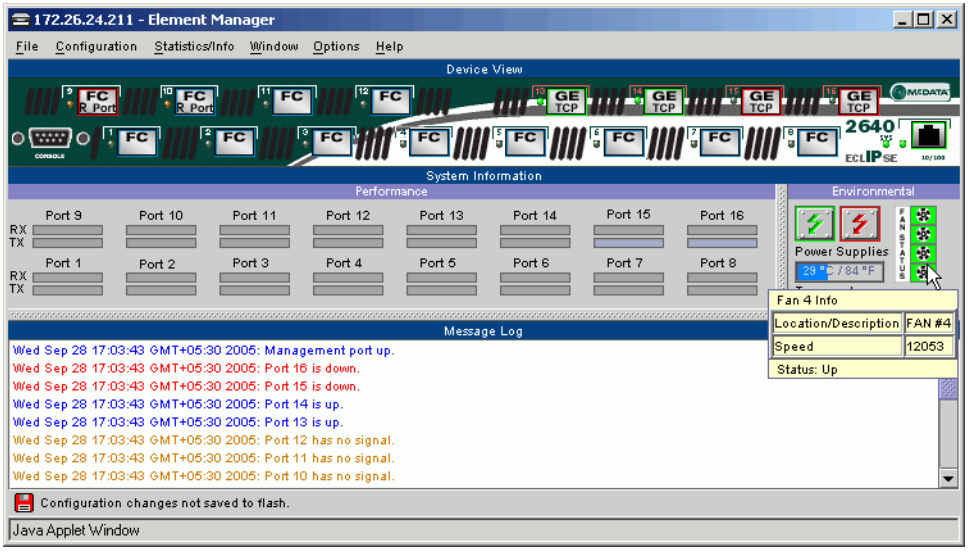


Figure 6-10 Fan Tool Tip

Message Log

Error conditions, warnings, configuration changes, and SAN Router state change information are all displayed in the *Message Log* (Figure 6-11). The *Message Log* is not persistent and there is no history of the transactions.

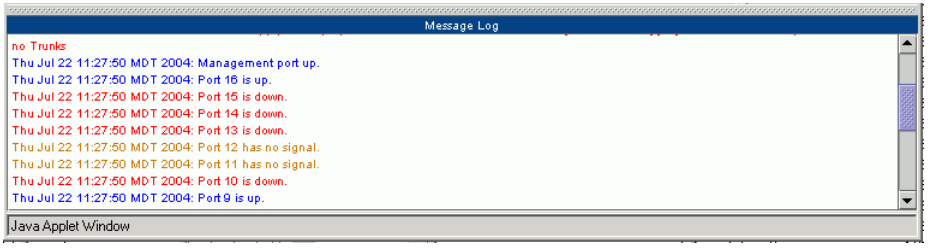


Figure 6-11 Message Log

The messages are color coded as noted in the Color Legend and listed in Table 6-4.

Table 6-4 Message Colors and meanings

Color	Meaning
Red	Error condition
Amber	Warning
Blue	Change applied in a configuration dialog box
Black	Information

To control the content in the *Message Log*, follow these instructions:

1. Right-click to display the *Message Log* menu.
2. Select the following parameters as required:
   - *Time Stamp* - If selected, displays the date stamp in messages.
   - *Verbose* - If selected, displays more messages about internal actions within Element Manager, such as polling.
3. Choose one of the following actions (optional):
   - *Select All* - Selects all messages in the log.
   - *Copy to Clipboard* - Copies the selected messages to the clipboard. You can then paste the messages into another application. Refer to *Granting Clipboard Access for Copy and Paste* on page 2-12 for information on how to configure Java security to allow copying to the clipboard.
   - *Clear Entries* - Deletes all messages in the log.

Flash Memory Icon

If the configuration has not been saved to flash memory, a red diskette icon appears in the bottom left corner of the device view with a message that changes are not saved to flash (Figure 6-1 on page 6-2). A green icon indicates changes have been saved.

Setting the Polling Interval

The Element Manager polls the SAN Router at a preset interval. To set the polling interval:

1. Select *Options>Poll Interval* to display the *Poll Interval* dialog box (Figure 6-12).

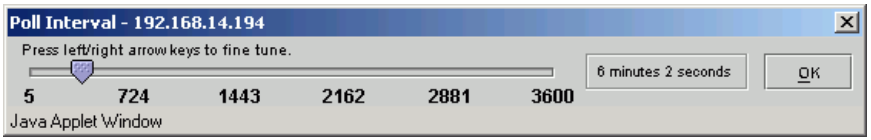


Figure 6-12 Poll Interval Dialog Box

2. Drag the pointer to the required interval. As you do, the new interval appears in the text box.
3. Click *OK* to make the change.

Using the System Log

The *System Log* (different from the Element Manager *Message Log*) contains errors or warning states encountered at the SAN Router. This could include ports going up and down, mSNS unable to zone, a SAN Router task failing, and so on. The *System Log* information will be routinely requested by Technical Support whenever you report a problem.

The Message Log is contained in Element Manager whereas the System Log is contained in the SAN Router.

Periodically, you should retrieve the *System Log* to preserve a copy, and then empty the contents. The System Log has a fixed size. New entries are written to the beginning of the log overwriting the oldest entries.

To retrieve and clear the system log, refer to *Retrieving and Clearing the System Log* on page 7-14.

Ping

The Element Manager provides options for checking remote connections through ping utility from the SAN Router.

To set up the ping network utility, follow these steps:

1. Select *Statistics/Info>Ping* to display the *Network Utilities* dialog box (Figure 6-13). You can use this to ping from the management port or iFCP/iSCSI ports.

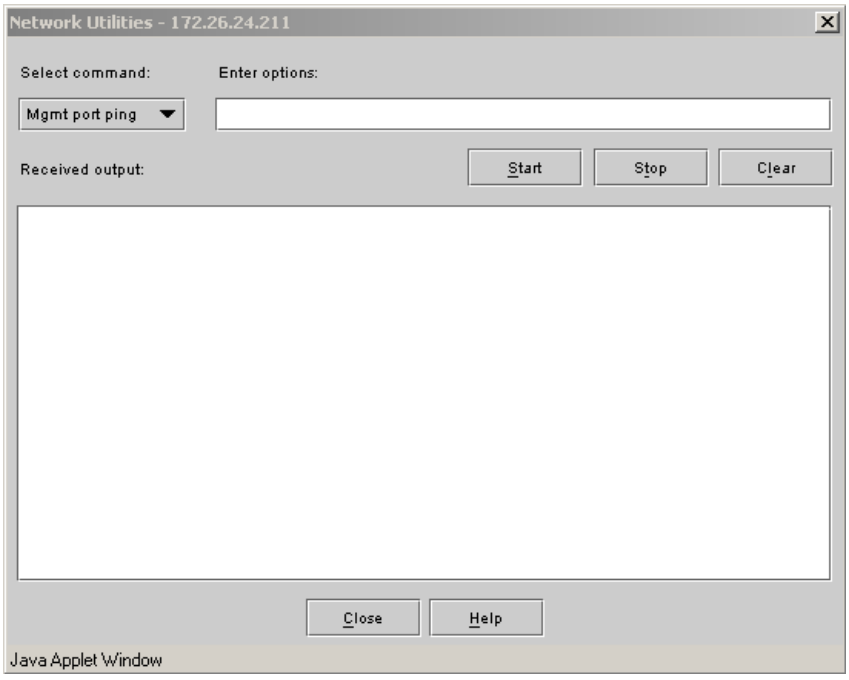


Figure 6-13 Network Utilities Dialog Box

2. Select *iFCP/iSCSI ping TCP* to execute a ping that egresses a TCP port.
3. Enter the following in the *Enter Options* box. DNS names are not supported.

```
-p port [-c count] [-s size] host
```

Table 6-5 Ping Options for iFCP Capable Ports

Item	Meaning
-p port	Port number to send the ping request from. This must be a TCP port.
-c count	If a count is specified, ping sends only that number of requests.
-s size	Datagram packet size (optional).
host	Destination IP address. DNS names are not supported.

4. Click *Start* to execute the command or *Stop* to abort it.

Viewing Statistics

You can view various accumulated statistics in table format using the Element Manager *Statistics/Info* menu. The types of statistics collected include:

- GE Port Statistics
- FC Port Statistics
- Port Traffic Statistics
- iFCP Port Compression Report
- MAC Forwarding
- IP Forwarding
- ARP (Address Resolution Protocol) Table
- Storage Name Service
- FC Device Properties
- Remote Connection Statistics

Sorting and Refreshing Report Data

You can sort and refresh all of the reports available through the Element Manager as follows:

- Click any column header to sort the list by that column. Click the same header again to switch between ascending and descending order.
- The column order may be changed by dragging column headers left or right.

Press **F5** or click the *Refresh* button to update the list with the latest information.

Gigabit Ethernet/Port Statistics

Select *Statistics/Info>GE Port* Statistics to display the *GE Port Statistics* dialog box (Figure 6-14 on page 6-15). This provides statistics for all GE ports in use on the SAN Router.

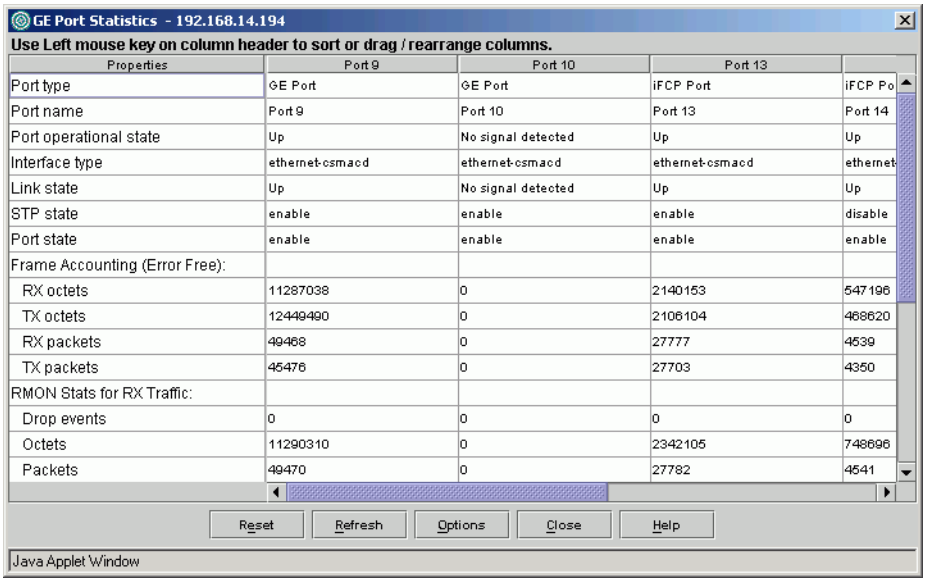


Figure 6-14 GE Port Statistics Dialog Box

Status information in the *GE Port Statistics* dialog box is described in Table 6-6.

NOTE: Port statistic counters, such as RX octets, TX octets, and errors, can be reset (via the *Reset* button) to a baseline count of zero and have the difference displayed between this new baseline and subsequent polls. Resetting the counters does not flush the counters in the SAN Router, rather it only re-adjusts the displayed values in this instance of Element Manager.

Table 6-6 Gigabit Ethernet/Port Statistics

Item	Meaning
Port type	Current port type or the port type which will be used after next SAN Router reset if this variable is set in NVRAM.
Port Name	User-defined name for this port.
Port operational state	Operation status of this port (Up, Down, No signal detected, Needs Reboot, or In Transition).
Interface type	Interface type. The only Interface type currently supported is ethernet-csmacd.

Table 6-6 Gigabit Ethernet/Port Statistics (Continued)

Item	Meaning
Link state	The state of Link Detect on the interface (up or no signal detected).
STP state	Enable or Disable STP protocol on the port.
Port state	Enable (1) and Disable (2) control for the interface.
Frame Accounting (Error Free)	• RX octets - number of octets received on the interface (not including octets in error). • TX octets - number of octets transmitted from the interface (not including octets in error). • RX Packet - number of packets received on the interface (not including packets in error). • TX Packet - number of packets transmitted from the interface (not including packets in error).
RMON (EtherStats)	• Drop Events - Number of times the SAN Router missed recording some RMON data due to a lack of resources. Normally 0. • Octets - The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is required, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval. The differences in the sampled values are Pkts and Octets, respectively, and the number of seconds in the interval is Interval. These values are used to calculate the Utilization as follows: Utilization = ((Pkts * 20) + Octets) / Interval * 1, 250, 000) for GE. Utilization = ((Pkts * 20) + Octets) / Interval * 1 25,000) for FE The result of this equation is the value Utilization which is the percent utilization of the Ethernet segment on a scale of 0 to 100 percent. • Packets - The total number of packets (including bad packets, Broadcast packets, and multicast packets) received.Broadcast Packets - The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets. • Multicast Packets - The total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address. • CRC alignment errors - The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

Table 6-6 Gigabit Ethernet/Port Statistics (Continued)

Item	Meaning
RMON (EtherStats) (continued)	• Undersize packets - The total number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed. • Fragments - The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Note that it is entirely normal for etherStatsFragments to increment. This is because it counts both runts and noise hits. • Oversize packets - The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Note that this definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms. The oversize packet total includes the jumbo frame count, if the Jumbo Frames feature is enabled. • Packets (64 octets) - The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets). • Packets (65-127 octets) - The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets). • Packets (128-255 octets) - The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets). • Packets (256-511 octets) - The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets). • Packets (512-1023 octets) - The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets). • Packets (1024-1518 octets) - The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

Fibre Channel/Port Statistics

Select *Statistics/Info>FC Port Statistics* to display the *FC Port Statistics* dialog box Figure 6-15 on page 6-18.This displays the statistics for all FC ports on the SAN Router. Statistics displayed in the *FC Port Statistics* dialog box are described in Table 6-7 on page 6-19.

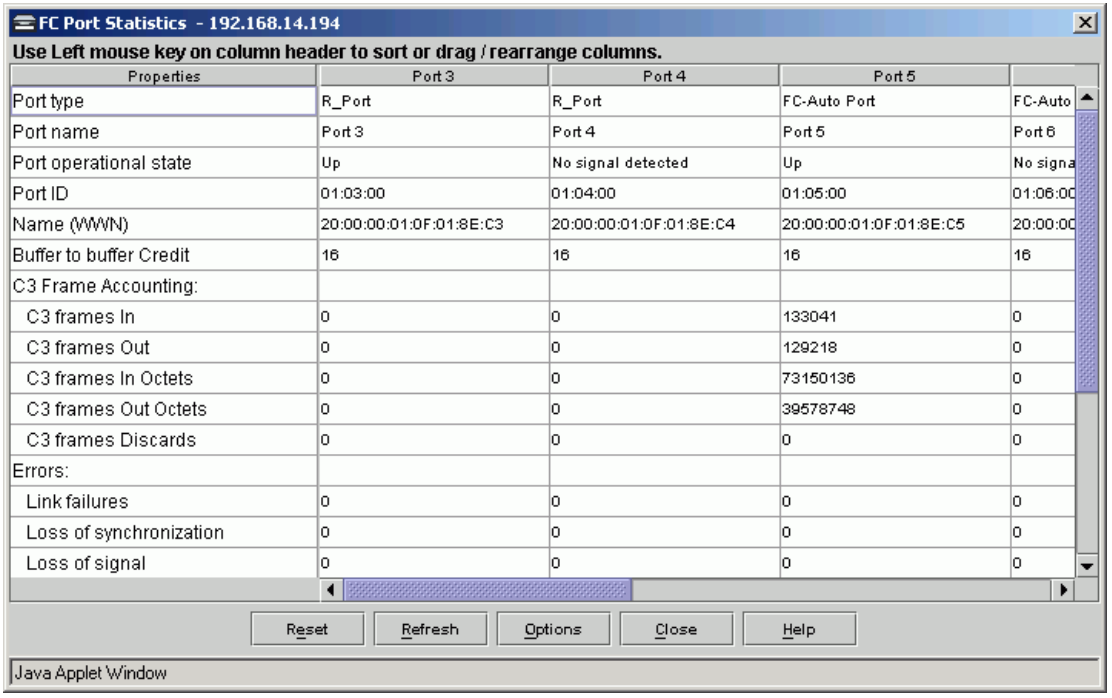


Figure 6-15 FC Port Statistics Dialog Box

NOTE: Port statistic counters, such as Frames In, and Errors, can be reset (using the *Reset* button) to a baseline count of zero and have the difference displayed between this new baseline and subsequent polls. Resetting the counters does not flush the counters in the SAN Router, rather it only re-adjusts the displayed values in the instance of Element Manager.

Table 6-7 FC Port Status Information

	Item	Meaning
Port Information	Port Type	R_Port, FC-Auto Port, F Port, L Port, or FL Port.
	Port Name	User-supplied label to identify the port.
	Port Operational State	Up, Down, No signal detected, or Needs Reboot.
	Port ID	P3-byte FCID; the Fibre Channel address within the fabric.
	Name (WWN)	Port name within the fabric.
	Buffer-to-buffer credit	Total number of receive buffers available.
C3 Frame Accounting	C3 Frames In	Class 3 Frames received.
	C3 Frames Out	Class 3 Frames delivered.
	C3 Frames In Octets	Class 3 frame octets including frame delimiters received.
	C3 Frames Out Octets	Class 3 frame octets including frame delimiters delivered.
	C3 Frames Discards	Class 3 frames discarded.
Errors	Link Failures	Number of link failures detected by this port.
	Loss of Synchronization	Number of loss of synchronization detected by this port.
	Loss of Signal	Number of loss of signal detected by this port.
	Protocol Error	Number of primitive sequence protocol errors detected by this port.
	Invalid Word	Number of invalid transmission word detected by this port.
	Invalid CRC	Number of invalid CRC detected by this port.
	Delimiter Errors	Number of Delimiter Errors detected by this port.
	Address Errors	Number of address identifier errors detected by this port.
	Link resets received	Number of Link Reset Protocol received by this port.
	Link resets out	Number of Link Reset Protocol issued by this port.
	Offline sequence received	Number of Offline Sequence received by this port.
	Offline sequence out	Number of Offline Sequence issued by this port.

Fibre Channel/Device Properties

To view information on the devices attached to every FC port on the SAN Router, select *Statistics/Info>Fibre Channel>Device Properties*. The *FC Device Properties* dialog box appears (Figure 6-16).

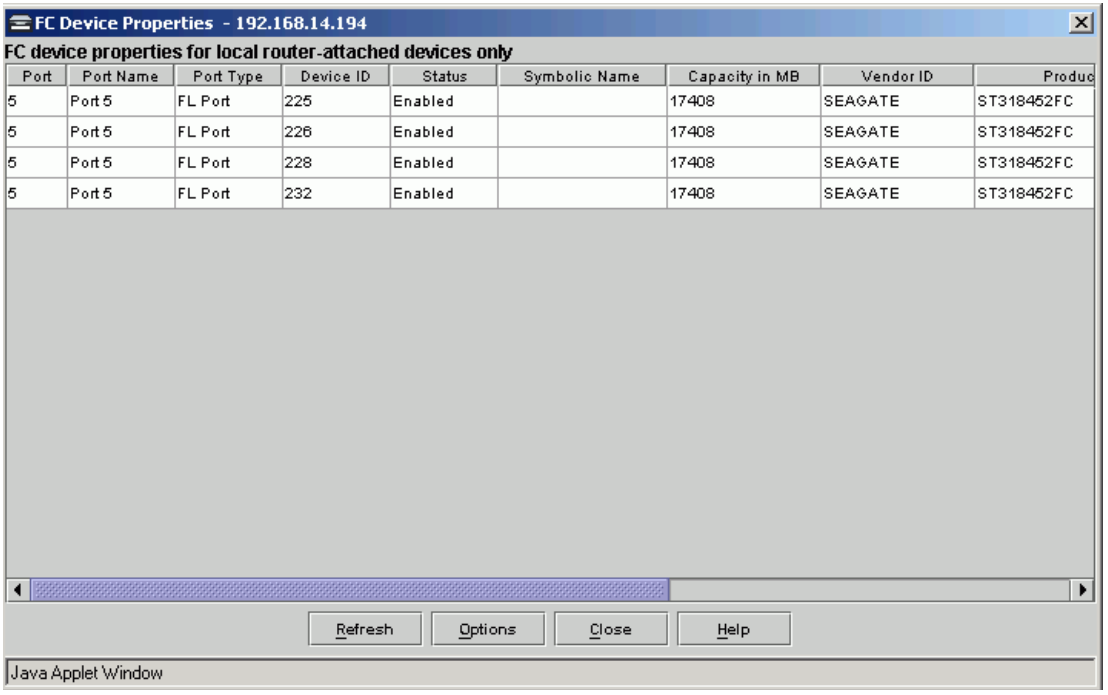


Figure 6-16 FC Device Properties Screen

Table 6-8 describes the *Fibre Channel Device Properties* information:

Table 6-8 Fibre Channel Device Properties Report

Item	Meaning
Port	The switch port to which the device is attached.
Port Name	The name assigned to the switch port via the *Port Configuration* dialog.
Port Type	The FC type of the switch port; usually FL or F.

Table 6-8 Fibre Channel Device Properties Report (Continued)

Item	Meaning
Device ID	The loop ID of the attached device. This is the third byte of the three-byte Fibre Channel ID.
Status	For an arbitrated loop; it tells whether the device is *Enabled* or *Bypassed*.
Device Symbolic Name	The Port Symbolic Name of the device.
Capacity	Storage device capacity in megabytes.
Vendor ID	The vendor name registered when the device logged into the fabric.
Product ID	The vendor product ID registered when the device logged into the fabric.
Device Type	The SCSI type of device. “Direct-access device” usually means a disk. “Sequential-access device” usually indicates a tape.
Port WWN	The FC port World Wide Name for the attached device.
Node WWN	The FC node World Wide Name for the attached device.

Port Traffic Statistics

To display the port traffic statistics, follow these instructions.

1. Select *Statistics/Info>Port Traffic* to display the *Port Traffic Report* dialog box (Figure 6-17 on page 6-22).

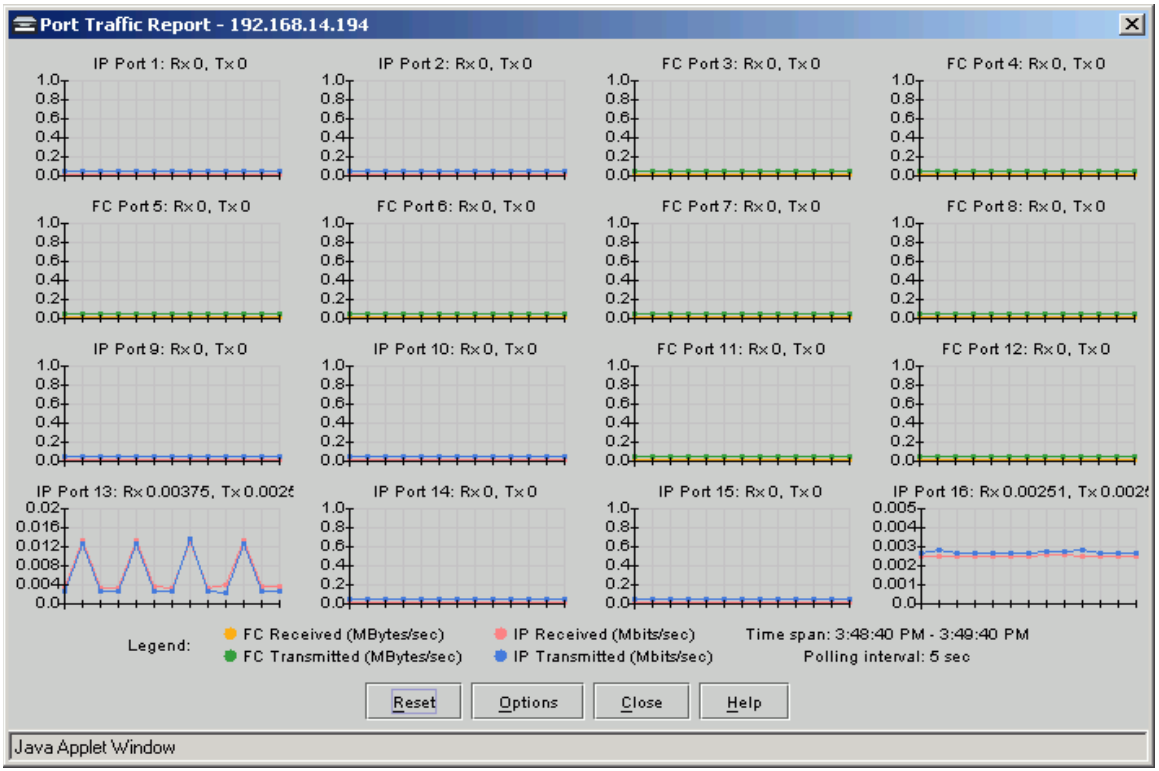


Figure 6-17 Port Traffic Report

The *Port Traffic Report* shows a recent history of traffic volume, in megabytes per second for FC ports and megabits per second for IP.

There is one graph for each port with two lines on each graph. Different colors are used in the FC and IP graphs.

For IP (iSCSI/iFCP) ports:

- The red line represents received data.
- The blue line represents transmitted data.

For FC ports:

- The orange line represents received data.
- The green line represents transmitted data.

2. Click the *Options* button to display the *Chart Options* dialog box (Figure 6-18 on page 6-23).

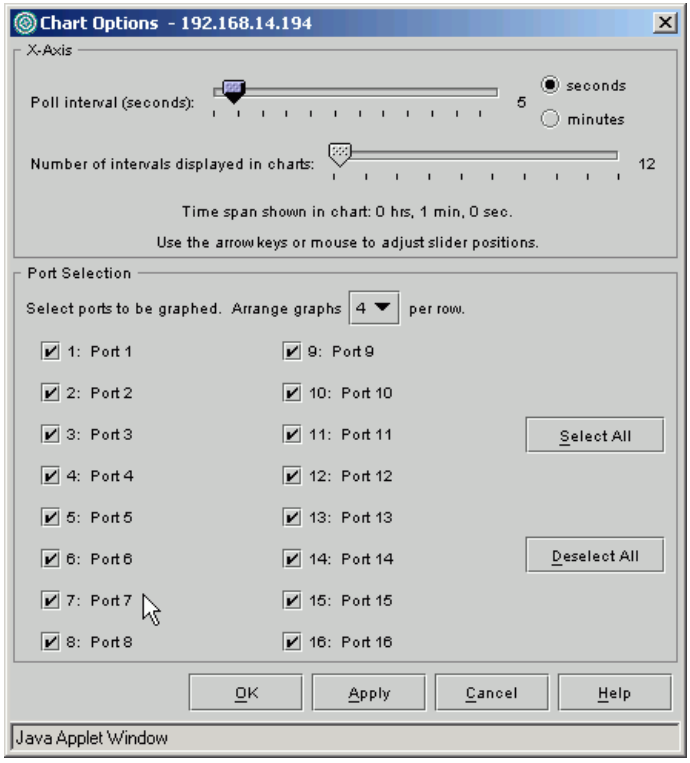


Figure 6-18 Chart Options Dialog Box

3. Click *seconds* or *minutes*, then use the arrow keys or mouse to adjust the slide bar to change the poll interval and the number of intervals to be displayed in each graph on the *Port Traffic Report*.
4. Select the ports to be included in the report.
5. Select the number of graphs to be displayed per row (1 to 4) from the drop-down list.
6. Click *Apply*.

If cookies are enabled in the web browser, the chart options are saved and re-used each time Element Manager is started.

iFCP Port Compression Report

The *iFCP Port Compression Report* shows a recent history of compressed traffic volume for each iFCP port on the SAN Router.

To display the iFCP port compression report, follow these instructions:

1. Choose *Statistics/Info>iFCP Compression Rates* to display the *iFCP Port Compression Report* dialog box (Figure 6-19(.

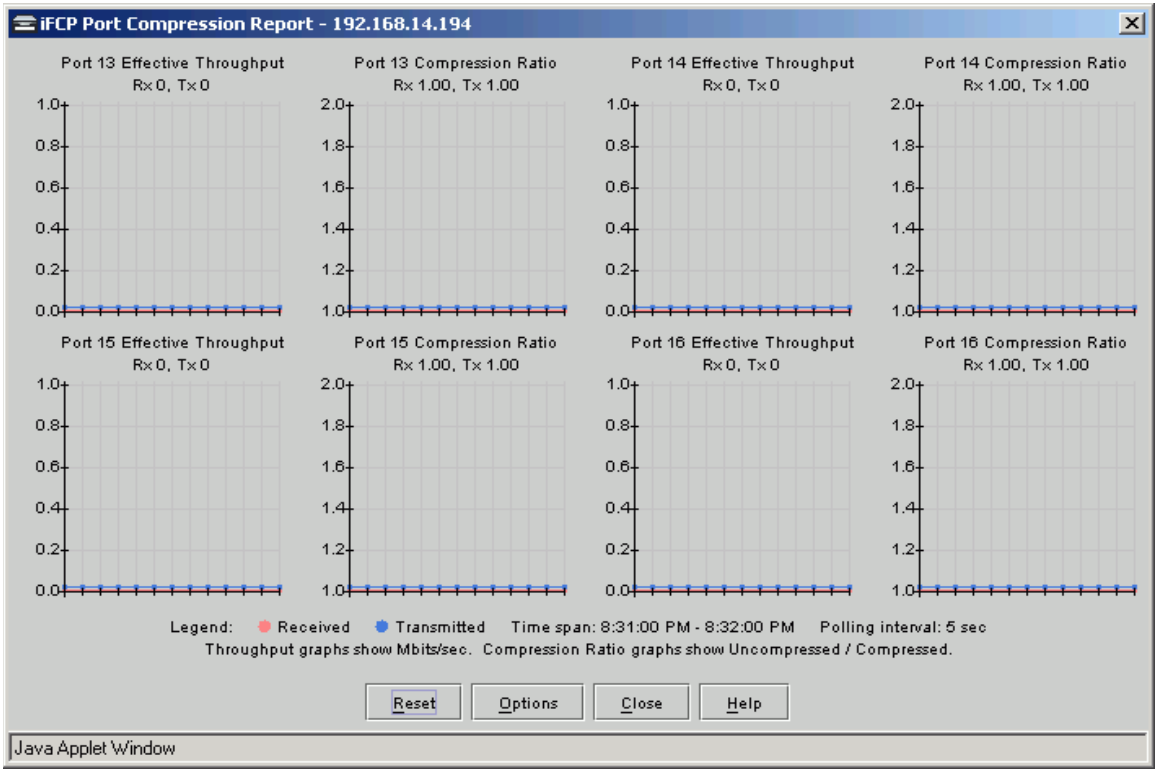


Figure 6-19 iFCP Port Configuration Report Dialog Box

There are two graphs for each port.

- Throughput is the measure of raw bandwidth (uncompressed data), expressed in megabits per second (Mbps) of iFCP traffic transmitted or received on the port.

- Compression Ratio conveys how "effectively" compression is working on the data. The ratio changes based on the data that is passing through the port at any given time and applies only to iFCP frames. For transmitted data, the Compression Ratio is displayed in the format "Original Data (uncompressed data): Compressed Data"; e.g. 4.266: 1. Received data is "decompressed" (if it arrived as compressed data) and the graph shows the ratio of the Decompressed Data: Compressed Data. For received data, this value matches the Compression Ratio of the peer port that is sending traffic to this port, provided the peer ports are communicating exclusively between each other.

Each graph displays two lines:

- The red line represents received data.
- The blue line represents transmitted data.

The graphs display useful data only when the compression feature is enabled. When compression is not configured, the effective throughput is the same as the actual throughput, and the compression ratio is always 1.0. You may also use the Port Traffic report to view the traffic statistics when the compression feature is not enabled.

2. Click the *Options* button to display the *Chart Options* dialog box (Figure 6-20) to adjust the polling rate, amount of time displayed in each graph, and the ports to be displayed.

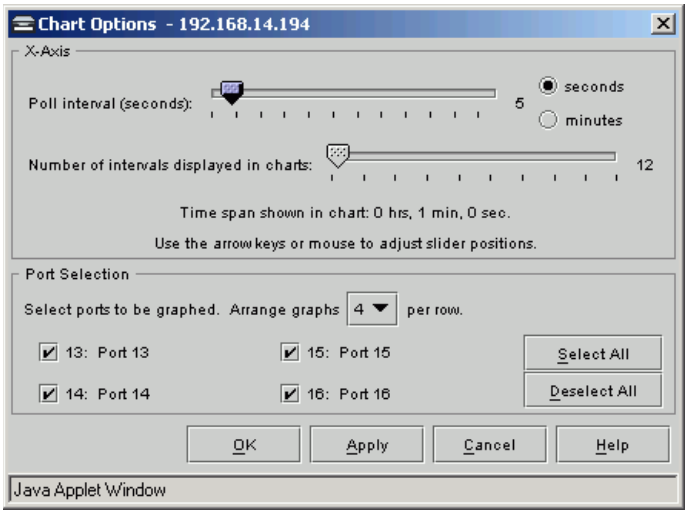


Figure 6-20 Chart Options Dialog Box

3. Click *seconds* or *minutes*, and use the arrow keys or mouse to adjust the slide bar to change the poll interval and the number of intervals to be displayed in each graph on the *iFCP Port Compression Report*.
4. Select the ports to be included in the report.
5. Select the number of graphs to be displayed per row (1 to 4) from the drop-down list.
6. Click *Apply*.

If cookies are enabled in the web browser, the chart options are saved and re-used each time Element Manager is started.

MAC Forwarding

To display the MAC forwarding table, follow these instructions:

Select *Statistics/Info>MAC Forwarding* to display the *MAC Forward Table* (Figure 6-21).

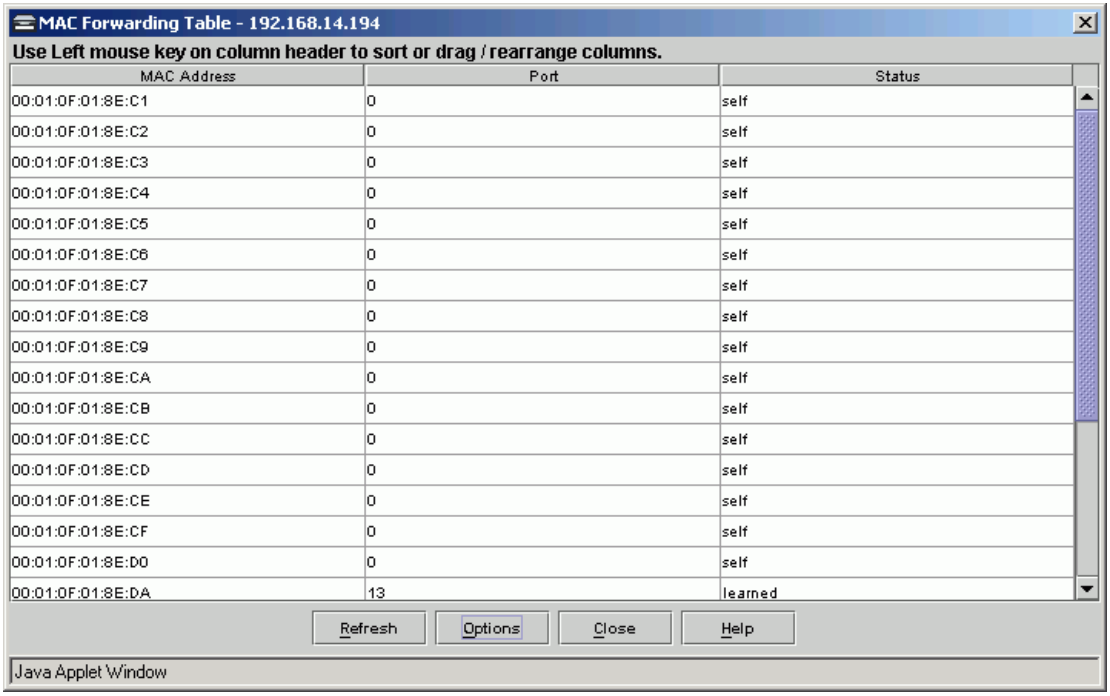


Figure 6-21 MAC Forward Table Dialog Box

Click the *Options* button to configure the data refresh rate in seconds.

Also known as the Forwarding Database for Transparent Bridges, this is a table of information about unicast entries for which the SAN Router has forwarding and/or filtering information.

Table 6-9 details information is in the *MAC Forwarding Table*.

Table 6-9 MAC Forwarding Report

Item	Meaning
MAC Address	The MAC address for which the SAN Router has forwarding and/or filtering information.
Port	The port number on which the MAC address was learned. A value of 0 indicates the MAC address was not learned but that the SAN Router does have some forwarding/filtering information about this address.
Status	An indicator of how the information was acquired: • Other - was learned by a method not included in this list. • Invalid - entry is no longer valid e.g., it was learned but has since aged-out. • Learned - the MAC address was learned on this port. • Self - the MAC address represents one of the SAN Router's addresses • Mgmt - a statically configured MAC address.

IP Forwarding

Use the *IP Forwarding* dialog box (Table 6-10 on page 6-29) to view the SAN Router's routing table, including dynamically learned from other switches. To display this dialog box, choose *IP Forwarding* from the *Statistics*/*Info* menu.

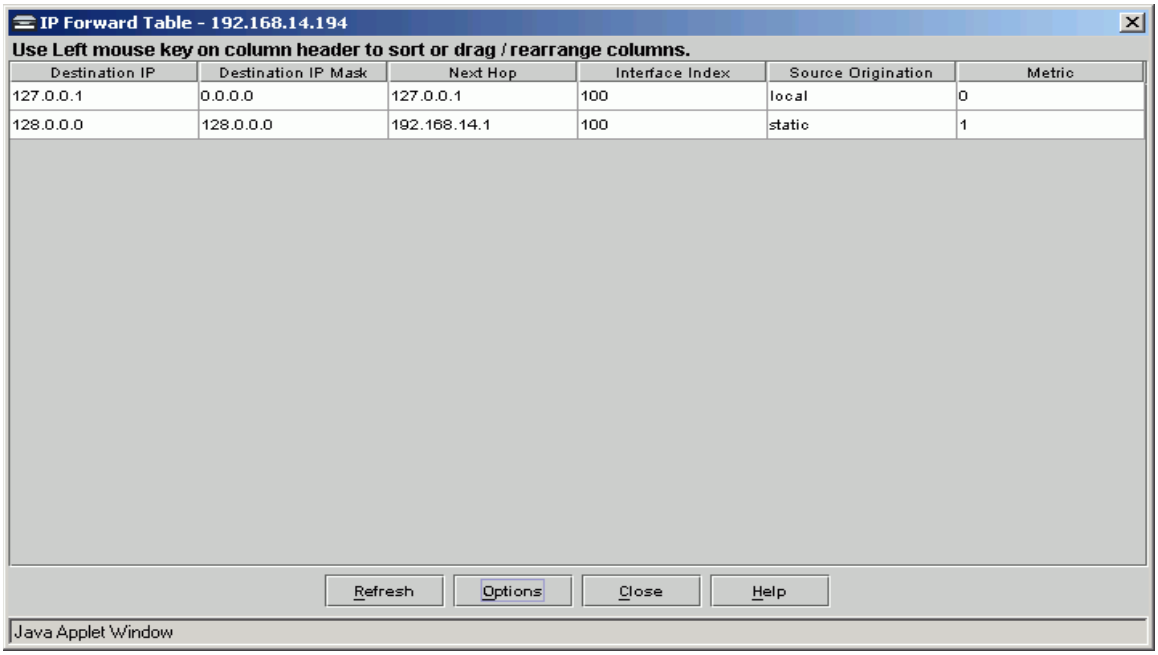


Figure 6-22 IP Forward Table Dialog Box

Click the *Options* button to configure the data refresh rate in seconds.

Table 6-10 describes information displayed in the *IP Forward Table* about the IP addresses learned and/or configured for each port.

Table 6-10 IP Forwarding

Item	Meaning
Destination IP	Destination IP address.
Destination IP Mask	Subnet mask of the destination IP address.
Next Hop	IP address of the next hop in this route.
Interface Index	Interface index value.
Source Origination	Routing mechanism.
Metric	Primary routing metric for the route.

ARP (Address Resolution Protocol) Table

The *ARP Table* dialog box (Figure 6-23) contains the active mapping of Ethernet MAC addresses to IP addresses for the SAN Router.

To display this dialog box, choose *ARP Table* from the *Statistics*/*Info* menu to display:

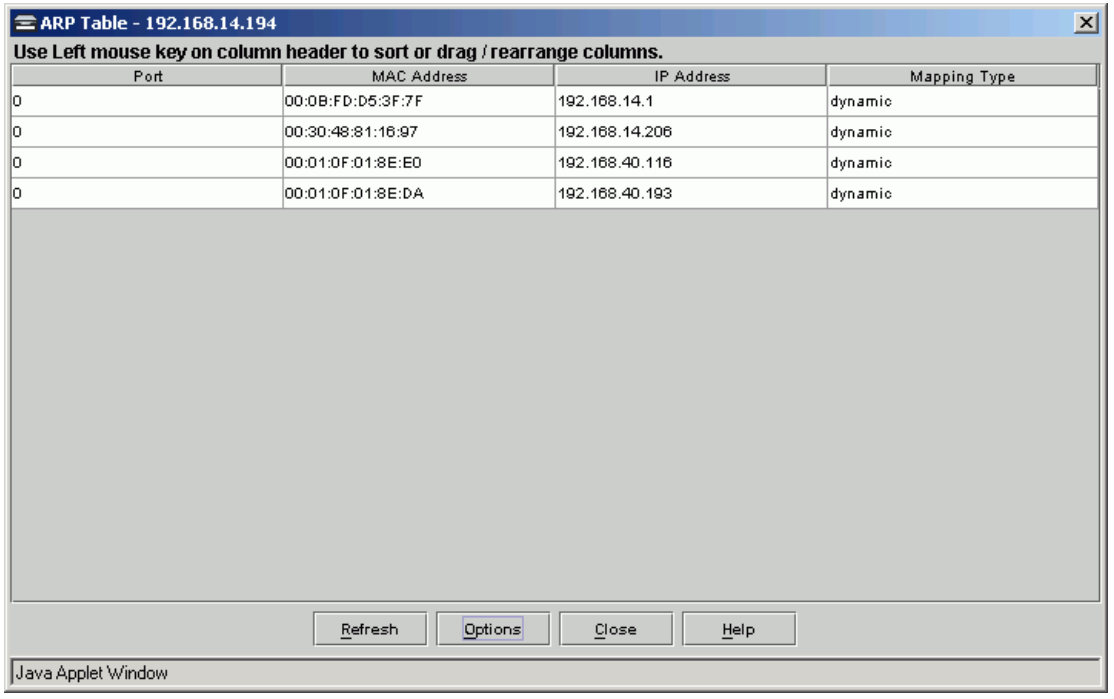


Figure 6-23 ARP Table Dialog Box

Table 6-11 on page 6-31 describes information is in the *ARP Table*.

Table 6-11 ARP Table

Item	Meaning
Port	The port number associated with the IP address/MAC address pair.
MAC Address	The MAC address associated with the IP address.
IP Address	The IP address associated with the MAC address.
Mapping Type	The type of mapping between the IP and MAC address. *Dynamic* signifies learned pair; *static* signifies statically configured.

metro Storage Name Server (mSNS)

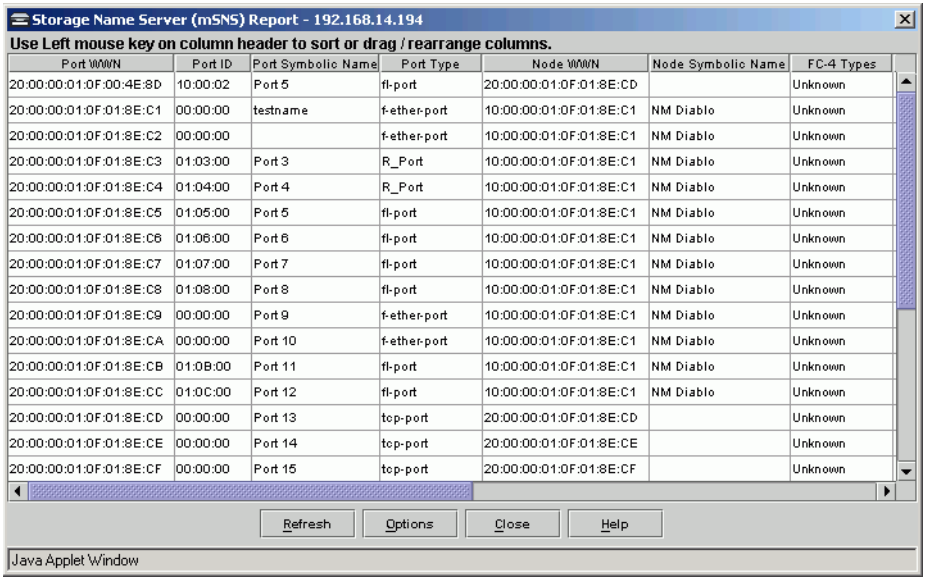
Choose *Storage Name Server (mSNS)* from the *Statistics/Info* menu to display the *Storage Name Server (mSNS) Report* dialog box (Figure 6-24 on page 6-32), which contains the complete contents of the mSNS. All devices known in the mSAN are displayed.

This report is created by querying the mSNS in the SAN Router. Contents are based on whether the SAN Router is configured as an mSNS client, or primary server.

The SAN Router is the primary server for the mSAN, and the report contains information for all devices in the FC fabric. If the SAN Router is a client or secondary server, the report contains information known to the local SAN Router only. The name server table contains an entry for each storage device port and SAN Router port known by the local name server.

Click the title of a column to sort the report by that column. Click the title again to reverse the sort order. You can also click and drag columns to reorder them in the table.

Click *Refresh* to update the report contents. Click *Options* to configure automatic refresh every few seconds.



Port WWN	Port ID	Port Symbolic Name	Port Type	Node WWN	Node Symbolic Name	FC-4 Types
20:00:00:01:0F:00:4E:8D	10:00:02	Port 5	fl-port	20:00:00:01:0F:01:8E:CD		Unknown
20:00:00:01:0F:01:8E:C1	00:00:00	testname	f-ether-port	10:00:00:01:0F:01:8E:C1	NM Diablo	Unknown
20:00:00:01:0F:01:8E:C2	00:00:00		f-ether-port	10:00:00:01:0F:01:8E:C1	NM Diablo	Unknown
20:00:00:01:0F:01:8E:C3	01:03:00	Port 3	R_Port	10:00:00:01:0F:01:8E:C1	NM Diablo	Unknown
20:00:00:01:0F:01:8E:C4	01:04:00	Port 4	R_Port	10:00:00:01:0F:01:8E:C1	NM Diablo	Unknown
20:00:00:01:0F:01:8E:C5	01:05:00	Port 5	fl-port	10:00:00:01:0F:01:8E:C1	NM Diablo	Unknown
20:00:00:01:0F:01:8E:C6	01:06:00	Port 6	fl-port	10:00:00:01:0F:01:8E:C1	NM Diablo	Unknown
20:00:00:01:0F:01:8E:C7	01:07:00	Port 7	fl-port	10:00:00:01:0F:01:8E:C1	NM Diablo	Unknown
20:00:00:01:0F:01:8E:C8	01:08:00	Port 8	fl-port	10:00:00:01:0F:01:8E:C1	NM Diablo	Unknown
20:00:00:01:0F:01:8E:C9	00:00:00	Port 9	f-ether-port	10:00:00:01:0F:01:8E:C1	NM Diablo	Unknown
20:00:00:01:0F:01:8E:CA	00:00:00	Port 10	f-ether-port	10:00:00:01:0F:01:8E:C1	NM Diablo	Unknown
20:00:00:01:0F:01:8E:CB	01:0B:00	Port 11	fl-port	10:00:00:01:0F:01:8E:C1	NM Diablo	Unknown
20:00:00:01:0F:01:8E:CC	01:0C:00	Port 12	fl-port	10:00:00:01:0F:01:8E:C1	NM Diablo	Unknown
20:00:00:01:0F:01:8E:CD	00:00:00	Port 13	tcp-port	20:00:00:01:0F:01:8E:CD		Unknown
20:00:00:01:0F:01:8E:CE	00:00:00	Port 14	tcp-port	20:00:00:01:0F:01:8E:CE		Unknown
20:00:00:01:0F:01:8E:CF	00:00:00	Port 15	tcp-port	20:00:00:01:0F:01:8E:CF		Unknown

Figure 6-24 Storage Name Server (mSNS) Report Dialog Box

Table 6-12 describes information that appears in the mSNS report.

Table 6-12 mSNS Report

Item	Meaning
Port WWN	FC WWN for each storage device port or switch port in the fabric.
Port ID	FC port ID address, in hexadecimal format, for the storage device or switch port.
Port Symbolic Name	Optional name registered in the name server by the storage device or switch.
Port Type	Type of port: N-port, NL-port, F-NL port, tcp-port, F-port, FL-port, R_Port, B-port or F-ether-port, UnavailableDev.
Node WWN	FC WWN of the associated node as defined in FC-GS-2.
Node Symbolic Name	Symbolic name of the node.
FC-4 Types	FC-4s supported by the port as defined in FC-GS-2.
FC COS	Class of services supported by the port.
Fabric Port WWN	Public or private FC node.
FC Port IP Address	If port type is N_Port or NL_Port, entry is for a storage device, and IP address is used for routing in local FC network If port type is F_Ether_Port, F_Port, or FL_Port, entry is for a switch port, and IP address is inband IP address. For F_EtherGtwy_Port types, it is the iFCP/iSCSI port IP address.
Node IP Address	The management IP address of the device.
FC IPA	Initial Process Associator of the Node. This is registered by some complex FC devices to assist with start-up initialization.

Remote Connection Statistics

1. Select *Statistics/Info>Remote Connections* to display the *Remote Connection Statistics* dialog box (Figure 6-25).

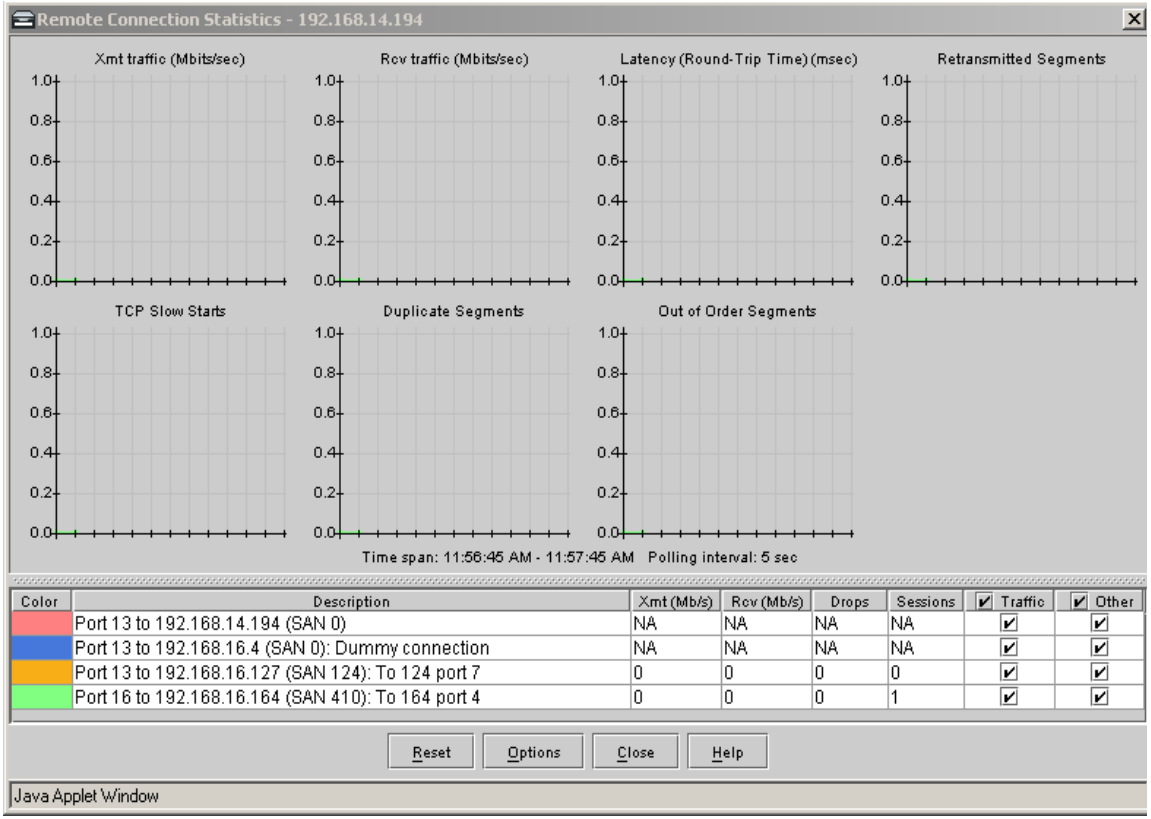


Figure 6-25 Remote Connection Statistics Dialog Box

The *Remote Connection Statistics* report shows traffic volume and errors for each iFCP connection from this SAN Router. All charts are line charts with one line per remote connection.

All configured and enabled remote connections are included in the legend. Disabled connections do not appear. Enabled connections that are currently down will appear in the legend, but the statistics will be shown as 0. Only primary connections are shown. Backup connections are not included.

The chart line colors in this report are customizable. To change a color, double-click the color in the first column of the table.

Table 6-13 on page 6-35 describes statistics displayed in this report.

Table 6-13 Remote Connection Statistics Report

Item	Meaning
Transmit Traffic	The average data rate sent to the remote SAN Router over the previous polling interval, in megabytes per seconds.
Receive Traffic	The average data rate received from the remote SAN Router over the previous polling interval, in megabytes per seconds.
Latency	The time in milliseconds required for the most recent *keep-alive* message to travel round-trip from the local to the remote SAN Router and back. Keep-alive messages are sent at an interval equal to 1/3 of the connection timeout value. Thus if the connection has a timeout value of 30 seconds (the default), the latency measurement is updated every 10 seconds.
Retransmitted Segments	The count of segments that had to be re-transmitted to the remote SAN Router during the last polling interval. A large number of re-transmitted segments indicates an unreliable WAN connection, resulting in poor throughput.
TCP Slow Starts	The count of congestion events on all TCP sessions within the iFCP connection. A congestion event is either a Slow Start (typically initiated by a timeout), or a Fast Recovery action (typically initiated by duplicate ACKs indicating a lost packet).
Dropped Connections	The number of times the connection to the remote SAN Router was lost during the last polling interval. This count represents failures in the WAN link that interrupted traffic to the remote SAN Router. The Dropped Connections count is cumulative but can be reset to zero via the *Reset* button. Resetting this counter does not change the counter in the SAN Router hardware. Resetting saves a baseline value and displays the difference between the current value and the saved baseline value. Closing and re-opening the *Remote Connection Statistics* report displays the cumulative total again. Reset also discards the graph data, so the graphs begin to display again.
Sessions	The number of initiator-target pairs (host-disk pairs) currently active to the remote SAN Router. For example, if three servers in the local mSAN each have four disks mounted from the remote SAN, there would be twelve sessions. This is also the current number of parallel TCP connections making up the logical remote SAN Router connection.
Traffic	Selecting this option presents the remote connections statistics for the traffic graphs (xmt and rcv traffic)
Other	Selecting this option presents the remote connections statistics for the other graphs (latency, retransmitted segments, and slow starts)

2. Click the *Options* button to display the *Chart Options* dialog box (Figure 6-26 on page 6-36). Use this dialog box to change the polling interval and the number of displayed intervals. The default polling interval is five (5) seconds.

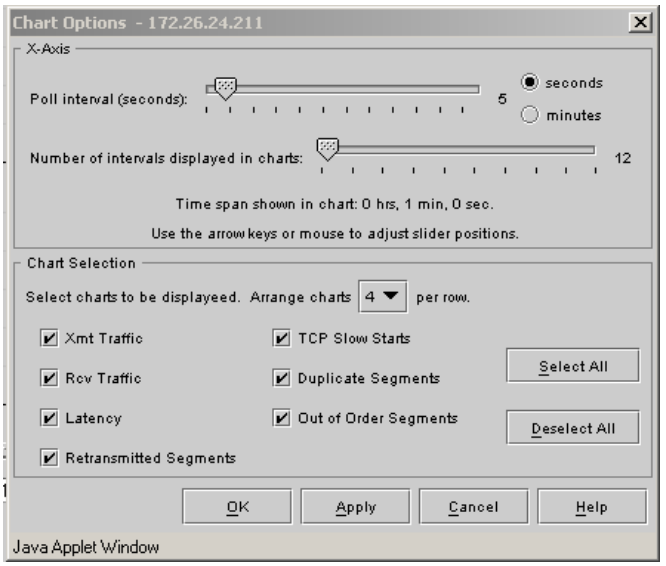


Figure 6-26 Chart Options Dialog Box

NOTE: The polling interval and chart options are saved if you close and reopen the *Remote Connection Statistics* report and when you close Element Manager for this SAN Router and log in later. However, if you switch the web browser to another web page and back, the polling interval and chart options reverts to the default value unless cookies are enabled in the web browser.

3. Click *seconds* or *minutes*, and then use the arrow keys or mouse to adjust the slide bars to change the poll interval or number of displayed intervals. The charts in the *Remote Connection Statistics* report are updated at each poll.
4. Select the charts you want to display.
5. Click *Apply*. Click *OK* to close the *Chart Options* dialog box.
6. Click *Close* to close the report screen.

Wrapping Counters

The SAN Router stores information in counters with a maximum value of four billion. When this value is reached, the counter resets to zero and the count begins again. When reporting statistics such as the number of bytes received or transmitted, the counter can quickly fill if the port is operating at full line rate. For a 1 Gbps FC port, this counter can wrap in as little as 31 seconds. If the graph poll rate is set at a period longer than this, the reported statistics can report incorrect results. Be sure to set the graph's polling period to accommodate the rate of traffic across the monitored port.

7

Configuration, Firmware, and System Log Maintenance

This chapter includes information for upgrading firmware, backing up and restoring configuration data, and retrieving and clearing the system log.

Use the following links to move through the chapter.

Upgrading Firmware (E/OSi)

Use the following steps to upgrade firmware on the SAN Router. Note that you may also need to upgrade the bootrom file if you have any other version installed. To determine if you need to upgrade bootrom and for instructions refer to *Upgrading bootrom (E/OSi)* on page 7-5.

Downloading Firmware

You can use the CLI or Element Manager to download and install a new version of the firmware for the SAN Router.

The SAN Router can store up to two versions of firmware – the currently active version and an inactive version. To download firmware, follow these instructions:

1. Select *File>Firmware Upgrade*. The *Firmware Upgrade* dialog box appears.

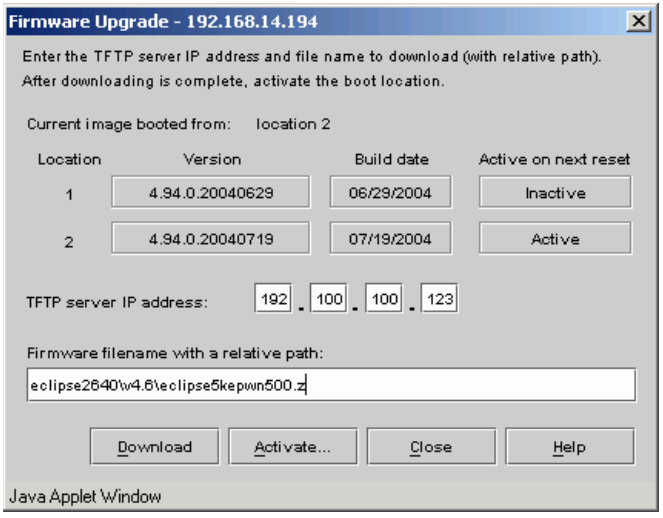


Figure 7-1 Firmware Upgrade Dialog Box

The dialog box shows the previous version, build date, the active/inactive status of both firmware locations. The TFTP server address and file name are blank the first time the dialog box appears. If the dialog is displayed again later, the last contents are displayed.

2. Enter or edit the TFTP server IP address where the firmware image is stored.
3. Enter or edit the path and file name on the TFTP server for the new firmware.
4. Click *Download*. When you download a new version, it is always saved in the inactive location.

Activating New Firmware

To activate the new firmware, follow these instructions:

1. Click the *Activate* button.

   The *Activate Boot Location* dialog box displays both firmware locations and their respective build dates.

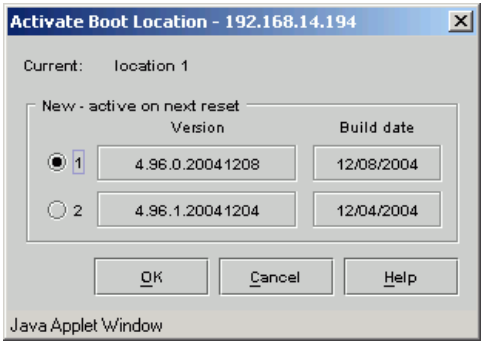


Figure 7-2 Activate Boot Location Dialog Box

2. Click the version you want to activate.
3. Click *OK*.
4. Choose *Reset System* from the *File* menu to make the version active. Now the newest version becomes active and the prior version is saved as inactive.

5. Close and restart the web browser to load the Element Manager from the new version. After resetting the SAN Router, it may take two or three minutes for the SAN Router's embedded web server to become ready.

Restoring Prior Firmware Version

To restore the prior firmware version in the event you experience problems on the network with the new version, use the following procedure.

1. Select *Firmware Upgrade* from the *File* menu.
2. Click the *Activate* button to display the *Activate Boot Location* dialog box (Figure 7-2 on page 7-3).
3. Click the prior (now inactive) version in the *Activate Boot Location* dialog box, then click *OK*.
4. Choose *Reset System* from the *File* menu to make the version active.
5. Close and restart the web browser to load the new Element Manager from the new version. After resetting the SAN Router, the SAN Router's embedded web server may take two or three minutes to become active.

Upgrading bootrom (E/OSi)

You can use the CLI or Element Manager to download and install bootrom to the SAN Router. The following instructions are for using the Element Manager.

1. To determine if the bootrom installed on your system requires an upgrade:
   - Select *Configuration/System/Properties* to display the *System Properties* dialog box. Check the version number in the *Boot ROM version* field.
   - Compare the bootrom version number to the bootrom version in Table 7-1 for the E/OSi firmware installed on your SAN Router.

Table 7-1 SAN Router E/OSi and bootrom Versions

E/OSi Version	bootrom Version	bootrom File Name
4.6	v1.0.3	ECP2k103bootrom.bin
4.7	v1.0.3	ECP2k103bootrom.bin

2. If you need to upgrade the bootrom to match your current E/OSI firmware, select *File>Firmware Upgrade*.

   The *Firmware Upgrade* dialog box appears (Figure 7-1 on page 7-2).

3. Enter or edit the TFTP server IP address where the `bootrom.bin` file is stored.
4. Enter or edit the fully qualified path and file name on the TFTP server for the new bootrom.bin file.
5. Click *Download*.
6. When the download completes, do not click *Activate* on the dialog box. Instead, reset the SAN Router. This will activate the new bootrom with the current version of E/OSi firmware installed on the system.

   To reset the SAN Router, select *Reset System* from the *File* menu. When the *Reset Options* dialog box displays, select the first option to *Reset System*.

Resetting the System

Certain configuration changes require you to reset the SAN Router before the changes take effect. Use *File>Reset System* from the Element Manager Window. These occurrences are described in previous chapters and are listed below for reference.

Table 7-2 Resetting the System

Dialog Box	Parameter Changed Requiring Reset
Inband Address Configuration *Configuration>System>Inband Address*	The Router's inband address, subnet mask address, and gateway address.
Advanced FC Port Configuration *Configuration>Port>Advanced FC Port*	The error detection and resource allocation timeout values.
Firmware Upgrade *File>Firmware Upgrade*	The activate boot location.
FC/Ethernet Port Configuration *Configuration>Port>FC/Ethernet*	The TCP port address, subnet mask, next hop gateway address, internal address
iFCP Setup *Configuration>iFCP>Setup*	The local mSAN ID.
Management Port Configuration *Configuration>Port>Management*	The management address and subnet mask address.

Selecting *Reset System* from the *File* menu displays the *Reset Options* dialog box (Figure 7-3).

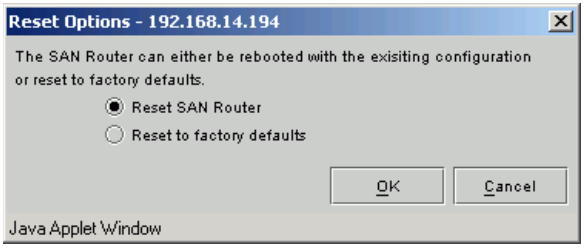


Figure 7-3 Reset Options Dialog Box

- *Reset SAN Router* - This resets the hardware and firmware while maintaining the existing configuration values. Be sure to select this option if you want to maintain any values you have set through configuration dialog boxes.
- *Reset to Factory defaults* - This resets the hardware and firmware and changes configuration values to the factory-defaults. Refer to *Factory Default Settings for the SAN Router* on page 7-8 for a list of these default settings. Make sure that no conflicts will occur by resetting to these defaults.

  For a list of default settings for SANvergence Manager parameters, refer to Chapter 1 in the *SANvergence Manager User Manual*.

NOTE: Both of these Reset options disrupt port operations.

Factory Default Settings for the SAN Router

The following table lists the default settings for parameters that you can configure through the SAN Router Element Manager dialog boxes and the menu path for changing these settings.

Table 7-3 Default Element Manager Parameter Settings

Parameter	Default Setting	Menu Path
System		
SAN Routing Cluster ID	1	Configuration>System>Operations
Enable remote access via Telnet	Enabled	Configuration>System>Operations
Router Inband address	0.0.0.0	Configuration>System>Inband Address
Router Subnet mask	0.0.0.0	Configuration>System>Inband Address
Default Gateway address	0.0.0.0	Configuration>System>Inband Address
SNMP Read-only Password	public	Configuration>System>SNMP Communities/Hosts
SNMP Read-modify Password	private	Configuration>System>SNMP Communities/Hosts
SNMP hosts	None defined	Configuration>System>SNMP Communities/Hosts
SNMP Traps	None defined	Configuration>System>SNMP Traps
SNTP	Disabled	Configuration>System>Date/Time
New Device Zoning	Not a member of any router zone	Configuration>System>New Device Zoning
Element Manager Poll Interval (in seconds)	30	Options>Poll Interval
10/100 BaseT Management Port		
Management Port IP address	0.0.0.0[a] *See note 'a' following this table.	Configuration>Port>Management
Management Port Subnet Mask	0.0.0.0	Configuration>Port>Management
Default Gateway	0.0.0.0	Configuration>Port>Management
Multi-function Ports		
General		

Table 7-3 Default Element Manager Parameter Settings (Continued)

Parameter	Default Setting	Menu Path
Multi-function port type	Fibre Channel	Configuration>Port>FC/Ethernet
Port Speed	Auto	Configuration>Port>FC/Ethernet
Port State	Enabled	Configuration>Port>FC/Ethernet
Port Parameters	FC-Auto	Configuration>Port>FC/Ethernet
Advanced		
E_D_TOV - Error Detection (sec)	2	Configuration>Port>Advanced FC Port
R_A_TOV - Resource Allocation (sec)	10	Configuration>Port>Advanced FC Port
Intelligent TCP ports		
Ethernet and IP Parameters		
Protocol	iFCP	Configuration>Port>FC/Ethernet
Port Speed	1 Gigabit	Configuration>Port>FC/Ethernet
Port State	Enabled	Configuration>Port>FC/Ethernet
Autonegotiations	Enabled	Configuration>Port>FC/Ethernet
iSCSI/iFCP port IP address	0.0.0.0	Configuration>Port>FC/Ethernet
iSCSI/iFCP port subnet mask	0.0.0.0	Configuration>Port>FC/Ethernet
iSCSI/iFCP port External router address	0.0.0.0	Configuration>Port>FC/Ethernet
iSCSI/iFCP port Internal SAN address	0.0.0.0	Configuration>Port>FC/Ethernet
TCP parameters		
Auto Reset Port on Severe Errors	Enabled	Configuration>Port>FC/Ethernet>Advanced
Smaller CWND Reduction	Disabled	Configuration>Port>FC/Ethernet>Advanced
Quick Start	Disabled	Configuration>Port>FC/Ethernet>Advanced
Reduced Slow Start Timeout	Disabled	Configuration>Port>FC/Ethernet>Advanced
Disable Standard Congestion Avoidance	Disabled	Configuration>Port>FC/Ethernet>Advanced
Reorder Resistance	Disabled	Configuration>Port>FC/Ethernet>Advanced
MTU Size	Auto	Configuration>Port>FC/Ethernet>Advanced

Table 7-3 Default Element Manager Parameter Settings (Continued)

Parameter	Default Setting	Menu Path
iSCSI parameters		
Selective ACKnowledgement	Disabled	Configuration>Port>FC/Ethernet>Advanced
Large PDU	Enabled	Configuration>Port>FC/Ethernet>Advanced
Initial R2T	Enabled	Configuration>Port>FC/Ethernet>Advanced
Store and Forward	Disabled	Configuration>Port>FC/Ethernet>Advanced
Target Read Padding	Disabled	Configuration>Port>FC/Ethernet>Advanced
Target Write Padding	Disabled	Configuration>Port>FC/Ethernet>Advanced
Immediate Data	Enabled	Configuration>Port>FC/Ethernet>Advanced
NOP Packets	Enabled	Configuration>Port>FC/Ethernet>Advanced
Authentication method	None	Configuration>Port>FC/Ethernet>Advanced
Login Retry timeout (in seconds)	Configure/60	Configuration>Port>FC/Ethernet>Advanced
First Burst Length (KB)	64	Configuration>Port>FC/Ethernet>Advanced
Max Burst Length (KB)	256	Configuration>Port>FC/Ethernet>Advanced
Max Rcv Data Segment Length (C\KB)	64	Configuration>Port>FC/Ethernet>Advanced
iFCP parameters		
Compression Level	None	Configuration>Port>FC/Ethernet>Advanced
Compression Method	LZO	Configuration>Port>FC/Ethernet>Advanced
Selective ACKnowledgement	Disabled	Configuration>Port>FC/Ethernet>Advanced
FastWrite	Disabled	Configuration>Port>FC/Ethernet>Advanced
Transmit Buffer Management	Disabled	Configuration>Port>FC/Ethernet>Advanced
General Configuration		
iSCSI		
Enable Auto Initiator Accept	Enabled	Configuration>iSCSI>Devices
Primary RADIUS Server		

Table 7-3 Default Element Manager Parameter Settings (Continued)

Parameter	Default Setting	Menu Path
IP Address	0.0.0.0	Configuration>iSCSI>RADIUS Server Configuration
UDP Port	1812	Configuration>iSCSI>RADIUS Server Configuration
Timeout (in seconds)	1	Configuration>iSCSI>RADIUS Server Configuration
Retries	1	Configuration>iSCSI>RADIUS Server Configuration
Secondary RADIUS Server		
IP Address	0.0.0.0	Configuration>iSCSI>RADIUS Server Configuration
UDP Port	1812	Configuration>iSCSI>RADIUS Server Configuration
Timeout (in seconds)	1	Configuration>iSCSI>RADIUS Server Configuration
Retries	1	Configuration>iSCSI>RADIUS Server Configuration
iFCP		
Local mSAN ID	0	Configuration>iFCP>Setup
Remote Connections	None	Configuration>iFCP>Remote Connections
Remote Gateway IP Address	0.0.0.0	Configuration>iFCP>Remote Connections>Add
Connection State	Enabled	Configuration>iFCP>Remote Connections>Add
Connection timeout	10	Configuration>iFCP>Remote Connections>Add
TCP Window Size	Auto	Configuration>iFCP>Remote Connections>Add
Exported Zones	None	Configuration>iFCP>Remote Connections>Add
iFCP Port Redundancy		
Backup for Port	Disabled	Configuration>iFCP>Port Redundancy
Timeout for backup activation (in seconds)	5	Configuration>iFCP>Port Redundancy
Recovery Method	Manual	Configuration>iFCP>Port Redundancy

a. If the SAN Router is shipped in a cabinet, then the default IP address will be 10.xx.yy.zz where,
xx is the cabinet number (1, 2, 3, etc.)
yy is the product type identifier (16 for the Eclipse 2640 SAN Router)
zz is the position in the rack, bottom to top (1, 2, 3, etc.)

Configuring Backup and Restore

CAUTION

You must backup the SAN Router configuration periodically so that you can restore the configuration in the event of a hardware failure or problems because of new configuration/software version.

The backup function copies all current settings, including zoning, configured on the SAN Router to the TFTP server. The restore copies the configuration from the TFTP server to the SAN Router. The restored configuration takes effect only after you reset the SAN Router.

Back up and restore zone set configurations for the mSAN using the *Load Zone Set* and *Save Zone Set* options under *File* menu in the SANvergence Manager *mSAN Configuration* window. The *Save* option saves all SNMP transactions needed to recreate the current zone configuration. The file also contains all necessary information for SNMP transactions including IP addresses and matching passwords (community strings) in encrypted form.

Backup

To back up the SAN Router configuration, follow these instructions:

1. Choose *File>Configuration>Backup* to display the *Backup Configuration* dialog box (Figure 7-4).

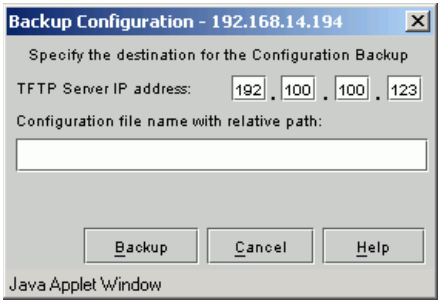


Figure 7-4 Backup Configuration Dialog Box

2. Enter the TFTP server IP address.

3. Enter the name of the file where the backup file will be stored. If you are entering a new file name, you must place it in an existing subdirectory of the TFTP root directory. The name may include a path if needed. The name is relative to the "root" directory defined in the TFTP server.
4. Click the *Backup* button.

Restore

To restore the SAN Router configuration from a backup file location, follow these instructions:

1. Select *File>Configuration>Restore* to display the *Restore Configuration* dialog box (Figure 7-5 on page 7-13).

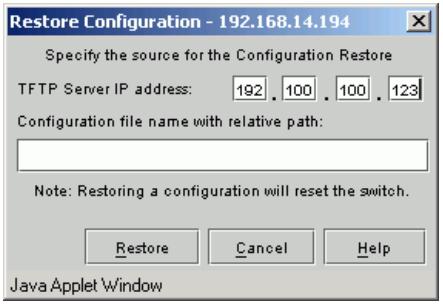


Figure 7-5 Restore Configuration Dialog Box

2. Enter the TFTP Server IP address.
3. Enter the name of a backup file from which you want to restore the configuration. The name may include a path if needed. The name is relative to the "root" directory defined in the TFTP server.
4. Click *Restore* to initiate the restore and automatic reset of the SAN Router.

Retrieving and Clearing the System Log

The *System Log* (different from the Element Manager *Message Log*) contains errors or warning states encountered at the SAN Router. The *System Log* information will be routinely requested by Technical Support whenever you report a problem.

Periodically, you should retrieve the *System Log* to preserve a copy, before emptying the contents. The System Log is of fixed size; new entries overwrite the existing oldest entries.

To upload the *System Log* from the SAN Router to the management workstation, follow these instructions:

1. Select *File>System Log>Retrieve* to display the *Retrieve System Log* dialog box (Figure 7-6 on page 7-14).

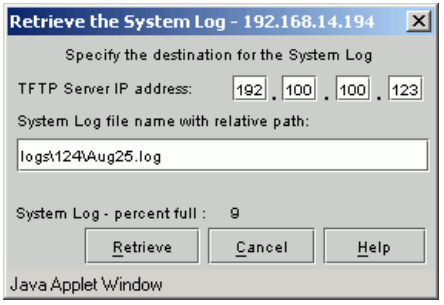


Figure 7-6 Retrieve the System Log Dialog Box

2. Type the IP address where the management workstation TFTP server resides.
3. Type or modify the name of the file where you want this segment of the log stored. For some TFTP servers, if you are creating a new file, you must place it in an existing subdirectory. The name may include a path if needed. The name is relative to the "root" directory defined in the TFTP server.
4. Click the *Retrieve* button.
5. Choose *File>System Log>Delete* to display the *Delete the System Log* dialog box (Figure 7-7). Use this dialog box to empty the contents after you retrieve the contents of the *System Log* from the SAN Router.

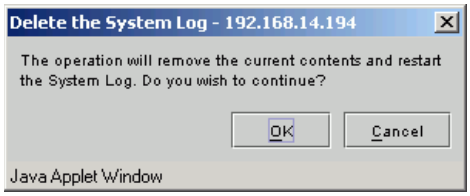


Figure 7-7 Delete the System Log

6. Click *OK* to empty the *System Log*. Deleting the system log contents avoids saving duplicate data the next time the log is retrieved.

8 Troubleshooting

This chapter gives the troubleshooting procedures for the Element Manager and the SAN Router.

Use the following links to move through this chapter.

Element Manager Troubleshooting

Use Table 8-1 on page 8-2 to troubleshoot problems you are having with the Element Manager application.

Table 8-1 Element Manager Problems and Solutions

Problem	Meaning and Solution
HTML Login page does not appear.	The browser error message: Could not reach the destination IP address or a *page not found* error or a DNS error. Either the SAN Router cannot be reached or the embedded web server in the SAN Router is not active. Try a ping request to the SAN Router to test connectivity. If the ping succeeds, it is likely that the embedded web server is down. The SAN Router may need to be rebooted to restart the web server. If the ping is not successful, there are several possible causes: • *A network problem between the management station and the SAN Router.* Try pinging other devices in the SAN Router's subnet. • *Incorrect or missing DNS entry.* Try starting Element Manager with the SAN Router's IP address instead of the host name. • *Access blocked by an HTTP proxy.* Check the web browser settings to disable any HTTP proxy. • *Wrong IP address.* Use a console connection to verify the management port address. If using inband management, such as managing through a FC/R port, use a console connection to verify the SAN Router's inband address. • *Missing default gateway or static route.* If the management station is not in the same subnet as the SAN Router's management port or inband address, then the SAN Router requires a default gateway or static route. Use a console connection to verify or add a default gateway or static route. • If the Management port hangs, use the CLI command *reset mgmt* to reset the management port
Login applet within the HTML Login page does not appear or takes a long time to appear.	The HTML Login page successfully loads but an empty gray box appears in the center of this page. The field to enter the password does not display. Sometimes a message appears in the upper left corner of the gray box stating that a jar file is being downloaded to the browsers. If the browser has been configured to use an HTTP proxy, there could be a lengthy delay (taking many minutes) to download the Element Manager java files from the SAN Router to the browsers. In Internet Explorer, use Tools>Internet Options>Connections>LAN to cancel all the selections. This will disable the proxy. To disable the proxy only for specific SAN Routers, click the *Advanced* button. Enter individual switch addresses or hostnames in the *Exceptions* box. (Using the '*' wildcard does not always work.) In Netscape 6, use Edit>Preferences> Advanced>Proxies to disable the proxy. To disable the proxy for only specific SAN Routers, enter the SAN Router inband IP addresses or hostnames in the *No Proxy for:* box.

Table 8-1 Element Manager Problems and Solutions (Continued)

Problem	Meaning and Solution
Login applet within the HTML Login page does not appear or takes a long time to appear. *(Continued)*	You can verify whether the correct version of the Java plug-in is installed by displaying the Windows *Control Panel*. A Duke or coffee-cup icon labeled "Java Plug-in" should display. Earlier versions my be present as well, but these are ignored by Element Manager. The Java plugin may be installed by any of the following methods: • Start Element Manager again and accept the offer to install the plug-in. • Install JRE v.1.4.2 from a CD. • Install SANvergence Manager (which includes the JRE 1.4.2). • Download the JRE from: http://java.sun.com/j2se/1.4.2/download.html. • On Solaris, use Netscape and select Help>About Plugins to see if the plug-in is listed. Having two different versions of the plug-in installed on the management workstation can also cause the problem. Uninstall one of the JRE versions.
After entering a password, an error message appears.	After entering a password and pressing the *Login* button, a message appears in the gray box and in an error dialog box that says "Incorrect password or device not responding." This could be due to one of the following: The wrong password was used or typed in incorrectly. Try re-typing the password with the appropriate access level (read or modify). Passwords are case-sensitive. Try a ping again to verify connectivity. If the ping succeeds, try to independently verify that the SNMP access is working. Start SANvergence Manager if it is available. If SANvergence Manager fails to connect to the SAN Router, the SNMP task on the SAN Router may be suspended. Contact Technical Support for further help. The SAN Router may be configured to accept SNMP only from certain IP addresses. This will prevent other management stations from logging in. Use a console connection to verify that the SNMP access control list is empty (disabled) or contains the management station's address.
Element Manager screen is not updated after entering the password.	Element Manager may not be responding. Check the error messages on the *Java Console* and report them to Customer Support. If there are no error messages and Element Manager repeatedly "hangs," you can set the Java Console to print out an Element Manager debug message. From the Windows *Control Panel*, start Java Plug-in 1.4.2 *Control Panel*. Select Show Java Console and enter this in the Java Runtime Parameters field:
Element Manager does not start on Windows 2000 with Internet Explorer 5.0.	In Internet Explorer 5.0 on Windows 2000, if the SAN Router URL does not end in "/", Element Manager does not start. A gray rectangle appears where the login prompt should be. This is a known problem with Internet Explorer 5.0 on Windows 2000. To fix this problem: upgrade to Internet Explorer 5.5 or 6.x, OR always end your Element Manager URLs with "/".

Table 8-1 **Element Manager Problems and Solutions (Continued)**

Problem	Meaning and Solution
Element Manager does not start on Solaris with Netscape.	If the Java plug-in is installed but not integrated with Netscape, Netscape stops with a black background and the logo displayed, but only a blank gray rectangle appears where the login button should be. To verify whether the plug-in is properly installed, click the Netscape *Help* button, then on About Plugins. Scroll down to see if Java Plug-in version 1.4.1 or 1.4.2 is listed. Plug-in installation directions are available at http://java.sun.com/j2se/1.4/install-solaris.html. Two steps are required: In your .profile or .cshrc, set the environment variable NPX_PLUGIN_PATH to the JRE directory containing the *javaplugin.so*. The default location is */usr/j2se/jre/plugin/sparc/ns4*. If the JRE was installed in a different location, substitute the real location for */usr/j2se/jre*. For Netscape 6, create a symbolic link from Netscape plugins directory to the JRE file *libjavaplugin_oji.so*. The default Netscape directory is */opt/SUNWns6/plugins*. The default JRE location is */use/j2se/jre/plugin/sparc/ns600/libjavaplugin-oji.so*.
The *Element Manager* window does not come up (after verifying the connection to the SAN Router).	• Ensure that the workstation for Element Manager meets the requirements described in *Workstation Requirements* on page 2-5. • Re-type the password for the appropriate login. • Verify that JRE 1.3.1 or higher is installed in your PC. • Make sure you are using one of the following supported browser versions: Netscape Navigator 6.x or higher Internet Explorer 6.0 or higher • When using Internet Explorer 5.0 there is a Microsoft issue that does not bring up an Element Manager from the browser unless you enter a "/" at the end of the URL. This is fixed in Internet Explorer 5.5+. • Make sure your display settings are set to: 1024 x 768 for the "Screen Area" and at least: 65536 for "Colors." • In Windows select Start>Settings>Control Panel>Display>Settings and check settings under the "Color" and "Screen Area" sections. • You may need to upgrade your display driver or adapter to achieve the best results.
The changes you make in Element Manager do not occur, or do not get saved after you reset the SAN Router.	• Most changes in Element Manager require you to click the *Apply* or *OK* button before you close the dialog box. • In order to save configuration changes beyond the next system reset, choose Save Configuration from the File menu. • Some changes don't take effect until you reset the SAN Router. Choose Reset System from the File menu.

SAN Router Troubleshooting

Use the following table to troubleshoot SAN Router problems, including configuration problems, through the Element Manager.

Table 8-2 SAN Router Problems and Solutions

Problem	Meaning and Solution
A yellow border appears around one of the ports on the Element Manager device view.	This indicates that the port is not properly configured or the port has been disabled. To enable the port: • Select *Configuration>Port>FC/Ethernet* to display the FC/Ethernet Configuration dialog box. • Select the affected port number from the drop-down list in the upper right corner. • Select the Enable Port checkbox. • Select OK.
There is a red outline around one of the ports on the Element Manager device view.	This indicates that the connection is down for that particular port. • The FC/R ports may display red if the cable is not plugged in securely. Check both to make sure that they have clicked into place. • Check cables for dents and tears, and make sure no large or sharp objects are on top of the cables (especially the FC/R cable).
You cannot download firmware when the management port has an IP address of 224.x.x.x or above	IP addresses of 224.x.x.x and above are Class D or Class E addresses that are specifically reserved for multicast addresses or for future use. Set the SAN Router management port IP address below 224.x.x.x to solve the problem.
You see the following error message: WARNING: IP ADDRESS IS 0, PLEASE SET IP ADDRESS AND RESET	The SAN Router does not yet have a valid inband IP address. Use the Inband Address Configuration dialog box (*Configuration >System >Inband Address*) to set the inband address.
Cannot download firmware using Element Manager.	• A TFTP server must be running on a server that the SAN Router can connect to through either the management port or a FC/R port. The TFTP protocol is not FTP. • File names and paths are critical. Try to move the firmware to the same directory on the servers where the TFTP server is located and use the name of the file with the new path in the dialog box. The path that you enter in Element Manager is always relative to the TFTP server's “root directory.” • Try pinging the IP address of the management port for out-of-band management or the SAN Router IP address for in-band management from the TFTP server (example: ping 192.168.2.170).

Table 8-2 SAN Router Problems and Solutions (Continued)

Problem	Meaning and Solution
After setting up iFCP configuration, remote devices are not displayed.	• Check both iFCP ports and make sure you have link lights between the port and the SAN Router/FC/R switch on either side. Ping across the link from local to the remote SAN Router. • Check in the Element Manager to make sure that each SAN Router has a unique mSAN ID (Configuration>iFCP>Setup) and that the SAN Router has been reset since this was changed. • Check in the Element Manager to make sure that the iFCP port IP addresses are on the same subnet or that the next hop router address is the correct next hop/gateway. • Check in the Element Manager to make sure that the Zone IDs are the same for the mutually exported zones (Configuration>iFCP>Remote Connections). • Check in the Element Manager to make sure that the remote SAN Router status is up by going to: Configuration>iFCP>Remote Connections and checking the Status column for the SAN Router in question. It should say "Up."
The operating system does not display the attached storage devices.	• Normally there is a problem with the connection, the interface, the zoning, port type or the drivers when the devices are not being recognized. Check the front panel of the SAN Router or use Element Manager to make sure the port type is set correctly for each port. Refer to the SAN Router's *Administration and Configuration Manual* for more details. Ensure that the transmit and receive optical lines are not reversed such that the transmitters are connected to each other. If you have SANvergence Manager, select one of the SAN Routers and select *mSAN Configuration* to display the *mSAN Configuration* win*dow.* Make sure the proper devices are listed and that they are in a common zone. If you need to make zone configuration changes, be sure to commit the changes and save them to flash memory in the SAN Router. Verify that the cables being used are intact and of good quality.

Table 8-2 SAN Router Problems and Solutions (Continued)

Problem	Meaning and Solution
You aren't sure which FC port type to assign.	FC port parameters that you can configure through the FC/Ethernet Port Configuration dialog box in the Element Manager include: • FC Auto - Ports that automatically sense whether the type of connection is F_Port or FL_Port. Use FC-Auto for connecting FC devices such as host bus adapters and storage targets. This will negotiate either arbitrated loop or point-to-point connections with the connected devices. • F_Port - A port to which non-loop N_Ports are attached. • FL_Port - A port to which one or more NL_Ports in an arbitrated loop are attached. • L_Port - Private loop or filer mode. In this mode, the port will come up in loop mode without requesting devices to do FLOGI; in other words, the connecting device is forced to be a private device. Most NAS filers need the port to be configured in this mode. • R_Port - A fabric extension port used to establish inter-switch links (ISLs) between a SAN Routers and FC switches. R_Port allows you to interconnect, zone, and manage existing fabrics with mSANs. R_Port is an added-cost option; it is not available in the basic SAN Router software package. Use R_Port to establish inter-switch links (ISLs) between FC switches and SAN Routers. R_Port allows you to interconnect, zone and manage existing fabrics with mSANs
You don't know whether to set your FC devices to Arbitrated Loop or Point-to-Point.	The SAN Router will support either arbitrated loop or point-to-point. Certain host bus adapter drivers or firmware have preferred modes in which they will try to negotiate one topology and revert to the other if that is not available. This is an unreliable method therefore we recommend you set your devices to point-to-point or arbitrated loop only mode.
The management station cannot access the management port of the SAN Router from a different subnet. Telnet access does not work. Cannot open the Element Manager for the SAN Router.	The SAN router has not been configured to reach the subnet. 1. Check whether IP connectivity exists to a different host in the SAN Router management subnet. 2. Try opening the Element Manager on a host residing on the same subnet as the SAN Router management port. In the Element Manger, select *Configuration >Port >Management* to display the *Management Port Configuration* dialog box. The management port subnet mask should be correct; it should not be 0.0.0.0. Select *Edit Gateway* to display the *Static Routing Configuratio*n dialog box. Select *Edit* under the *Permanent static route for management* area at the bottom of the dialog box, Set the *Permanent route next hop* to the next hop gateway IP address of the subnet. 3. Select *File>Save Configuration*, then *File>Reset System* to enable the changes.

Glossary

- *American National Standard Dictionary for Information Systems* (ANSI X3.172-1990), copyright 1990 by the American National Standards Institute (ANSI). Copies can be purchased from the American National Standards Institute, 25 West 42nd Street, New York, NY 10036. Definitions from this text are identified by *(A)*.
- *ANSI/EIA Standard - 440A: Fiber Optic Terminology*, copyright 1989 by the Electronic Industries Alliance (EIA). Copies can be purchased from the Electronic Industries Alliance, 2500 Wilson Blvd., Arlington, VA, 22201. Definitions from this text are identified by *(E)*.
- *IBM Dictionary of Computing* (ZC20-1699). Definitions from this text are identified by *(D)*.
- *Information Technology Vocabulary*. The terms and definitions taken from ISO/IEC 2382-1:1993, Information Technology Vocabulary - Part 1: Fundamental Terms, are reproduced with the permission of the International Organization for Standardization, ISO. This standard can be obtained from any ISO member and from the web site of the ISO Central Secretariat at the following address: www.iso.org. Copyright remains with ISO. Definitions of published parts of this vocabulary are identified by *(I)*.

NUMERICS

8B/10B A data encoding scheme developed by IBM, translating byte-wide data to an encoded 10-bit format.

10BaseT An implementation of the Institute of Electrical and Electronics Engineers (IEEE) Ethernet standard on 24-gauge unshielded twisted-pair wiring, a baseband medium at 10 Mbps.

100BaseT An implementation of the Institute of Electrical and Electronics Engineers (IEEE) Ethernet standard on 24-gauge unshielded twisted-pair wiring, a baseband medium at 100 Mbps.

A

AC *See* alternating current.

access The ability and means necessary to store data in, to retrieve data from, to transfer data into, to communicate with, or to make use of any resource of a storage device, a system, or area such as random access memory (RAM) or a register.

access time The amount of time, including seek time, latency, and controller time, necessary for a storage device to retrieve information.

address resolution protocol ARP. The protocol by which a host computer maintains a cache of address translations, allowing the physical address of the computer to be derived from the Internet address *(D)*.

agent Software that processes queries on behalf of an application and returns replies.

alarm (1) A notification of an abnormal condition within a system that provides an indication of the location or nature of the abnormality to either a local or remote alarm indicator. (2) A simple network management protocol (SNMP) message notifying an operator of a network or device problem.

alias A nickname representing a world-wide name.

AL_PA *See* arbitrated loop physical address.

alternating current AC. Electric current that reverses direction at regular sinusoidal intervals *(D)*. *Contrast with* direct current. *See* volts alternating current. *See also* alternating current/direct current converter.

alternating current/direct current converter AC/DC converter. A type of electronic equipment that changes AC energy into DC energy. Used as power sources in all modern electronic equipment.

American National Standard Code for Information Interchange ASCII. A standard character set consisting of 7-bit coded characters (8-bit including parity check) used for information exchange between systems and equipment *(D)*.

American National Standards Institute ANSI. A national organization consisting of producers, consumers, and general interest groups that establishes procedures by which accredited organizations create and maintain industry standards in the United States *(A, D)*.

ANSI *See* American National Standards Institute.

API *See* application program interface.

application (1) The use to which a data processing system is put, for example, a payroll application, an airline reservation application, or a network application. (2) A collection of software components used to perform specific types of work on a computer *(D)*.

application client The source object of the small computer system interface (SCSI) commands and destination for the command responses.

application program (1) A program that is specific to the solution of an application problem. Synonymous with application software. (2) A program written for or by a user that applies to the user's work, such as a program that does inventory control or payroll. (3) A program used to connect and communicate with stations in a network, enabling users to perform application-oriented activities *(I)*.

application program interface API. A set of programming functions and routines that provides access between protocol layers, such as between an application and network services.

application-specific integrated circuit ASIC. An asynchronous transfer mode (ATM) local area network/wide area network (LAN/WAN) circuit using cell relay transport technology. ASICs are designed for a specific application or purpose,

such as implementing the lower-layer Fibre Channel protocol (FC-0). They are particularly suited to sending video and audio information, as well as text. ASICs differ from general-purpose devices such as memory chips or microprocessors.

arbitrated loop One of the three connection topologies offered by Fibre Channel protocol. Up to 126 node ports and one fabric port can communicate without the need for a separate switched fabric. *See also* point-to-point.

arbitrated loop physical address AL_PA. A 1-byte value used in the arbitrated loop topology that identifies loop ports (L_Ports). This value then becomes the last byte of the address identified for each public L_Port on the loop.

arbitration Process of selecting one device from a collection of devices that request service simultaneously.

archive (1) To copy files to a long-term storage medium for backup. (2) Removing data, usually old or inactive files, from a system and permanently storing the data on removable media to reclaim system hard disk space.

area The second byte of the node port (N_Port) identifier.

ARP *See* address resolution protocol.

array Two or more disk drives connected to a host, and connected and configured such that the host perceives the disk drives to be one disk.

ASCII *See* American National Standard Code for Information Interchange.

ASIC *See* application-specific integrated circuit.

availability The accessibility of a computer system or network resource.

B

b *See* bit.

B *See* byte.

backbone Cable on which two or more stations or networks may be attached, typically used to link computer networks at one site with those at another. Smaller branch networks are sometimes called ribs.

backplane The backplane provides direct current (DC) power distribution and connections for all logic cards.

backup To copy files to a second medium (disk or tape) as a precaution in case the first medium fails.

backup diskette A diskette that contains duplicate information from an original diskette. The backup diskette is used in case information on the original diskette is unintentionally changed or destroyed *(D)*.

bandwidth (1) The amount of data that can be sent over a given circuit. (2) A measure of how fast a network can move information, usually measured in Hertz (Hz).

baud The unit of signaling speed, expressed as the maximum number of times per second the signal can change the state of the transmission line or other medium. The units of baud are seconds to the negative 1 power. Note: With Fibre Channel scheme, a signal event represents a single transmission bit.

BB_Credit *See* buffer-to-buffer credit.

ber *See* bit error rate.

bezel A removable panel that covers empty drive bays and port cards.

bidirectional In Fibre Channel protocol, the capability to simultaneously communicate at maximum speeds in both directions over a link.

bit Abbreviated as b. (1) Binary digit, the smallest unit of data in computing, with a value of zero or one *(D)*. (2) A bit is the basic data unit of all digital computers. It is usually part of a data byte or data word; however, a single bit can be used to control or read logic ON/OFF functions. (3) A bit is a single digit in a binary number. Bits are the basic unit of information capacity on a computer storage device. Eight bits equals one byte.

bit density Expressed as bits per inch (bpi), the number of bits that can be written on one inch of track on a disk surface.

bit error rate Abbreviated as ber. Ratio of received bits that contain errors to total of all bits transmitted.

bits per inch Abbreviated as bpi. Indicates the density of information on a hard drive.

blended fabric A routed storage area network (SAN) that includes both Fibre Channel and IP components in the SAN. The IP component could be iSCSI, or iFCP.

blocked port In a director or switch, the attribute that when set, removes the communication capability of a specific port. A blocked port continuously transmits the offline sequence.

boot (1) To start or restart a computer. (2) Loading the operating system.

bpi *See* bits per inch.

bps Bits per second.

Bps Bytes per second.

bridge (1) An attaching device that connects two local area network (LAN) segments to allow the transfer of information from one LAN segment to the other. A bridge can connect the LAN segments directly by network adapters and software in a single device, or can connect network adapters in two devices through software and use of a telecommunication link between the two adapters *(D)*. (2) A functional unit that connects two LANs that use the same logical link control protocol, but may use different media access control protocols *(D,T)*. *Contrast with* network router. (3) A device that connects and passes packets between two network segments that use the same communications protocol.

bridge port B_Port. (1) In Fibre Channel protocol, a fabric inter-element port used to connect bridge devices with E_Ports on a switch. B_Ports provide a subset of E_Port functionality. (2) A McDATA term for a physical interface between the fabric (switch) and a bridge device. The interface is identical to an expansion port (E_Port), but it does not participate in full expansion port protocols. As such, it does not assign domain IDs or participate in routing protocol. *See also* expansion port; fabric loop port; fabric port; generic port; hub port; node loop port; node port; segmented expansion port.

British thermal unit Btu. The quantity of heat required to raise the temperature of one pound of water by one degree Fahrenheit *(D)*.

broadband Large bandwidth communications channel capable of multiple, parallel high-speed transmissions.

broadcast In Fibre Channel protocol, to send a transmission to all node ports (N_Ports) on a fabric. *See also* broadcast frame.

broadcast frame In Fibre Channel protocol, a frame whose destination address specifies all node ports (N_Ports) in the fabric. *See also* broadcast.

Btu *See* British thermal unit.

buffer Storage area for data in transit. Buffers compensate for differences in processing speeds between devices. *See* buffer-to-buffer credit.

buffer-to-buffer credit BB_Credit. (1) The maximum number of receive buffers allocated to a transmitting node port (N_Port) or fabric port (F_Port). Credit represents the maximum number of outstanding frames that can be transmitted by that N_Port or F_Port without causing a buffer overrun condition at the receiver. (2) The maximum number of frames a port can transmit without receiving a receive ready signal from the receiving device. BB_Credit can be adjustable to provide different levels of compensation.

bus The path that carries data between the computer (microprocessor) and peripheral devices. An IDE interface cable and a small computer system interface (SCSI) cable are both examples.

bypassed port If a port is bypassed, all serial channel signals route past the port. A device attached to the port cannot communicate with other devices in the loop.

byte Abbreviated as B. A byte generally equals eight bits, although a byte can equal from four to ten bits. A byte can also be called an octet *See also* octet.

C

cache Random access memory (RAM) that is used by the redundant array of independent disks (RAID) controller to increase I/O throughput. If

write-back caching is enabled, this RAM can contain data that is not yet written to the disks in the array. In normal circumstances, this data is flushed from the RAM to the disk drives in the array with a maximum latency of 64 ms. If power fails to the subsystem (preventing the data from being written to the disk drives in the array), the battery holds the data for approximately 72 hours. If power is restored within that period, the data is flushed into the array and operation continues normally. If power has not been restored within 72 hours the data is lost.

cache memory A memory subsystem that stores recently used instructions and data for fast access. The larger the cache, the more information that can be stored, and the fewer time-consuming memory accesses a central processing unit (CPU) must make to complete a task. Cache is very fast memory, typically static random access memory (SRAM).

capacity The amount of information, measured in bytes, that can be stored on a hard drive.

cascade Linking two or more FC switches to form a larger switch or fabric. The switched link through fiber cables attached between one or more expansion ports (E_Ports). *See also* expansion port.

central processing unit CPU. The heart of the computer, this is the component that actually executes instructions.

central processor complex CPC. A physical grouping of hardware that includes a main storage device, one or more central processors, timers, and channels.

chained Two directors or switches that are physically attached.

one or two channels (primary and secondary). If a motherboard has only one channel, it may be necessary to add a controller card to create a secondary channel.

channel-attached (1) Pertaining to direct attachment of devices by data I/O channels to a computer *(D)*. (2) Pertaining to devices attached to a control unit by cables, not telecommunication lines *(D)*. *Synonymous with* local.

Class 2 Fibre Channel service Provides a connectionless (not dedicated) service with notification of delivery or nondelivery between two node ports (N_Ports).

Class 3 Fibre Channel service Provides a connectionless (not dedicated) service without notification of delivery or nondelivery between two node ports (N_Ports). *Synonymous with* datagram.

Class F Fibre Channel service — Used by switches to communicate across interswitch links (ISLs) to configure, control, and coordinate a multiswitch fabric.

Class of Fibre Channel service — Defines the level of connection dedication, acknowledgment, and other characteristics of a connection.

client — A node that requests network services from a server. Typically the node is a personal computer (PC).

client/server computing — Architectural model that functionally divides that execution of a unit of work between activities initiated by an end user or program (client) and those maintaining data (servers). Originally thought to make mainframes obsolete.

cluster — A group of processors interconnected by a high-speed network (typically dedicated) for increased reliability and scalability. Clusters are groupings of multiple servers in which information is shared among systems. When a server in a cluster fails, one of the other servers in the cluster assumes the responsibility of the failed server, thereby ensuring server, application, and data availability.

command — (1) A character string from an external source to a system that represents a request for system action *(D)*. (2) A request from a terminal to perform an operation or execute a program *(D)*. (3) A value sent through an I/O interface from a channel to a control unit that specifies the operation to be performed *(D)*.

communications tray — The communications tray is a sliding tray located in the middle of the Fabricenter cabinet. The communications tray holds the laptop personal computer (PC), zip drive, and zip drive power supply.

community name (SNMP) — A name that represents an simple network management protocol (SNMP) community that the agent software recognizes as a valid source for SNMP requests. A product recognizes a management station as a valid recipient for trap information when the station's community names are configured.

community profile — Information that specifies which management objects are available to what management domain or simple network management protocol (SNMP) community name.

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

component (1) Hardware or software that is part of a functional unit *(D)*. (2) A functional part of an operating system; for example, the scheduler or supervisor *(D)*.

computer A programmable machine that responds to a specific set of instructions in a well-defined manner and executes a prerecorded list of instructions (a program). Computers are both electronic and digital and are made up of both hardware (the actual machine-wires, transistors, and circuits) and software (instructions and data).

concurrent firmware upgrade Firmware is upgraded without disrupting switch operation.

concurrent maintenance Ability to perform maintenance tasks, such as removal or replacement of field-replaceable units (FRUs), while a hardware product is operating.

connectionless Non-dedicated link. Typically used to describe a link between nodes which allows the switch to forward Class 2 or Class 3 frames as resources (ports) allow. Contrast this with the dedicated bandwidth that is required in a Class 1 Fibre Channel Service (FC-1) point-to-point link.

connectivity The ability of devices to link together.

connector *Synonym for* optical fiber connector.

console *See* personal computer; server.

controller A computer module that interprets signals between a host and a peripheral device. The controller often is part of the peripheral device. *See* disk controller; disk drive controller; interface controller.

control program A computer program that schedules and supervises execution of programs in a computer system *(I)*.

control unit port CUP. An internal director or switch port on the control processor (CTP) card (labelled FE) that communicates with channels to report error conditions and link initialization *(D)*.

CPU *See* central processing unit.

CRC *See* cyclic redundancy check.

credit *See* buffer-to-buffer credit.

CUP *See* control unit port.

customer support *Synonym for* technical support.

cyclic redundancy check CRC. System of error checking performed at both the sending and receiving station using the value of a particular character generated by a cyclic algorithm. When the values generated at each station are identical, data integrity is confirmed.

D

daisy chaining Connecting one device to another in such a way that signals pass from one device to the next.

DASD *See* direct access storage device.

database A collection of data with a given structure for accepting, storing, and providing on-demand data for multiple users. *(I)*

data center A collection of servers and data storage devices, usually in one location, administered by an information technology/information services (IT/IS) manager.

data directory Critical information for all managed products (including directors and switches). Information stored here includes:

- All configuration data
- All log files
- Call-home settings
- Firmware library
- Zoning library

datagram *Synonym for* Class 3 Fibre Channel service.

data integrity Refers to the validity of data. Data integrity can be compromised in a number of ways including human errors when data is entered, errors that occur when data is transmitted from one computer to another, software bugs or viruses, hardware malfunctions (disk crashes), and

natural disasters (fires and floods). There are many ways to minimize these threats to data integrity such as backing up data regularly, controlling access to data via security mechanisms, designing user interfaces that prevent the input of invalid data, and using error detection and correction software when transmitting data.

data recovery Salvaging data stored on damaged media, such as magnetic disks and tapes. There are a number of software products that can help recover data damaged by a disk crash or virus. Of course, not all data is recoverable, but data recovery specialists can often restore a surprisingly high percentage of the data on damaged media.

dB *See* decibel.

dBm Decibels referenced to one milliwatt. Zero dBm equals one milliwatt, with a logarithmic relationship as the value increases *(D)*.

DC *See* direct current.

decibel Abbreviated as dB. A standard unit used to express gain or loss of optical power, expressed as the ratio of input power to output power on a logarithmic basis *(D)*.

default Pertaining to an attribute, value, or option that is assumed by a system when none is explicitly specified *(D, I)*.

default zone A zone that contains all attached devices that are not members of a separate active zone.

destination A point or location, such as a processor, director or switch, or server, to which data is transmitted *(D)*.

destination address D_ID. An address identifier that indicates the targeted destination of a data frame.

device (1) Mechanical, electrical, or electronic hardware with a specific purpose *(D)*. *See also* managed product.

(2) *See* node.

diagnostics (1) The process of investigating the cause or nature of a problem in a product or system *(D)*. (2) Procedures or tests used by computer users and service personnel to diagnose hardware or software problems *(D)*.

dialog box A pop-up window in the user interface with informational messages or fields to be modified or completed with the required options.

D_ID *See* destination address.

digital transmission Information is converted to binary computer code (a series of 0s and 1s). The information is sent in this format and then converted into its original format when it reaches its destination.

direct access storage device DASD. (1) Generic classification for a storage peripheral that can respond directly to random requests for information. Usually refers to a disk drive. (2) A storage device that provides direct access to data, and in which access time is independent of data location.

direct current DC. Electric current that continuously flows in one direction *(D)*. *Contrast with* alternating current. *See* volts direct current. *See also* alternating current/direct current converter.

director An intelligent, highly-available, FC switch providing any-to-any port connectivity between nodes (end devices) on a switched fabric. The director sends data transmissions (data frames) between nodes in accordance with the address information present in the frame headers of those transmissions.

disaster recovery A program that is designed to help companies get back to normal activities after a catastrophic interruption. Through failover to a parallel system, or by restoration of the failed system, disaster recovery restores the system to its normal operating mode.

disk controller The chip or circuit that controls the transfer of data between the disk and buffer. *See also* disk drive controller; interface controller.

disk drive controller The hard disk drive controller electronics that include the disk controller and the interface controller. *See also* disk controller; interface controller.

diskette A thin magnetic disk enclosed in a plastic jacket, which is removable from a computer and is used to store and transport data *(D)*.

diskette drive The hardware mechanism by which a computer reads data from and writes data to removable diskettes *(D)*.

disk mirroring The duplication of disks and controllers so that two access paths exist in case a failure occurs on one of them.

disk operating system DOS. The computer program that controls the organization of data, files, and processes on the computer.

DNS name Domain name system or domain name service. Host or node name for a device or managed product that is translated to an Internet protocol (IP) address through a domain name server.

domain A Fibre Channel term describing the most significant byte in the node port (N_Port) identifier for the Fibre Channel device. It is not used in the Fibre Channel small computer system interface (FC-SCSI) hardware path ID. It is required to be the same for all SCSI targets logically connected to a Fibre Channel adapter.

domain ID Domain identifier. A number that uniquely identifies a switch in a multiswitch fabric. A distinct domain ID is automatically allocated to each switch in the fabric by the principal switch. The preferred domain ID is the domain ID value that a switch requests from the principal switch. If the value has not been allocated to another switch in the fabric, it will be granted by the principal switch and will become the requesting switch's active domain ID. The active domain ID is the domain ID that has been assigned by the principal switch and that a switch is currently using.

domain name server In TCP/IP, a server program that supplies name-to-address translation by mapping domain name to internet addresses. *(D)*

DOS *See* disk operating system.

DRAM *See* dynamic random access memory.

drop-down menu A menu that appears when a heading in a navigation bar is clicked on with the mouse. The objects that appear in the drop-down menus are organize by their headings in the navigation bar.

dump The file that is created when the director detects a software fault. It contains various data fields that, when extracted, assist in the debugging of software.

duplex In data communication, pertaining to transmission in which data is sent and received at the same time *(D)*. *Contrast with* half duplex.

duplex connector An optical fiber component that terminates jumper cable fibers in one housing and provides physical keying for attachment to a duplex receptacle *(D)*.

duplex receptacle A fixed or stationary optical fiber component that provides a keyed attachment method for a duplex connector *(D)*.

dynamic connection A connection between two ports, established or removed by the directors and that, when active, appears as one continuous link.

The capability that allows connections to be established and removed at any time.

dynamic random access memory DRAM. Random access memory that resides in a cell consisting of a capacitor and transistor. DRAM data deteriorates (that is, is dynamic) unless the capacitor is periodically recharged by the controlling microprocessor. DRAM is slow, but relatively inexpensive *(D)*. *Contrast with* static random access memory.

E

EDI *See* electronic data interchange.

E_D_TOV *See* error-detect time-out value.

EE-PROM *See* electronically erasable programmable read-only memory.

EFC Enterprise Fabric Connectivity. The Fibre Channel protocol infrastructure made up of switches and directors in an enterprise. EFC is used to describe products such as EFC Management, EFC Manager application, or EFC Server.

EFC Audit Log Enterprise Fabric Connectivity *Audit Log*. Log displayed though the EFC Manager application that provides a history of user actions performed at the EFC Server through the EFC Manager application. This information is useful for system administrators and users.

EFCM Enterprise Fabric Connectivity Management. The management scheme for McDATA products. This includes the EFC Server, EFC Manager application, EFC Management Services application, and all Product Manager applications and their associated services.

EFC Management Services application EMS Application; Enterprise Fabric Connectivity Management Services Application. Software application that provides back-end product-independent services to the EFC Manager application. EFC

Management Services application runs only on the EFC Server and cannot be downloaded to remote workstations.

EFC Manager application — Enterprise Fabric Connectivity Manager application. (1) Software application that is the system management framework providing the user interface for managing McDATA Fibre Channel connectivity products. (2) The software application that implements the management user interface for all managed hardware products. The EFC Manager application can run both locally on the EFC Server and remotely on a user workstation.

EFCM Lite — Enterprise Fabric Connectivity Manager Lite version. EFCM Lite bundles the Product Manager application for a specific switch or director, the Enterprise Fabric Connectivity (EFC) Manager application, and the Fabric Manager application for installation on a customer-supplied server platform. Functionally, EFCM Lite and the standard EFCM applications installed on an EFC server are identical, except that EFCM Lite does not support the Call-Home and the automated Zip drive back up feature. In addition, EFCM Lite requires installation of the remote client application to a remote user workstation from the EFCM Lite CD.

EIA — *See* Electronic Industries Association.

electromagnetic interference — EMI. Undesirable electromagnetic emissions generated by solar activity, lightning, and electronic devices. The emissions interfere with or degrade the performance of another electronic device *(D)*.

electronically erasable programmable read-only memory — EE-PROM. A memory chip that can be loaded with data and later erased and loaded with update information.

electronic data interchange — EDI. The electronic transfer of preformatted business documents, such as purchase orders and bills of lading, between trading partners.

Electronic Industries Association — EIA. The governing body that publishes recommended standards for physical devices and associated interfaces. For example, RS-232 is the EIA standard that defines computer serial port connectivity *(D)*. *See also* Telecommunications Industry Association.

electronic mail — E-mail. Any communications service that permits the electronic transmission and storage of messages and attached or enclosed files.

electrostatic discharge ESD. The undesirable discharge of static electricity that can damage or degrade electronic circuitry *(D)*.

Element Manager application Application that implements the management user interface for a director, switch, or SAN Router.

e-mail *See* electronic mail.

EMI *See* electromagnetic interference.

EMS application *See* EFC Management Services application.

enclosure The physical box, rack, or box set that provides power, mechanical protection, external interfaces, and cooling for the small computer system interface (SCSI) devices.

enhanced availability feature EAF. A backup field-replaceable unit (backup FRU) that is ordered and installed to provide redundancy and reduce disruption in case of failure *(D)*.

enterprise The entire storage system. The series of computers employed largely in high-volume and multi-user environments such as servers or networking applications; may include single-user workstations required in demanding design, engineering and audio/visual applications.

Enterprise Fabric Connectivity *See* EFC.

Enterprise Fabric Connectivity Audit Log *See* EFC Audit Log.

Enterprise Fabric Connectivity Management *See* EFCM.

Enterprise Fabric Connectivity Management Services application *See* EFC Management Services application.

Enterprise Fabric Connectivity Manager application — *See* EFC Manager application.

Enterprise Fabric Connectivity Manager Lite — *See* EFCM Lite.

Enterprise Systems Architecture — ESA™. A computer architecture introduced by IBM in 1988 as ESA/370. The architecture added access registers to improve virtual memory management and increase storage from 2 gigabyte to 6 terabytes. The architecture was enhanced with the introduction of ESA/390 in 1990 *(D)*.

Enterprise Systems Connection — ESCON™. An IBM architecture, technology, and set of products and services introduced in 1990 that provides a dynamically connected environment using fiber-optic cables as the data transmission medium *(D)*.

Enterprise Systems Connection Director — ESCON™ Director. A device that provides connectivity capability and control for attaching any two links to each other through the ESON channel. Specifically, any of the hardware devices provided for interconnecting IBM-compatible mainframe equipment through the proprietary ESCON channel connection. IBM's model numbers for ESCON directors include the 9031 and 9033.

E_Port — *See* expansion port.

erase — To remove electrically or magnetically stored data, leaving the space where the data was stored unoccupied *(D)*.

error-detect time-out value — E_D_TOV. The time the switch waits for an expected response before declaring an error condition.

error message — Indication that an error has been detected *(D)*. *See also* information message; warning message.

ESA™ — *See* Enterprise Systems Architecture.

ESCON™ — *See* Enterprise Systems Connection.

ESCON™ Director — *See* Enterprise Systems Connection Director.

ESD — *See* electrostatic discharge.

Ethernet A widely implemented local area network (LAN) protocol that uses a bus or star topology and serves as the basis for the Institute of Electrical and Electronics Engineers (IEEE) 802.3 standard, which specifies the physical and software layers.

Ethernet hub A device used to connect the EFC Server and the directors it manages.

event code A three-digit number that specifies the exact event that occurred. This code provides information on system failures, such as hardware failures, failure locations, or general information on normal system events.

exchange A term that refers to one of the Fibre Channel protocol "building blocks," composed of one or more non concurrent sequences.

expansion port E_Port. Physical interface on a FC switch within a fabric, that attaches to an E_Port on another FC switch through an interswitch link (ISL) to form a multiswitch fabric. *See also* bridge port; fabric loop port; fabric port; generic port; hub port; node loop port; node port; segmented expansion port.

explicit fabric login The process by which a node port (N_Port) learns the characteristics of the fabric to which it is attached by sending a fabric login command (FLOGI) frame to the fabric port (F_Port) address FFFFFE (hexadecimal).

F

fabric Entity that interconnects node ports (N_Ports) and is capable of routing (switching) Fibre Channel frames, using the destination ID information in the Fibre Channel frame header accompanying the frames. A switch is the smallest entity that can function as a complete switched fabric topology.

A collection of one or more FC switches interconnected by E_Port ISLs. A fabric has its own fabric services such as a simple name server (SNS) and a management server. Routes between various end points in the fabric are calculated within the context of the fabric using Fabric Shortest Path First (FSPF) algorithms. Traditionally, a fabric has been referred to as a SAN or a SAN island.

fabric attached devices (FADs) End nodes that are attached to ports on FC switches within a fabric.

fabric element Any active director, switch, or node in a switched fabric.

fabric login The process by which node ports (N_Ports) establish their operating parameters. During fabric login, the presence or absence of a fabric is determined, and paths to other N_Ports are mapped. Specific operating characteristics for each port, such as buffer-to-buffer credit (BB_Credit) and data frame size, are also established.

fabric login command FLOGI. The command that establishes the initial operating parameters and topology for a fabric. The command is accepted by a fabric port (F_Port) *(D)*.

fabric loop port FL_Port. A fabric port (F_Port) that contains arbitrated loop (AL) functions associated with the Fibre Channel arbitrated loop (FC-AL) topology. The access point of the fabric for physically connecting an arbitrated loop of node loop ports (NL_Ports). *See also* bridge port; expansion port; fabric port; generic port; hub port; node loop port; node port; segmented expansion port.

fabric mode *See* interoperability mode.

fabric port F_Port. Physical interface within the fabric that connects to a node port (N_Port) through a point-to-point full duplex connection. *See also* bridge port; expansion port; fabric loop port; generic port; hub port; node loop port; node port; segmented expansion port.

fabric services The services that implement the various Fibre Channel protocol services that are described in the standards. These services include the fabric controller (login server), name server, and management server.

fabric switches A device which allows the communication between multiple devices using Fibre Channel protocols. A fabric switch enables the sharing bandwidth and end-nodes using basic multiplexing techniques.

failover Automatic and nondisruptive transition of functions from an active field-replaceable unit (FRU) that has failed to a backup FRU.

fast/wide SCSI *See* fast/wide small computer system interface.

fast/wide small computer system interface Fast/wide SCSI. Fast and wide are relative terms in comparing previous SCSI standards and products. Fast, as defined in SCSI-2, refers to a maximum synchronous transfer rate of 10 MHz. Wide refers to a data path of 16 bits.

fault tolerance The ability of a system to respond gracefully to an unexpected hardware or software failure. There are many levels of fault tolerance, the lowest being the ability to continue operation in the event of a power failure. Many fault-tolerant computer systems mirror all operations.

FC *See* Fibre Channel.

FC-0 The Fibre Channel layer that describes the physical link between two ports, including the transmission media, transmitter and receiver circuitry, and interfaces *(D)*. This consists of a pair of either optical fiber or electrical cables (link media) along with transceiver circuitry which work together to convert a stream of bits at one end of the link to a stream of bits at the other end.

FC-1 Middle layer of the Fibre Channel physical and signaling interface (FC-PH) standard, defining the 8B/10B encoding/decoding and transmission protocol.

FC-2 The Fibre Channel layer that specifies the signaling protocol, rules, and mechanisms required to transfer data blocks. The FC-2 layer is very complex and provides different classes of service, packetization, sequencing, error detection, segmentation, and reassembly of transmitted data *(D)*.

FC-3 The Fibre Channel layer that provides a set of services common across multiple node ports (N_Ports) of a Fibre Channel node. The services are not commonly used and are essentially reserved for Fibre Channel architecture expansion *(D)*.

FC-4 The Fibre Channel layer that provides mapping of Fibre Channel capabilities to upper level protocols (ULP), including Internet protocol (IP) and small computer system interface (SCSI) *(D)*.

FCA *See* Fibre Channel Association.

FC-AL *See* Fibre Channel arbitrated loop.

FC adapter Fibre Channel adapter. *See* host bus adapter.

FCC Federal Communications Commission.

FCC-IOC *See* Fibre Channel I/O controller.

FCFE *See* Fibre Channel fabric element.

FCFE-MIB *See* Fibre Channel fabric element management information base.

FCIA *See* Fibre Channel Industry Association.

FC IP *See* Fibre Channel IP address.

FCMGMT *See* Fibre Channel management framework integration.

FC_NAT Fibre Channel Network Address Translation. The SAN router does address translation when devices in different fabrics communicate with each other. These devices could be from fabrics within an mSAN or from different mSANs within an iSAN. This address translation is a key component of SAN Routing and is used to maintain the autonomous nature of each of the fabrics. Address translation shields the fabrics from having addressing conflicts with other fabrics that are using the same domain IDs.

FC-PH *See* Fibre Channel physical and signaling interface.

feature key A unique key to enable additional product features. This key is entered into the *Configure Feature Key* dialog box in the Product Manager application to activate optional hardware and software features. Upon purchasing a new feature, McDATA will provide the feature key to the customer.

fiber The fiber-optic cable made from thin strands of glass through which data in the form of light pulses is transmitted. It is used for high-speed transmissions over medium (200 m) to long (10 km) distances.

fiber-optic cable *Synonym for* optical cable.

fiber optics The branch of optical technology concerned with the transmission of radiant power through fibers of transparent materials such as glass, fused silica, or plastic *(E)*. Telecommunication applications of fiber optics use optical fibers. A single fiber or a non spatially aligned fiber bundle is used for each information channel. Such fibers are often

called optical fibers to differentiate them from fibers that are used in non communication applications *(D)*.

fibre A generic Fibre Channel term used to cover all transmission media types specified in the Fibre Channel physical layer (FC-PH) standard such as optical fiber, copper twisted pair, and copper coaxial cable.

Fibre Channel FC. Integrated set of standards recognized by American National Standards Institute (ANSI) which defines specific protocols for flexible information transfer. Logically, a point-to-point serial data channel, structured for high performance.

Fibre Channel adapter FC adapter. *See* host bus adapter.

Fibre Channel address A 3-byte node port (N_Port) identifier which is unique within the address domain of a fabric. Each port may choose its own identifier, or the identifier may be assigned automatically during fabric login.

Fibre Channel arbitrated loop FC-AL. A high-speed (100 Mbps) connection which is a true loop technology where ports use arbitration to establish a point-to-point circuit. Data can be transferred in both directions simultaneously, achieving a nominal transfer rate between two devices of 200 Mbps.

Fibre Channel Association FCA. The FCA is a non-profit corporation consisting of over 150 members throughout the world. Its mission is to nurture and help develop the broadest market for Fibre Channel products through market development, education, standards monitoring, and fostering interoperability among members' products.

Fibre Channel fabric element FCFE. Any device linked to a fabric.

Fibre Channel fabric element management information base FCFE-MIB. A table of variables available to network management stations and resident on a switch or director. Through the simple network management protocol (SNMP) these pointers can be manipulates to monitor, control, and configure the switch or director.

Fibre Channel Industry Association FCIA. A corporation consisting of over 100 computer industry-related companies. Its goal is to provide marketing support, exhibits, and trade shows for its member companies. The FCIA complements activities of the various standards committees.

Fibre Channel I/O controller

FCC-IOC. In a director, the integrated controller on the control processor (CTP) card dedicated to the task of managing the embedded Fibre Channel port. In a director or switch, the FCC-IOC controls the embedded Fibre Channel port and configures the ports' application-specific integrated circuits (ASICs).

Fibre Channel IP address

FC IP. The default Fibre Channel IP on a new switch is a temporary number divided by the switch's world-wide name (WWN). The system administrator needs to enter a valid IP address.

Fibre Channel management framework integration

FCMGMT. A standard defined by the Fibre Alliance to provide easy management for Fibre Channel-based devices such as switches, hubs, and host-bus adapters.

Fibre Channel physical and signaling interface

FC-PH. The American National Standards Institute (ANSI) document that specifies the FC-0 (physical signaling), FC-1 (data encoding), and FC-2 (frame construct) layers of the Fibre Channel protocol *(D)*.

Fibre Channel standard

American National Standards Institute (ANSI) standard that provides a common, efficient data transport system that supports multiple protocols. The architecture integrates both channel and network technologies, and provides active, intelligent interconnection among devices. All data transmission is isolated from the control protocol, allowing use of point-to-point, arbitrated loop, or switched fabric topologies to meet the needs of an application.

Fibre Connection

FICON. An IBM set of products and services introduced in 1999 that is based on the Fibre Channel Standard. FICON technology uses fiber-optic cables as the data transmission medium, and significantly improves I/O performance (including one Gbps bi-directional data transfer). FICON is designed to coexist with ESCON™ channels, and FICON-to-ESCON control unit connections are supported *(D)*.

fibre port module

FPM. A 1 gigabit-per-second module that contains four generic ports (G_Ports).

FICON

See Fibre Connection.

FICON Management Server

An optional feature that can be enabled on the director or switch or switch through the Product Manager application. When enabled, host control and management of the director or switch or switch is provided through an S/390 Parallel Enterprise or 2/Series Server attached to a director or switch or switch port.

field-replaceable unit FRU. Assembly removed and replaced in its entirety when any one of its components fails *(D)*.

file server A computer that stores data centrally for network users and manages access to that data.

file transfer protocol FTP. A transmission control protocol/Internet protocol (TCP/IP) -based client/server protocol used to transfer files to and from a remote host. Does not perform any conversion or translation.

firewall A networking device that blocks unauthorized access to all or parts of a network.

firewall zoning Hardware enforced access between F_Ports enforced at the source port. The hardware verifies the destination port against the zone defined for the source port.

firmware Embedded program code that resides and runs on, for example, directors, switches, and hubs.

FLASH memory Reusable nonvolatile memory that is organized as segments for writing, and as bytes or words for reading. FLASH memory is faster than read-only memory, but slower than random access memory *(D)*.

FLOGI *See* fabric login command.

FL_Port *See* fabric loop port.

FPM *See* fibre port module.

F_Port *See* fabric port.

frame A variable-length packet of data that is transmitted in frame relay technology.

FRU *See* field-replaceable unit.

FTP *See* file transfer protocol.

full-duplex The capability to transmit in two directions simultaneously.

G

gateway address (1) In transmission control protocol/Internet protocol (TCP/IP), a device that connects two systems that use the same or different protocols. (2) In TCP/IP, the address of a router to which a device sends frames destined for addresses not on the same physical network (for example, not on the same Ethernet) as the sender. The hexadecimal format for the gateway address is XXX.XXX.XXX.XXX.

Gb *See* gigabit.

GB *See* gigabyte.

GbIC *See* gigabit interface converter.

Gbps Acronym for gigabits per second.

generic port G_Port. Physical interface on a director or switch that can function either as a fabric port (F_Port) or an expansion port (E_Port), depending on the port type to which it connects. *See also* bridge port; expansion port; fabric loop port; fabric port; hub port; node loop port; node port; segmented expansion port.

GHz *See* gigahertz.

gigabit Gb. A unit of measure for data storage, equal to approximately 134,217,728 bytes. Approximately one eighth of a gigabyte.

gigabit Ethernet An evolving standard that will be used to support ultra high-speed connections along the backbone of Internet and intranet networks. Supports transmission rates of one Gigabit per second.

gigabit interface converter GbIC. A removable module that converts an electrical serial data stream to an optical or amplified electrical serial data stream. Contains connector for attaching fiber-optic cable.

gigabyte GB. A unit of measure for data storage, equal to 1,073,741,824 bytes. Generally approximated as one billion bytes *(D)*.

gigahertz GHz. One billion cycles per second (Hertz) *(D)*.

G_Port *See* generic port.

graphical user interface GUI. A visually oriented interface where the user interacts with representations of real-world objects displayed on the computer screen. Interactions with such objects produce actions that are intuitive to the user *(D)*.

ground That portion of a conducting circuit connected to the earth *(D)*.

GSM card A generic port (G_Port) module card containing shortwave laser ports for multimode fiber-optic cables.

GUI *See* graphical user interface.

H

half duplex The capacity to transmit in two directions, but not simultaneously.

hard drive An electromechanical device used for information storage and retrieval, incorporating one or more rotating disks on which data is recorded, stored, and read magnetically.

hardware Physical equipment (director, switch, or personal computer) as opposed to computer programs or software.

hardware management console The console runs the Hardware Management console application (HWMCA), and is the operations and management personal computer (PC) platform for S/390 and z/Series servers.

HBA *See* host bus adapter.

Hertz Hz. A unit of frequency equal to one cycle per second.

heterogeneous fabric A fabric containing open-fabric-compliant products from various vendors. *Contrast with* homogeneous fabric.

hexadecimal A numbering system with base of sixteen; valid numbers use the digits 0 through 9 and characters A through F, where A represents 10 and F represents 15 *(D)*.

high availability A performance feature characterized by hardware component redundancy and concurrent maintenance. High-availability systems maximize system uptime while providing superior reliability, availability, and serviceability.

high performance parallel interface — HiPPI. A point-to-point, high speed channel that operates in parallel between two devices at distances of up to 10 km. An American National Standards Institute (ANSI) standard for 800 Mbps channel link.

high speed serial data connect — HSSDC. An option for connecting a subsystem to a host computer.

HiPPI — *See* high performance parallel interface.

homogeneous fabric — A fabric consisting of only one vendor's products. *Contrast with* heterogeneous fabric.

hop — (1) Data transfer from one node to another node. (2) Describes the number of switches that handle a data frame from its origination point through it's destination point.

hop count — The number of hops a unit of information traverses in a fabric.

host — The computer that other computers and peripherals connect to.

host bus adapter — HBA. Logic card that provides a link between the server and storage subsystem, and that integrates the operating systems and I/O protocols to ensure interoperability.

host processor — (1) A processor that controls all or part of a user application network *(I)*. (2) In a network, the processing unit in which resides the access method for the network *(D)*.

hot pluggable — *See* concurrent maintenance.

hot spare — *See* field-replaceable unit.

hot swap — *See* concurrent maintenance.

hot-swapping — *See* concurrent maintenance.

H_Port — *See* hub port.

HSSDC — *See* high speed serial data connect.

HTTP — *See* hypertext transport protocol.

hub (1) In Fibre Channel protocol, a device that connects nodes into a logical loop by using a physical star topology. (2) In Ethernet, a device used to connect the EFC Server and the directors it manages.

hub port H_Port. In arbitrated loop devices, a port that uses arbitrated loop protocols. The physical interface that attaches to a loop device, either an end device or another loop interconnect device (hub).

hyperlink A predefined link for jumping from one location to another, within the same computer or network site or even to a location at a completely different physical location. Commonly used on the world wide web for navigation, reference, and depth where published text will not suffice.

hypertext transport protocol HTTP. A simple protocol that allows world wide web pages to be transferred quickly between web browsers and servers.

Hz *See* Hertz.

I

ID *See* identifier.

identifier ID. (1) One or more characters used to identify or name a data element and possibly to indicate certain properties of that data element *(D, T)*. (2) A sequence of bits or characters that identifies a program, device, or system to another program, device, or system.

IEEE *See* Institute of Electrical and Electronics Engineers.

IML *See* initial machine load.

Imported Devices A device from a different fabric or a different mSAN that must be accessible is first registered in the router metro storage name server (mSNS) by a process called importing, whereby a virtual representation of the remote device is registered in the local fabric and the local mSAN.

inband address The internal router inband IP address configured through the Inband Address Configuration dialog box in the Element Manager is used for:

- Addressing storage traffic between the local SAN Router and directly-attached storage devices router-attached (storage) devices (RADs). Similarly, this address may be used as the external "router" next hop IP address by directly-attached devices RADs to transmit storage traffic to other SAN Routers in the internal IP network.
- Communication between the metro storage name servers (mSNS) on the different SAN Routers.
- Communicating with other SAN Routers across a metro area storage area network (mSAN).
- mSNS messages, spanning tree messages, and routing control messages from other SAN Routers are sent to this inband address.

inband management Management of the director or switch through Fibre Channel. An interface connection to a port card. *Contrast with* out-of-band management.

industry standard architecture ISA. Bus architecture designed for personal computers (PCs) that use an Intel 80386, 80486, or Pentium microprocessor. ISA buses are 32 bits wide and support multiprocessing.

Infiniband The name applied to the merged specifications for Next Generation Input Output (NCGIO) from Intel and System IO from Compaq, HP, and IBM. Infiniband is a serial interconnect technology with a wire/fiber data speed of 2.5 GB. The basic Infiniband is a full-duplex dual wire/fiber.

information message Message notifying a user that a function is performing normally or has completed normally. *See also* error message; warning message.

information services IS. IS is the name of the department responsible for computers, networking, and data management. *See also* information technology.

information technology IT. The broad subject concerned with all aspects of managing and processing information, especially within a large organization or company. Because computers are central to information management, computer departments within companies and universities are often called IT departments. *See also* information services; ITE.

initial machine load IML. Hardware reset for all installed control processor (CTP) cards on the director or switch. This reset does not affect other hardware. It is initiated by pushing the *IML* button on a director's or switch's operating panel.

initial program load IPL. The process of initializing the device and causing the operating system to start. An IPL may be initiated through a menu option or a hardware button.

initial program load configuration IPL configuration. In S/390 mode, information stored in a director or switch's nonvolatile memory that contains default configurations. The director or switch loads the file for operation when powered on.

input/output I/O. (1) Pertaining to a device whose parts can perform an input process and an output process at the same time *(I)*. (2) Pertaining to a functional unit or channel involved in an input process, output process, or both, concurrently or not, and to the data involved in such a process *(D)*. (3) Pertaining to input, output, or both *(D)*. (4) An operation or device that allows input and output.

input/output controller IOC. A functional unit in a data processing system that controls one or more devices or units of peripheral equipment *(A, D, I)*.

Institute of Electrical and Electronics Engineers IEEE. An organization of engineers and technical professionals that promotes the development and application of electronic technology and allied sciences.

integrated product Hardware product that is mounted in the Fabricenter cabinet. For example, any director or switch shipped with in the Fabricenter cabinet is an integrated product.

interface (1) A shared boundary between two functional units, defined by functional, signal, or other characteristics. The concept includes the specification of the connection of two devices having different functions *(I)*. (2) Hardware, software, or both, that link systems, programs, or devices *(D)*.

interface controller The chip or circuit that translates computer data and commands into a form suitable for use by the hard drive and controls the transfer of data between the buffer and the host. *See also* disk controller; disk drive controller.

internal IP address Storage traffic that is to be transported through the external network by iFCP or iSCSI must first be delivered to the iFCP/iSCSI port that

will perform the iFCP/iSCSI encapsulation. The SAN Router's internal IP address is used by the iFCP/iSCSI port to receive this storage traffic from the internal network. This traffic is then re-addressed and re-encapsulated into an iFCP/iSCSI connection that traverses the external network. This address is configured through the *FC/Ethernet Port Configuration* dialog box in the Element Manager.

Internet Fibre Channel Protocol (iFCP) A gateway-to-gateway protocol for providing Fibre Channel fabric services to Fibre Channel end devices over a TCP/IP network. The iFCP protocol uses TCP for congestion control, error detection, and recovery.

Internet protocol IP. Network layer for the transmission control protocol/Internet protocol (TCP/IP) protocol used on Ethernet networks. IP provides packet routing, fragmentation, and reassembly through the data link layer *(D)*.

Internet protocol address IP address. Unique string of numbers (in the format xxx.xxx.xxx.xxx) that identifies a device on a network.

internetworked SAN (iSAN) An internetworked storage area network (iSAN) is a collection of one or more fabrics interconnected using one or more SAN routers, where typically, at least one fabric is in a distant location outside the metro area. An iSAN is characterized by high latency and low bandwidth ISLs (T1, T3, OC3, etc.) such as those found in wide area networks. An iSAN has at least two SAN routers that are interconnected using iFCP connections. An iSAN is also a collection of two or more mSANs. SAN routing done within an iSAN is referred to as iSAN Routing or SAN Routing over distance. An iSAN could also be deployed entirely within a data center to scale beyond the metrics of an mSAN.

internetworked SAN routing Internetworked storage area network (iSAN) routing is routing across an IP network to a remote mSAN interconnected by SAN Routers.

Internet Small Computer Interface (iSCSI) Protocol The iSCSI protocol defines a means of transporting SCSI packets over TCP/IP, providing for an interoperable solution which can take advantage of existing internet infrastructure, internet management facilities and address distance limitations.

interoperability Ability to communicate, execute programs, or transfer data between various functional units over a network.

interoperability mode Interop mode. An operating mode set through McDATA director and switch management software that allows products to operate in homogeneous or heterogeneous fabrics.

interop mode *See* interoperability mode.

inter-router ISL Two or more SAN routers can be interconnected using inter-router interswitch links (ISLS) for box-level redundancy and/or to provide more R_Ports for connecting fabrics. Currently, the inter-router links are GE connections. The protocol used to communicate between the routers over the GE connections could be Internet Fibre Channel Protocol (iFCP).

interrupt A signal sent by a subsystem to the central processing unit (CPU) that signifies a process has either completed or could not be completed.

interswitch link ISL. Physical expansion port (E_Port) connection between two directors in a fabric.

interswitch link hop ISL hop. *See* hop.

intranet A private version of the Internet that provides a cost-effective way to publicize critical information and that provides an interactive communication path for heterogeneous systems. Internal to a specific organizational structure and secured from or disconnected from the global Internet.

I/O *See* input/output.

IP *See* Internet protocol.

IP address *See* Internet protocol address.

IPL *See* initial program load.

IPL configuration *See* initial program load configuration.

IS *See* information services.

ISL *See* interswitch link.

ISL hop Interswitch link hop. *See* hop.

isolated E_Port Isolated expansion port. *See* segmented expansion port.

isolated expansion port Isolated E_Port. *See* segmented expansion port.

IT *See* information technology.

ITE Information technology equipment. *See also* information technology.

J

Java An object-oriented programming language derived from C++ that produces code that is platform independent. Developed by Sun Microsystems designed for distribution and distributable applications development. Java applications require a program called the Java Virtual Machine (JVM) to execute. JVMs have been developed for many of the mainstream platforms and operating systems.

JBOD *See* just a bunch of disks.

jumper cable Optical cable that provides physical attachment between two devices or between a device and a distribution panel. *Contrast with* trunk cable. *See also* optical cable.

just a bunch of disks JBOD. Refers to a rack of disks without data redundancy or striping.

K

Kb *See* kilobit.

KB *See* kilobyte.

kilobit Kb. A unit of measure for data storage, equaling 1,024 bits, or two to the tenth power. Kilobits are generally approximated as being one thousand bits.

kilobyte KB. A unit of measure for data storage, equaling 1,024 bytes, or two to the tenth power. Kilobytes are generally approximated as being one thousand bytes.

L

LAN *See* local area network.

laser Laser is an acronym for light amplification by stimulated emission of radiation. A device that produces a very powerful narrow beam of coherent light of a single wavelength by simulating the emissions of photons from atoms, molecules, or ions.

latency Amount of time elapsed between receipt of a data transmission at a switch's incoming fabric port (F_Port) from the originating node port (N_Port) to retransmission of that data at the switch's outgoing F_Port to the destination N_Port. The amount of time it takes for data transmission to pass through a switching device.

LCD Liquid crystal display.

LED *See* light-emitting diode.

LIC *See* licensed internal code.

licensed internal code LIC. Software provided for use on specific IBM machines and licensed to customers under the terms of IBM's customer agreement. Microcode can be LIC and licensed as such *(D)*.

light-emitting diode LED. A semiconductor chip that emits visible or infrared light when electricity passes through it. LEDs are used on switch or director field-replaceable units (FRUs) and the front bezel to provide visual indications of hardware status or malfunctions.

LIN *See* link incident.

link Physical connection between two devices on a switched fabric. A link consists of two conductors, one used for sending and the other for receiving, thereby providing a duplex communication path.

link incident LIN. Interruption to link due to loss of light or other causes. *See also* link incident alerts.

link incident alerts A user notification, such as a graphic symbol in the Product Manager application *Hardware View* that indicates that a link incident has occurred. *See also* link incident.

LIP *See* loop initialization primitive.

LMA — *See* loader/monitor area.

load balancing — Ability to evenly distribute traffic over multiple interswitch links within a fabric. Load balancing on McDATA directors and switches takes place automatically.

loader/monitor area — LMA. Code that resides in the loader/monitor area of the control processor (CTP) card. Among other functions, LMA code provides I/O functions available through the maintenance port, operator panel, server interface, terminal window command functions, power up diagnostics, field-replaceable unit (FRU) power-on hours update, and data read/write control, and LMA code/licensed internal code (LIC) download functions *(D)*.

local — *Synonym for* channel-attached.

local area network — LAN. A computer network in a localized geographical area (for example, a building or campus), whose communications technology provides a high-bandwidth medium to which many nodes are connected *(D)*. *See also* metropolitan area network; metro-area storage area network (mSAN); wide area network.

logical partition — LPAR. A processor hardware subset defined to support the operation of a system control program, and can be used without affecting any of the applications in another partition *(D)*.

logical port address — In a director or switch, the address used to specify port connectivity parameters and to assign link addresses for the attached channels and control units.

logical unit number — LUN. In Fibre Channel addressing, a logical unit number is a number assigned to a storage device which, in combination with the storage device's node port's world-wide name, represents a unique identifier for a logical device on a storage area network. Peripherals use LUNs to represent addresses. A small computer system interface (SCSI) device's address can have up to eight LUNs.

login server — Entity within the Fibre Channel fabric that receives and responds to login requests.

longwave — Lasers or light-emitting diodes (LEDs) that emit light with wavelengths around 1300 nm. When using single mode (9 nm) fiber, longwave lasers can be used to achieve lengths greater than 2 Km.

loop A loop is a configuration of devices connected to the fabric via a fabric loop port (FL_Port) interface card.

loop address In Fibre Channel protocol, a term indicating the unique ID of a node in Fibre Channel loop topology, sometimes referred to as a loop ID.

loopback plug In a fiber optic environment, a type of duplex connector used to wrap the optical output signal of a device directly to the optical input. *Contrast with* protective plug. *Synonymous with* wrap plug.

loopback test Test that checks attachment or control unit circuitry, without checking the mechanism itself, by returning the output of the mechanism as input.

loop initialization primitive LIP. In an arbitrated loop device, a process by which devices connected to hub ports (H_Ports) on the arbitrated loop device notify other devices and the switch of the presence in the loop by sending LIP sequences and subsequent frames through the loop. This process allows linked arbitrated loop devices to perform fabric loop port (FL_Port) arbitration as they link through hub ports.

loop master In an arbitrated loop device, a reference to the loop master world-wide name (WWN) field in the *Loop View*, the loop master is the arbitrated loop device that is responsible for allocating arbitrated loop physical addresses (AL-PAs) on the loop. An arbitrated loop device becomes the loop master through arbitration when there are multiple arbitrated loop devices on the loop. The arbitrated loop device with the lowest WWN becomes the loop master.

loop port L_Port. *Synonym for* hub port.

loop switches Loop switches support node loop port (NL_Port) Fibre Channel protocols. Switches sold as loop support but upgradeable to fabric switches recounted as loop switches.

LPAR *See* logical partition.

L_Port Loop port. *Synonym for* hub port.

LUN *See* logical unit number.

M

MAC address — *See* media access control address.

mainframe — A powerful multi-user computer capable of supporting many hundreds or thousands of users simultaneously.

maintenance analysis procedure — MAP. A written or online set of procedures that guide maintenance personnel through step-by-step instructions for hardware fault isolation, repair, and verification *(D)*.

maintenance port — Connector on the director or switch where a PC running an American National Standard Code for Information Interchange (ASCII) terminal emulator can be attached or dial-up connection made for specialized maintenance support.

MAN — *See* metropolitan area network.

managed product — Hardware product that can be managed with the EFC Product Manager application. McDATA directors and switches are managed products. *See also* device.

management information base — MIB. Related set of software objects (variables) containing information about a managed device and accessed via simple network management protocol (SNMP) from a network management station.

management session — A session that exists when a user logs on to the EFC Manager application. EFC can support multiple concurrent management sessions. The user must specify the network address of the EFC Manager application's server at logon time.

MAP — *See* maintenance analysis procedure.

Mb — Megabit.

MB — *See* megabyte.

Mbps — Megabits per second.

MBps — Megabytes per second.

media access control address — MAC address. Hardware address of a node (device) connected to a network.

megabyte MB. A unit of measure for data storage, equal to 1,048,576 bytes. Generally approximated as one million bytes.

memory A device or storage system capable of storing and retrieving data.

menu A list of items displayed on a monitor from which a user can make a selection.

menu bar The menu bar is located across the top of a monitor window. Pull-down menus are displayed by clicking on the menu bar option with the mouse, or by pressing **Alt** with the underlined letter of the name for the menu bar option *(D)*.

message path controller card MPC card. In the ED-5000 Director, a card that provides the mechanism for messages to be sent and received between ports on the director. The card also provides a system clock source, and central control and distribution of clocks for MPC, G_Port module (GPM), and central memory module (CMM) cards. *See also* Fibre Channel I/O controller.

metropolitan area network MAN. A network capable of high-speed communications over distances up to about 100 kilometers. *See also* local area network; metro-area storage area network (mSAN); wide area network.

metropolitan storage name server (mSNS) The SAN Router's metro storage name server (mSNS) stores the inventory of hosts and storage devices in the mSAN, as well as zoning information, to specify which hosts can use which storage devices.

MIB *See* management information base.

mirroring The writing of data to pairs of drives in an array, creating two exact copies of the drive contents. This procedure provides a backup of data in case of a failure.

modem Modem is an abbreviation for modulator/demodulator. A communication device that converts digital computer data to signals and signals to computer data. These signals can be received or transmitted by the modem via a phone line or other method of telecommunication.

ms Millisecond.

metro-area storage area network (mSAN)

A metro-area storage area network (mSAN) is a collection of one or more fabrics interconnected using one or more SAN routers, where all the fabrics are within a data center or in different data centers that are within the metro area. An mSAN is characterized by low latency, high quality and high bandwidth ISLs such as those found within the data center or within the metro area using technologies such as dark fiber, xWDM, MAN services, etc. If there are multiple SAN routers in an mSAN, they are interconnected using mFCP connections. SAN routing done within an mSAN is referred to as mSAN Routing or SAN Routing within the data center. An mSAN may be referred to as a local mSAN within the context of its own mSAN, while all the other mSANs that it is communicating with are referred to as remote mSANs. *See also* local area network; metropolitan area network; wide area network.

multimedia

A simultaneous presentation of data in more than one form, such as by means of both visual and audio.

multimode optical fiber

A graded-index or step-index optical fiber that allows more than one mode (light path) to propagate *(D)*. *Contrast with* singlemode optical fiber.

Multiple Virtual Storage

MVS™. The generic name for an IBM-licensed operating system used on System/370 and later mainframe processors. Introduced in 1974, it continues to be used though it has been mostly superseded by the newer IBM operating system, Operating System/390 (OS/390™) *(D)*.

Multiple Virtual Storage/Enterprise Systems Architecture

MVS/ESA™. *See* Enterprise Systems Architecture; Multiple Virtual Storage.

multiplexer

A device that allows two or more signals to be transmitted simultaneously on a single channel.

multiswitch fabric

Fibre Channel fabric created by linking more than one director or fabric switching device within a fabric.

MVS™

See Multiple Virtual Storage.

MVS/ESA™

See Multiple Virtual Storage/Enterprise Systems Architecture.

N

name server (1) In TCP/IP, *see* domain name server. (2) In Fibre Channel protocol, a server that allows node ports (N_Ports) to register information about themselves. This information allows N_Ports to discover and learn about each other by sending queries to the name server.

name server zoning Node port (N_Port) access management that allows N_Ports to communicate if and only if they belong to a common name server zone.

NAS *See* network-attached storage.

network An arrangement of hardware, software, nodes, and connecting branches that consists of a data communication system. The International Organization for Standardization (ISO) seven-layer specification partitions a computer network into independent modules from the lowest (physical) layer to the highest (application) layer *(D)*.

network address Name or address that identifies a device on a transmission control protocol/Internet protocol (TCP/IP) network. The network address can be either an IP address in dotted-decimal notation (composed of four three-digit octets in the format xxx.xxx.xxx.xxx) or a domain name (as administered on a customer network).

network-attached storage NAS. Storage connected directly to the network, through a processor and its own operating system. Lacks the processor power to run centralized, shared applications.

network interface card NIC. An expansion board inserted into a computer so the computer can be connected to a network. Most NICs are designed for specific types of networks, protocols, and medias, although some can serve multiple networks.

network management The broad subject of managing computer networks. There exists a wide variety of software and hardware products that help network system administrators manage a network. Network management covers a wide area, including security, performance, and reliability.

network router An attaching device that connects two local area network (LAN) segments, which use similar or different architectures, at the reference model network layer *(D)*. *Contrast with* bridge.

never principal The setting that prevents the product from becoming the principal switch for a fabric.

next hop gateway address The iFCP/iSCSI ports on the SAN Router interact with the external IP network as if they were independent IP hosts. Each iFCP/iSCSI port needs a gateway address of an external router that can forward the storage traffic to the remote iFCP/iSCSI port. This next hop gateway address is the first-hop gateway address.

NIC *See* network interface card.

nickname Alternate name assigned to a world-wide name for a node, director or switch in the fabric.

NL_Port *See* node loop port.

node In Fibre Channel protocol, an end device (server or storage device) that is or can be connected to a switched fabric. *See also* device.

node loop port NL_Port. A physical interface within an end device (node) that participates in a loop containing one or more fabric loop ports (FL_Ports) or other NL_Ports. *See also* bridge port; expansion port; fabric loop port; fabric port; generic port; hub port; node port; segmented expansion port.

node port N_Port. Physical interface within an end device that can connect to an fabric port (F_Port) on a switched fabric or directly to another N_Port (in point-to-point communications). *See also* bridge port; expansion port; fabric loop port; fabric port; generic port; hub port; node loop port; segmented expansion port.

node port identifier N_Port ID. In Fibre Channel protocol, a unique address identifier by which an N_Port is uniquely known. It consists of a domain (most significant byte), an area, and a port, each 1 byte long. The N_Port ID is used in the source identifier (S_ID) and destination identifier (D_ID) fields of a Fibre Channel frame.

nondisruptive maintenance *See* concurrent maintenance.

nonvolatile random access memory NV-RAM. RAM that retains its content when the device power is turned off.

N_Port *See* node port.

N_Port ID *See* node port identifier.

NV-RAM *See* nonvolatile random access memory.

O

octet An 8-bit quantity, often called a byte or word. An octet can equal a byte as long as the byte equals eight bits. *See also* byte.

OEM *See* original equipment manufacturer.

offline Referring to data stored on a medium, such as tape or even paper, that is not available immediately to the user.

offline diagnostics Diagnostics that only operate in stand alone mode. User operations cannot take place with offline diagnostics running.

offline sequence OLS. (1) Sequence sent by the transmitting port to indicate that it is attempting to initialize a link and has detected a problem in doing so. (2) Sequence sent by the transmitting port to indicate that it is offline.

offline state When the switch or director is in the offline state, all the installed ports are offline. The ports transmit an offline sequence (OLS) and they cannot accept a login got connection from an attached device. *Contrast with* online state.

ohm A unit of electrical resistance equal to that of a conductor in which a current of one ampere is produced by a potential of one volt across the conductor terminals *(D)*.

OLS *See* offline sequence.

online Referring to data stored on the system so it is available immediately to the user.

online diagnostics Diagnostics that can be run by the customer engineer while the operational software is running. These diagnostics do not impact user operations.

online state When the switch or director is in the online state, all of the unblocked ports are allowed to log in to the fabric and begin communicating. Devices can connect to the switch or director if the port is not blocked

and can communicate with another attached device if both devices are in the same zone, or if the default zone is enabled. *Contrast with* offline state.

Open Systems Architecture OSI. A model that represents a network as a hierarchical structure of functional layers. Each layer provides a set of functions that can be accessed and used by the layer above. Layers are independent, in that implementation of a layer can be changed without affecting other layers *(D)*.

operating system OS. Software that controls execution of applications and provides services such as resource allocation, scheduling, I/O control, and data management. Most operating systems are predominantly software, but partial hardware implementations are possible *(D, T)*.

Operating System/390 OS/390™. An integrated, open-enterprise server operating system developed by IBM that incorporates a leading-edge and open communications server, distributed data and file services, parallel Sysplex™ support, object-oriented programming, distributed computing environment, and open application interfaces *(D)*.

optical cable Single fiber, multiple fibers, or a fiber bundle in a structure built to meet optical, mechanical, and environmental specifications *(D, E)*. *See also* jumper cable; trunk cable. *Synonymous with* fiber-optic cable.

optical drive backup A data backup system that uses rewriteable optical cartridges (ROCs) as the storage medium *(D)*.

optical fiber connector *Synonymous with* connector.

ordered set In Fibre Channel protocol, four 10-bit characters (a combination of data and special characters) providing low-level link functions, such as frame demarcation and signaling between two ends of a link. It provides for initialization of the link after power-on and for some basic recovery functions.

original equipment manufacturer OEM. A company that has a special relationship with computer producers. OEMs buy components and customize them for a particular application. They sell the customized computer under their own name. OEMs may not actually be the original manufacturers. They are usually the customizers and marketers.

OS *See* operating system.

OS/390™ *See* Operating System/390.

OSI *See* Open Systems Architecture.

out-of-band management Transmission of management information, using frequencies or channels other than those routinely used for information transfer.

P

packet In Fibre Channel protocol, Logical unit of information (usually in the form of a data frame) transmitted on a network. It contains a header (with all relevant addressing and timing information), the actual data, and a trailer (which contains the error checking function, usually in the form of a cyclic redundancy check), and frequently user data.

panel A logical component of the interface window. Typically, a heading and/or frame marks the panel as an individual entity of the window. Size and shape of the panel and its data depend upon the purpose of the panel and may or may not be modified.

partition A way to logically divide a hard drive so that an operating system treats each partition as a separate hard drive. Each partition has a unique drive letter.

PC *See* personal computer.

persistent binding A form of server-level access control that uses configuration information to bind a server to a specific Fibre Channel storage volume (or logical device), using a unit number.

personal computer PC. A portable computer that consists of a system unit, display, keyboard, mouse, one or more diskette drives, and internal fixed-disk storage *(D)*.

point-to-point A Fibre Channel protocol topology that provides a single, direct connection between two communication ports. The director or switch supports only point-to-point topology *(D)*. *See also* arbitrated loop.

port Receptacle on a device to which a cable leading to another device can be attached. Ports provide Fibre Channel connections *(D)*.

port address name A user-defined symbolic name of 24 characters or less that identifies a particular port address.

port card Field-replaceable hardware component that provides the port connections for fiber cables and performs specific device-dependent logic functions.

port card map Map showing port numbers and port card slot numbers inside a hardware cabinet.

POST *See* power-on self-test.

power-on self-test POST. Series of diagnostic tests that are run automatically by a device when the power is turned on

preferred domain ID Configured value that a switch will request from the Principal Switch. If the preferred value is already in use, the Principal Switch will assign a different value.

preventive service planning bucket PSP bucket. Collected problems after early ship of an IBM product.

principal switch In a multiswitch fabric, the switch that allocates domain IDs to itself and to all other switches in the fabric. There is always one principal switch in a fabric. If a switch is not connected to any other switches, it acts as its own principal switch.

printed wiring assembly PWA. A thin board on which integrated circuits and other electronic components are placed and connected to each other via thin copper traces.

private device A loop device that cannot transmit a fabric login command (FLOGI) command to a switch or director, nor communicate with fabric-attached devices. *Contrast with* public device.

private loop A private loop is not connected to a switched fabric, and the switch's embedded expansion port (E_Port) and fabric loop port (FL_Port) are inactive. All devices attached to the loop can only communicate with each other. *Contrast with* public loop.

processor complex A system configuration that consists of all the machines required for operation, for example, a processor unit, a processor controller, a system display, a service support display, and a power and coolant distribution unit.

product name User-configurable identifier assigned to a managed product. Typically, this name is stored on the product itself. A director or switch product name can also be accessed by a simple network management protocol (SNMP) manager as the system name.

prohibited port connection In a director or switch, in S/390 operating mode, an attribute that removes dynamic connectivity capability.

proprietary Privately owned and controlled. In the computer industry, proprietary is the opposite of open. A proprietary design or technique is one that is owned by a company. It also implies that the company has not divulged specifications that would allow other companies to duplicate the product. Increasingly, proprietary architectures are seen as a disadvantage. Consumers prefer open and standardized architectures, which allow them to mix and match products from different manufacturers.

protective plug In a fiber-optic environment, a type of duplex connector (or cover) that provides physical protection *(D)*. *Contrast with* loopback plug.

protocol (1) Set of semantic and syntactic rules that determines the behavior of functional units in achieving communication. (2) In systems network architecture, the meanings of and sequencing rules for requests and responses for managing the network, transferring data, and synchronizing network component states *(D)*. (3) A specification for the format and relative timing of data exchanged between communicating devices *(D, I)*.

PSP bucket *See* preventive service planning bucket.

public device A loop device that can transmit a fabric login command (FLOGI) to a switch, receive acknowledgement from the switch's login server, register with the switch's name server, and communicate with fabric-attached devices. Public devices communicate with fabric-attached devices through the switch's bridge port (B_Port) connection to a director or switch. *Contrast with* private device.

public loop A public loop is connected to a switched fabric (through the switch bridge port (B_Port)), and the switch has an active embedded fabric loop port (FL_Port) that is user transparent. All devices attached to the loop can communicate with each other, and public devices attached to the loop can communicate with fabric-attached devices. *Contrast with* private loop.

pull-down menu *See* drop-down menu.

PWA *See* printed wiring assembly.

R

radio frequency interference RFI. Electromagnetic radiation which is emitted by electrical circuits carrying rapidly changing signals, as a by-product of the normal operation, and which causes unwanted signals (interference or noise) to be induced in other circuits.

RAID *See* redundant array of independent disks.

RAM *See* random access memory.

random access memory RAM. A group of computer memory locations that is numerically identified to allow high-speed access by the controlling microprocessor. A memory location is randomly accessed by referring to its numerical identifier *(D)*. *Contrast with* read-only memory. *See* also dynamic random access memory; nonvolatile random access memory; static random access memory.

R_A_TOV *See* resource allocation time-out value.

read-only memory ROM. An information storage chip with permanent memory. Stored information cannot be changed or deleted except under special circumstances *(D)*. *Contrast with* random access memory.

redundancy Performance characteristic of a system or product whose integral components are backed up by identical components to which operations will automatically failover in the event of a component failure. Redundancy is a vital characteristic of virtually all high-availability (24 hours/7 days per week) computer systems and networks.

redundant array of independent disks RAID. Grouping of hard drives in a single system to provide greater performance and data integrity. RAID systems have features that ensure data stored on the drives are safe and quickly retrievable.

remote notification A process by which a system is able to inform remote users and workstations of certain classes of events that occur on the system. E-mail notification and the configuration of simple network

management protocol (SNMP) trap recipients are two examples of remote notification programs that can be implemented on director-class switches.

remote user workstation Workstation, such as a personal computer (PC), using EFC Manager application and Product Manager application software that can access the EFC Server over a local area network (LAN) connection.

repeater A device that generates and often amplifies signals to extend transmission distance.

rerouting delay An option that ensures that frames are delivered in order through the fabric to their destination.

resource allocation time-out value R_A_TOV. R_A_TOV is a value used to time-out operations that depend on the maximum possible time that a frame could be delayed in a fabric and still be delivered.

rewriteable optical cartridge ROC. A plastic cartridge with a recording medium that uses magneto-optical read/write technology, and is removable from a computer and used to store and transport data *(D)*.

RFI *See* radio frequency interference.

ring topology A logically circular, unidirectional transmission path without defined ends, in which control is distributed or centralized *(D)*. *See also* token ring.

RISC Reduced instruction set computer. A type of microprocessor that recognizes a limited number of instructions. A benefit of this is that a RISC is faster than a complex central processing unit (CPU) which has more instructions to follow.

ROC *See* rewriteable optical cartridge.

ROM *See* read-only memory. *Contrast with* random access memory.

routed SAN A collection of individual fabrics, connected by intermediate (multi-protocol) storage networking devices. This SAN functions as a single large storage network providing any-to-any connectivity, while maintaining the autonomous nature of each of the individual fabrics. The storage networking devices that are interconnecting the various fabrics are called SAN Routers and the process by which

SAN routers send data from one end node to another in a routed SAN is called SAN Routing or SAN Internetworking.

router attached devices (RADs) End nodes that are either directly attached to an Fibre Channel port on a SAN Router or were imported from a different fabric via a SAN Router are referred to as router-attached devices. Devices that are directly attached to an Fibre Channel port on a router are called local router-attached devices (LRADs) within the context of that mSAN. Devices that are imported from a different fabric within the mSAN or a different mSAN altogether (for example, they were imported over iFCP connections) are called remote router-attached devices (RRADs).

router fabric manager An R_Port that controls the zoning, fabric discovery, device registration and other fabric related activities between the router and an attached fabric. The router fabric manager acts a conduit between the SNS in the fabric and the router SNS (mSNS and/or iSNS).

router zone set A group of router zones (that may or may not have members) that you can activate or deactivate as a single entity across the mSAN is called a router zone set.

routing domain Virtual domains that enable representation/addressing of devices that are not part of a local fabric. The SAN router uses two routing domains – one to enable routing between various fabrics within an mSAN, and the other to enable routing between mSANs. The two routing domains are visible within a fabric

R_Port An mSAN Routing E_Port (R_Port) is a port on a SAN router used for an ISL connection to a FC switch.

RS-232 The Electronic Industry Association (EIA)-recommended specification for asynchronous serial interfaces between computers and communications equipment. It specifies both the number of pins and type of connection, but does not specify the electrical signals *(D)*.

S

SA/MVS™ *See* System Automation for Operating System/390.

mSAN *See* metro-area storage area network (mSAN); system area network.

SANavigator SANavigator management software provides easy, centralized management of a SAN and quick access to all device configuration applications.

SAN ID A number between 0 and 4,294,967,295 that uniquely identifies an mSAN.

SANpilot interface The interface provides a graphical user interface (GUI) similar to the Product Manager application, and supports director or switch configuration, statistics monitoring, and basic operations. With director or switch firmware installed, administrators or operators with a browser-capable personal computer (PC) and an Internet connection can monitor and manage the director or switch through the SANpilot interface.

SANpilot interface timeout If the SANpilot interface is running but no user activity occurs, (such as viewing different pages, refreshing, or reconfiguring information), the application times out after 30 minutes. The user must log in again. A login dialog box displays if the user attempts to access any pages after the timeout has occurred.

SANpilot interface window The window for the SANpilot interface. The window is divided into two separate panels: the navigation panel on the left, and the main panel on the right.

SAN Router cluster ID The R_Port SAN routing cluster ID is used by the SAN Router R_Ports to register a unique virtual node WWN to the connected fabrics. Third-party management applications use this WWN to manage the SAN Router.

SAN Router time zone The Simple Network Transfer Protocol (SNTP) server's time zone that is configured in the Element Manager *Date/Time* dialog box. This allows SNTP clients to adjust the time to their local time zone as needed.

SA OS/390™ *See* System Automation for Operating System/390.

scalable Refers to how well a system can adapt to increased demands. For example, a scalable network system could start with just a few nodes but easily expands to thousands of nodes. Scalability is important because it allows the user to invest in a system with confidence that a business will not outgrow it. Refers to anything whose size can be changed.

SCSI — *See* small computer system interface.

segment — A fabric segments when one or more switches cannot join the fabric because of various reasons. The switch or switches remain as separate fabrics.

segmented E_Port — *See* segmented expansion port.

segmented expansion port — Segmented E_Port. E_Port that has ceased to function as an E_Port within a multiswitch fabric due to an incompatibility between the fabrics that it joins. *See also* bridge port; fabric loop port; fabric port; generic port; hub port; node loop port; node port.

serial port — A full-duplex channel that sends and receives data at the same time. It consists of three wires: two that move data one bit at a time in opposite directions, and a third wire that is a common signal ground wire.

server — A computer that provides shared resources, such as files and printers, to the network. Used primarily to store data, providing access to shared resources. Usually contains a network operating system.

SFP transceivers — *See* small form factor pluggable transceivers.

shared mode — If a director or switch is in shared mode, all devices on the loop share the 100MB bandwidth available on the loop. In shared mode, only one end device can communicate with another device through the fabric loop port (FL_Port) on the director or switch.

shortwave — Lasers or light-emitting diodes (LEDs) that emit light with wavelengths around 780 nm or 850 nm. When using multimode fiber (50 nm) shortwave lasers can be used with Fibre Channel links less than 500 m. To achieve longer lengths, single-mode fiber is required. The preferred fiber core size is 50 micron as this fiber has large bandwidth so that the distance is limited by the fiber attenuation. A 62.5 micron core size is also supported for compatibility with existing FDDI installations. Fiber of this type has smaller bandwidth and, in this case, the distance is limited by the fiber bandwidth.

simple mail transfer protocol — SMTP. A transmission control protocol/Internet protocol (TCP/IP) protocol that allows the user to create, send, and receive text messages. SMTP protocols specify how messages are passed across a link from one system to another. They do not specify how the mail application accepts, presents, or stores the mail.

simple network management protocol

SNMP. A transmission control protocol/Internet protocol (TCP/IP)-derived protocol governing network management and monitoring of network devices.

simple network management protocol community

SNMP community. Also known as SNMP community string. SNMP community is a cluster of managed products (in SNMP terminology, hosts) to which the server or managed product running the SNMP agent belongs.

simple network management protocol community name

SNMP community name. The name assigned to a given SNMP community. Queries from an SNMP management station to a device running an SNMP agent will only elicit a response if those queries are addressed with the correct SNMP community name.

simple network management protocol management station

SNMP management station. An SNMP workstation personal computer (PC) used to oversee the SNMP network.

simple network management protocol version 1

SNMP v1. The original standard for SNMP is now referred to as SNMP v1. The ES-2500 uses SNMP v1.

simple network management protocol version 2

SNMP v2. The second version of the SNMP standard. This version expands the functionality of SNMP and broadens its ability to include OSI-based, as well as TCP/IP-based, networks as specified in RFC 1441 through 1452.

singlemode optical fiber

An optical fiber that allows one wavelength-dependent mode (light path) to propagate *(D)*. *Contrast with* multimode optical fiber.

small computer system interface

SCSI. An interface standard that enables computers to communicate with peripherals connected to them. Commonly used in enterprise computing and in Apple Macintosh systems. Usually pronounced as "scuzzy." The equivalent interface in most personal computers is enhanced integrated drive electronics (EIDE). *See* fast/wide small computer system interface.

A narrow SCSI adapter supports up to eight devices, including itself. SCSI address 7 has the highest priority followed by 6, 5, 4, 3, 2, 1, 0, with 0 being the lowest priority.

small form factor pluggable transceivers — SFP transceivers. Laser-based optical transceivers for a wide range of networking applications requiring high data rates. The transceivers, which are designed for increased densities, performance, and reduced power, are well-suited for Fibre Channel applications.

SMTP — *See* simple mail transfer protocol.

SNMP — *See* simple network management protocol.

SNMP community — *See* simple network management protocol community.

SNMP community name — *See* simple network management protocol community name.

SNMP management station — *See* simple network management protocol management station.

SNMP v1 — *See* simple network management protocol version 1.

SNMP v2 — *See* simple network management protocol version 2.

SONET — *See* synchronous optical network.

SRAM — *See* static random access memory.

state — The state of the switch or director. Possible values include online, offline, testing, and faulty. See offline state; online state.

static random access memory — SRAM. SRAM is microprocessor-cache random access memory. It is built internal to the microprocessor or on external chips. SRAM is fast, but relatively expensive *(D). Contrast with* dynamic random access memory.

stored addresses — In S/390 mode, a method for configuring addresses.

subnet — A portion of a network that shares a common address component. On transmission control protocol/Internet protocol (TCP/IP) networks, subnets are defined as all devices whose IP addresses have the same prefix. Dividing a network into subnets is useful for both security and performance reasons. IP networks are divided using a subnet mask.

subnet mask — A mask used by a computer to determine whether another computer with which it needs to communicate is located on a local or remote network. The network mask depends upon the class of networks to

which the computer is connecting. The mask indicates which digits to look at in a longer network address and allows the router to avoid handling the entire address. Subnet masking allows routers to move the packets more quickly. Typically, a subnet may represent all the machines at one geographic location, in one building, or on the same local area network.

switch A device that connects, filters and forwards packets between local area network (LAN) segments or storage area network (SAN) nodes or devices.

switched mode If the arbitrated loop device is in switched mode, each pair of communicating ports on the arbitrated loop device can share the 100MB bandwidth. In switched mode, up to three pairs of loop devices can communicate with each other simultaneously. Or, a public device on the loop can communicate with another device on the fabric while up to two pairs of loop devices can communicate simultaneously.

switchover Changing a backup field-replaceable unit (FRU) to the active state, and the active FRU to the backup state.

switch priority Value configured into each switch in a fabric that determines its relative likelihood of becoming the fabric's principal switch. Lower values indicate higher likelihood of becoming the principal switch. A value of 1 indicates the highest priority; 225 is the lowest priority. A value of 225 indicates that the switch is not capable of acting as the principal switch. The value 0 is illegal.

synchronous optical network SONET. A standard for optical network elements. Basic level is 51.840 megabit/second (OC-1); higher levels are *n* times the basic rate (OC-*n*).

System Automation for Operating System/390 SA OS/390™. IBM licensed software that provides System/390 Parallel Sysplex™ management, automation capabilities, and integrated systems and network management. SA OS/390 manages host, remote processor, and I/O operations. SA OS/390 integrates the functions of Automated Operations Control for Multiple Virtual Storage (MVS™), ESCON™ Manager, and Target System Control Facility *(D)*.

system name *See* product name.

T

TB *See* terabyte.

TCP *See* transmission control protocol.

TCP/IP *See* transmission control protocol/Internet protocol.

technical support Single point of contact for a customer when assistance is needed in managing or troubleshooting a product. Technical support provides assistance twenty-four hours a day, seven days a week, including holidays. The technical support number is **(800) 752-4572** or **(720) 566-3910**. *Synonymous with* customer support.

Telecommunications Industry Association TIA. A member organization of the Electronic Industries Association (EIA), TIA is the trade group representing the communications and information technology industries. *See also* Electronic Industries Association.

telnet The Internet standard protocol for remote terminal connection over a network connection.

terabyte TB. One thousand (1,000) gigabytes; one terabyte of text on paper would consume 42,500 trees. At 12 characters per inch, 1 TB of data in a straight line would encircle the earth 56 times and stretch some 1.4 million miles equalling nearly three round trips from the earth to the moon.

TIA *See* Telecommunications Industry Association.

TKRG *See* token ring controller adapter card.

token A sequence of bits passed from one device to another on a token ring network that signifies permission to transmit over the network. The token consists of a starting delimiter, access control field, and end delimiter. If a device has data to transmit, it appends the data to the token *(D)*.

token ring A local area network (LAN) configuration where devices attach to a network cable in a closed path or ring. A token (unique sequence of bits) circulates on the ring to allow devices to access the LAN for data transmission *(D)*. *See also* ring topology.

token ring controller adapter card TKRG. The circuit card that provides a port to connect a director or switch to a 4/16 Mbps token ring local area network (LAN) *(D)*.

topology Logical and/or physical arrangement of stations on a network.

transceiver modules Transceiver modules come in longwave, extra longwave, or shortwave laser versions, providing a single fiber connection.

transfer rate The speed with which data can be transmitted from one device to another. Data rates are often measures in megabits (Mbps) or megabytes (MBps) per second, or gigabits (Gbps) or gigabytes per second (GBps).

transistor-transistor logic TTL. A common type of digital circuit in which the output is derived from two transistors. The term TTL is often used to describe any system based on digital circuitry.

transmission control protocol TCP. The transport layer for the transmission control protocol/Internet protocol (TCP/IP) protocol widely used on Ethernet networks and any network that conforms to U.S. Department of Defense standards for network protocol. TCP provides reliable communication and control through full-duplex connections *(D)*.

transmission control protocol/Internet protocol TCP/IP. A layered set of protocols (network and transport) that allows sharing of applications among devices on a high-speed local area network (LAN) communication environment *(D)*. *See also* transmission control protocol; Internet protocol.

trap Unsolicited notification of an event originating from a simple network management protocol (SNMP) managed device and directed to an SNMP network management station.

trap host Simple network management protocol (SNMP) management workstation that is configured to receive traps.

trap recipient In simple network management protocol (SNMP), a network management station that receives messages through SNMP for specific events that occur on the arbitrated loop device.

trunk cable Cable consisting of multiple fiber pairs that do not directly attach to an active device. This cable usually exists between distribution panels and can be located within, or external to, a building *(D)*. *Contrast with* jumper cable. *See also* optical cable.

TTL *See* transistor-transistor logic.

twisted pair Relatively low-speed transmission medium consisting of two insulated wires arranged in a regular spiral pattern. The strands are twisted to improve protection against electromagnetic and radio frequency interference. The wires may be shielded or unshielded.

U

UDP *See* user datagram protocol.

UL *See* Underwriters Laboratories.

ULP *See* upper level protocol.

unblocked port Devices communicating with an unblocked port can login to the director or switch and communicate with devices attached to any other unblocked port (assuming that this is supported by the current zoning configuration).

Underwriters Laboratories UL. A laboratory organization accredited by the Occupational Safety and Health Administration and authorized to certify products for use in the home and workplace *(D)*.

unicast Communication between a single sender and a single receiver over a network.

uniform resource locator URL. A URL is the address of a document or other resource on the Internet.

uninterruptable power supply UPS. A buffer between public utility power or another power source, and a system that requires precise, uninterrupted power *(D)*.

universal port module UPM. A flexible 1 gigabit-per-second or 2 gigabit-per-second module that contains four generic ports (G_Ports).

UNIX A popular multi-user, multitasking operating system originally designed to be a small, flexible system used exclusively by programmers. UNIX was one of the first operating systems to be written in a high-level programming language, namely C. This meant that it could be installed on virtually any computer for which a C compiler existed. Due to its portability, flexibility, and power, UNIX

has become the leading operating system for workstations. Historically, it has been less popular in the personal computer market, but the emergence of a new version called Linux is revitalizing UNIX across all platforms.

upper level protocol ULP. Protocols that map to and run on top of the Fibre Channel FC-4 layer. ULPs include Internet protocol (IP) and small computer system interface (SCSI) *(D)*.

UPS *See* uninterruptable power supply.

URL *See* uniform resource locator.

user datagram protocol UDP. A connectionless protocol that runs on top of Internet protocol (IP) networks. User datagram protocol/Internet protocol (UDP/IP) offers very few error recovery services, instead providing a direct way to send and receive datagrams over an IP network. UDP/IP is primarily used for broadcasting messages over an entire network. *Contrast with* transmission control protocol/Internet protocol.

V

VAC *See* volts alternating current.

VDC *See* volts direct current.

virtual machine VM®. (1) A virtual data processing system that appears to be at the exclusive disposal of a single user, but whose functions are accomplished by sharing the resources of a real data processing system. (2) A functional simulation of a computer system and its associated devices, multiples of which can be controlled concurrently by one operating system *(D, T)*.

virtual storage VS. (1) Storage space that may be regarded as addressable main storage by the user of a computer system in which virtual addresses are mapped to real addresses. The size of virtual storage is limited by the addressing scheme of the computer system and by the amount of auxiliary storage available, not by the number of main storage locations. (2) Addressable space that is apparent to the user as processor storage space, from which the instructions and the data are mapped to the processor storage locations *(A, D, I)*.

vital product data VPD. System-level data stored by field-replaceable units (FRUs) in the electrically erasable programmable read-only memory. This data includes serial numbers and identifies the manufacturer.

VM® *See* virtual machine.

VM/ESA® Virtual machine/Enterprise Systems Architecture. *See* virtual machine.

volt A measure of the difference in electrical potential between two points in a conductor, equal to one ohm resistance carrying a constant current of one ampere, with a power dissipation of one watt *(D)*. *See* volts alternating current; volts direct current.

volts alternating current VAC. A term for classifying the system in which volts exist. VAC means that the volts exist in a circuit where the electricity can travel in either direction. *Contrast with* volts direct current. *See* volt.

volts direct current VDC. A term for classifying the system in which volts exist. VDC means that the electricity has a specific path it must follow. *Contrast with* volts alternating current. *See* volt.

VPD *See* vital product data.

VS *See* virtual storage.

W

WAN *See* wide area network.

warning message A message that indicates a possible error has been detected. *See also* error message; information message.

watt A unit of power in the International System equal to one joule (Newton-meter) per second *(D)*.

wide area network WAN. A network capable of transmission over large geographic areas that uses transmission lines provided by a common-carrier. *See also* local area network; metropolitan area network; metro-area storage area network (mSAN).

window The main window for the EFC Manager application or Product Manager applications. Each application has a unique window that is divided into separate panels for the title, navigation control, alerts, and the main or *Product View*. The user performs all management and monitoring functions for these Fibre Channel products through the application window.

Windows A graphical user interface and windowing system introduced by Microsoft Corporation in 1985. Windows runs on top of the MS-DOS operating system *(D)*.

workstation A terminal or microcomputer usually connected to a network or mainframe at which a user can perform applications.

world-wide names WWN. Eight-byte string that uniquely identifies a Fibre Channel entity (that is, a port, a node, a switch, a fabric), even on global networks.

wrap plug *Synonym for* loopback plug.

wrap test A test that checks attachment or control unit circuitry, without checking the mechanism itself, by returning the output of the mechanism as input. A wrap test can transmit a specific character pattern through a system and compare the pattern received with the pattern transmitted *(D)*.

write authorization Permission for an simple network management protocol (SNMP) management station with the proper community name to modify writable management information base (MIB) variables.

WWN *See* world-wide names.

Z

zip drive A high capacity floppy disk and disk drive developed by the Iomega Corporation. Zip disks are slightly larger than conventional floppy disks. The storage capacity for zip disks is between 100 and 250 MB of data. The zip drive and disk is used for backing up the EFC Server, and is located on the communications tray behind the EFC Server.

zone Set of devices that can access one another. All connected devices may be configured into one or more zones. Devices in the same zone can

see each other. Those devices that occupy different zones cannot. A *Fabric Zone* is created in fabric using tools supported by a fabric switch or director. A *Router Zone* is created in SAN Router using tools used to manage SAN Router. *See also* zone set; zoning.

Zone ID Every SAN router zone has a unique name and a unique ID. Zone IDs are used by the router to identify a zone whereas zone names are more for usability/readability for the user. Zone IDs come into play whenever a device needs to be shared between mSANs over an iFCP link.

zone member Specification of a device to be included in a zone. A zone member can be identified by the port number of the director or switch to which it is attached or by its port world-wide name (WWN). In multiswitch fabrics, identification of end-devices or nodes by WWN is preferable.

zone set A collection of zones that may be activated as a unit.

zoning Grouping of several devices by function or by location. All devices connected to a connectivity product, such as the director or switch, may be configured into one or more zones.

Index

F

G

H

I

L

M

N

O

P

R

S

T

V

Z