user guide

# hp StorageWorks iSCSI storage router 2122

Product Version: 1.0

Second Edition (January 2003)

Part Number: 304835-002

This user guide provides instructional information for installing and configuring the SR2122 iSCSI Storage Router.

invent

Hewlett-Packard Company makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Hewlett-Packard Company shall not be liable for technical or editorial errors or omissions contained herein. The information is provided “as is” without warranty of any kind and is subject to change without notice. The warranties for Hewlett-Packard Company products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty.

HP StorageWorks iSCSI Storage Router 2122 User Guide
Second Edition (January 2003)
Part Number: 304835-002

# contents

## About this Guide

## 1 Product Overview

## 2 Installation

## 5 Configuring the Storage Router

## 6 Configuring System Parameters

## 7 Configuring VLAN

## 8 Configuring SCSI Routing

## 9 Configuring Authentication

# about this guide

This user guide provides information to help you:

- Install the SR2122 iSCSI Storage Router
- Configure the SR2122 iSCSI Storage Router

About this Guide topics include:

- Conventions, page xii
- Rack Stability, page xiv
- Getting Help, page xiv

# Conventions

Conventions consist of the following:

- Document Conventions
- Text Symbols
- Equipment Symbols

## Document Conventions

The document conventions included in Table 1 apply in most cases.

**Table 1: Document Conventions**

| Element | Convention |
|---|---|
| Cross-reference links | Figure 1 |
| Key and field names, menu items, buttons, and dialog box titles | **Bold** |
| File names, application names, and text emphasis | Italics |
| User input, command and directory names, and system responses (output and messages) | `Monospace font`<br>`COMMAND NAMES` are uppercase monospace font unless they are case sensitive |
| Variables | *`<monospace, italic font>`* |
| Website addresses | Underlined sans serif font text: <br>http://www.hp.com |

## Text Symbols

The following symbols may be found in the text of this guide. They have the following meanings.

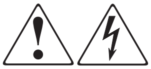
**WARNING:** Text set off in this manner indicates that failure to follow directions in the warning could result in bodily harm or loss of life.

**Caution:** Text set off in this manner indicates that failure to follow directions could result in damage to equipment or data.

**Note:** Text set off in this manner presents commentary, sidelights, or interesting points of information.

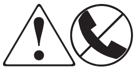
## Equipment Symbols

The following equipment symbols may be found on hardware for which this guide pertains. They have the following meanings.



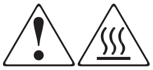
Any enclosed surface or area of the equipment marked with these symbols indicates the presence of electrical shock hazards. Enclosed area contains no operator serviceable parts.

**WARNING:** To reduce the risk of injury from electrical shock hazards, do not open this enclosure.



Any RJ-45 receptacle marked with these symbols indicates a network interface connection.

**WARNING:** To reduce the risk of electrical shock, fire, or damage to the equipment, do not plug telephone or telecommunications connectors into this receptacle.



Any surface or area of the equipment marked with these symbols indicates the presence of a hot surface or hot component. Contact with this surface could result in injury.

**WARNING:** To reduce the risk of injury from a hot component, allow the surface to cool before touching.

Power supplies or systems marked with these symbols indicate the presence of multiple sources of power.

**WARNING:** To reduce the risk of injury from electrical shock, remove all power cords to completely disconnect power from the power supplies and systems.

Any product or assembly marked with these symbols indicates that the component exceeds the recommended weight for one individual to handle safely.

**WARNING:** To reduce the risk of personal injury or damage to the equipment, observe local occupational health and safety requirements and guidelines for manually handling material.

## Rack Stability

Rack stability protects personal and equipment.

**WARNING:** To reduce the risk of personal injury or damage to the equipment, be sure that:

- The leveling jacks are extended to the floor.
- The full weight of the rack rests on the leveling jacks.
- In single rack installations, the stabilizing feet are attached to the rack.
- In multiple rack installations, the racks are coupled.
- Only one rack component is extended at any time. A rack may become unstable if more than one rack component is extended for any reason.

## Getting Help

If you still have a question after reading this guide, contact an HP authorized service provider or access our website: http://www.hp.com.

## HP Technical Support

In North America, call technical support at 1-800-652-6672, available 24 hours a day, 7 days a week.

**Note:** For continuous quality improvement, calls may be recorded or monitored.

Outside North America, call technical support at the nearest location. Telephone numbers for worldwide technical support are listed on the HP website under support: http://www.hp.com/support.

Be sure to have the following information available before calling:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Applicable error messages
- Operating system type and revision level
- Detailed, specific questions

## HP Storage Website

The HP website has the latest information on this product, as well as the latest drivers. Access storage at: http://www.hp.com. From this website, select the appropriate product or solution.

## HP Authorized Reseller

For the name of your nearest HP authorized reseller:

- In the United States, call 1-800-345-1518
- In Canada, call 1-800-263-5868
- Elsewhere, see the HP website for locations and telephone numbers: http://www.hp.com.

# Product Overview

# 1

This chapter is the starting point for installing the storage router hardware. It provides some very basic information you should know before proceeding to other chapters in this manual, and contains the following topics:

Installing and configuring a Storage Router consists of the following tasks:

- Installing the Storage Router
- Configuring the storage router software
- Installing and configure the iSCSI drivers

# Basic Description

The Storage Router is a 1U, rack-mountable router (see Figure 1) that provides IP hosts access to Fibre Channel storage through an IP network.

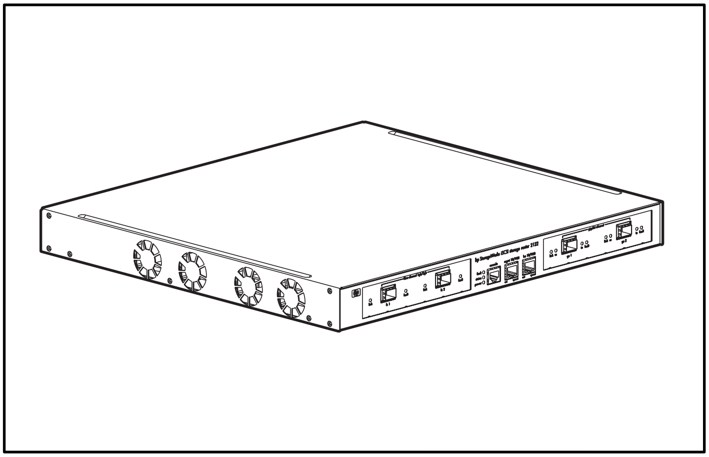


**Figure 1:  Storage router chassis**

The Storage Router provides access to Fibre Channel storage as if the IP hosts were directly attached to the storage (see Figure 2). For more information about the types of storage access available with the Storage Router, see Chapter 4, “Software Overview,” and other related documentation.

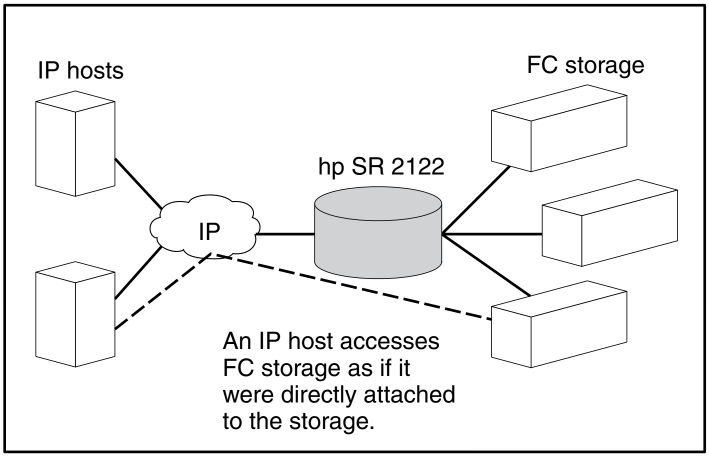


**Figure 2:  IP hosts accessing storage through the Storage Router**

## Port Descriptions

The Storage Router provides two 1-Gigabit Ethernet ports, a console port, a 10/100 Ethernet management port, a 10/100 Ethernet high availability (HA) port, and two 1-Gigabit/2-Gigabit Fibre Channel ports (see Figure 3).

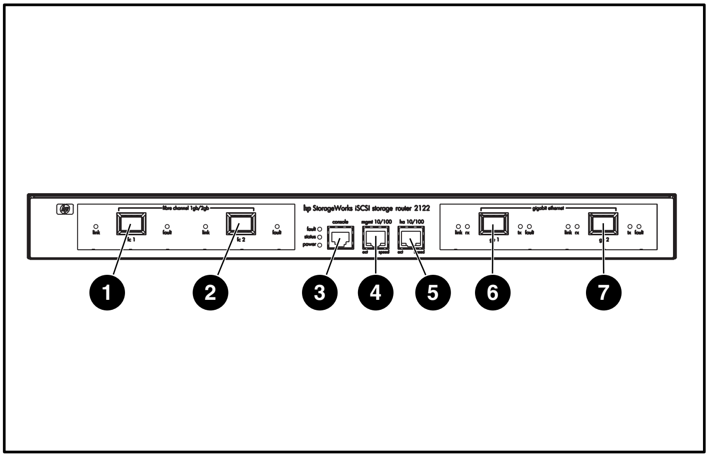


**Figure 3: Storage router ports**

❶ Fibre Channel 1G/2G, FC 1

❷ Fibre Channel 1G/2G, FC 2

❸ Console port, CONSOLE

❹ 10/100 Ethernet management port, MGMT 10/100

❺ 10/100 Ethernet high availability (HA) port, HA 10/100

❻ Gigabit Ethernet, GE 1

❼ Gigabit Ethernet, GE 2

The following sections describe the ports

- Gigabit Ethernet Ports, page 4
- Console Port, page 4
- 10/100 Ethernet Management Port, page 4
- 10/100 Ethernet HA Port, page 4
- Fibre Channel Ports, page 5

## Gigabit Ethernet Ports

The Gigabit Ethernet ports are labeled GE 1 and GE 2 (see Figure 3). Each port provides a 1-Gigabit Ethernet interface for connecting to IP hosts that require access to storage. Each port uses a small form-factor pluggable (SFP) module for connection to the port's physical medium. See Appendix B, "Cable and Port Pinouts," for SFP module specifications. Each Gigabit Ethernet port has LEDs indicating its status, as described in the "Front Panel LEDs" section on page 5.

## Console Port

The console port is labeled CONSOLE. (see Figure 3) It is an EIA/TIA-232 interface for connecting to the serial port of a PC running terminal emulation software. Using the console port, you can manage the Storage Router with the storage router command line interface (CLI). The console port uses an 8-pin RJ-45 receptacle; it has no LEDs.

## 10/100 Ethernet Management Port

The 10/100 Ethernet management port is labeled MGMT 10/100 (see Figure 3). It is a 10BaseT/100BaseT Ethernet interface for connecting to a management network. Through a management network, you can manage the Storage Router using the CLI, the web-based GUI, or SNMP. The 10/100 Ethernet management port uses an 8-pin RJ-45 receptacle and has LEDs indicating its status, as described in the "Front Panel LEDs" section on page 5.

## 10/100 Ethernet HA Port

The 10/100 Ethernet high-availability (HA) port is labeled HA 10/100 (see Figure 3). It is a 10BaseT/100BaseT Ethernet interface for connecting to an HA network. The port allows the Storage Router to function in a multiple-node cluster with other Storage Routers to provide fault-tolerant operation. The 10/100 Ethernet HA port uses an 8-pin RJ-45 receptacle and has LEDs indicating its status, as described in the "Front Panel LEDs" section on page 5.

### Fibre Channel Ports

The Fibre Channel ports are labeled FC 1 and FC 2 (see Figure 3). Each port provides a 1-Gigabit/2-Gigabit Fibre Channel interface for connecting to storage systems, Fibre Channel switches, Fibre Channel hosts, or other HP storage networking products. Each Fibre Channel port can be configured as one of the following port types: G_Port, GL_Port, F_Port, FL_Port, or TL_Port. Each port uses a small form-factor pluggable (SFP) module for connection to the port's physical medium. See Appendix B, "Cable and Port Pinouts," for SFP module specifications. Each Fibre Channel port has LEDs indicating its status, as described in the "Front Panel LEDs" section that follows.

## Front-Panel LEDs

The front-panel LEDs provide status indications about the storage router chassis and its ports (see Figure 4).

- Each Gigabit Ethernet port, GE 1 and GE 2, has four LEDs, labeled LINK, RX, TX, and FAULT. The LEDs are located to the left and right of each Gigabit Ethernet port.
- The FAULT, STATUS, and POWER LEDs indicate the overall status of the Storage Router. The LEDs are located to the left of the CONSOLE port.
- The 10/100 Ethernet management port, MGMT 10/100, has two LEDs, labeled ACT and SPEED. The ACT LED is located at the left-bottom corner of the port; the SPEED LED is located at the right-bottom corner of the port.
- The 10/100 Ethernet HA port, HA 10/100, has two LEDs, labeled ACT and SPEED. The ACT LED is located at the left-bottom corner of the port; the SPEED LED is located at the right-bottom corner of the port.
- Each Fibre Channel port has two LEDs, labeled LINK and FAULT. The LEDs are located to the left and right of each Fibre Channel port.

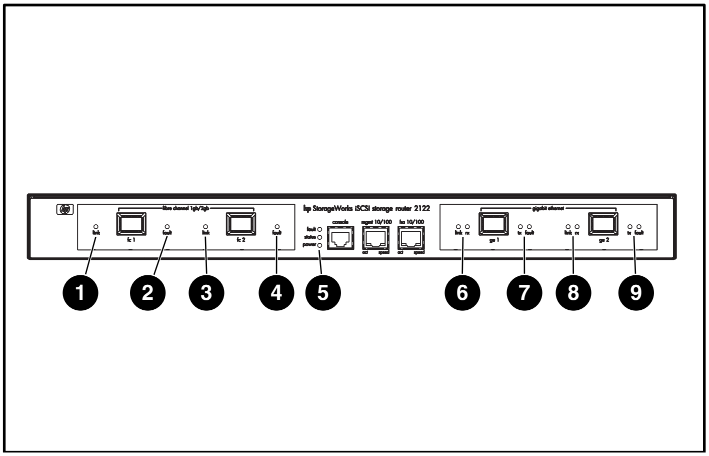


**Figure 4: Front panel LEDs**

❶ FC 1 LINK

❷ FC 1 FAULT

❸ FC 2 LINK

❹ FC 2 FAULT

❺ FAULT, STATUS, POWER

❻ GE 1 LINK and RX

❼ GE 1 TX and FAULT

❽ GE 2 LINK AND RX

❾ GE 2 TX and FAULT

**Table 2: Front panel LED descriptions**

| LED | | Color | Description |
|---|---|---|---|
| GE 1 and GE 2 LEDs | LINK | Green | Port is operational |
| | TX | Green | Packets are being transmitted |
| | RX | Green | Packets are being received |
| FAULT | | Red | On — Error in Storage Router |
| | | | Flashing — Error in a storage router component |
| Status | | Green | On — Successful boot up |
| | | | Flashing — Booting up |
| POWER | | Green | Power is on |
| MGMT 10/100 LEDs | ACT | Green | Link is active |
| | SPEED | Yellow | Port speed is 100Mbps |

| LED | | Color | Description |
|---|---|---|---|
| HA 10/100 LEDs | ACT | Green | Link is active |
| | SPEED | Yellow | Port speed is 100Mbps |
| FC 1 and FC 2 LEDs | ACT | Yellow | Frames are being transmitted or received |
| | LOG | Green | On — Port is properly connected |
| | | | Flashing once per second — Port is logging in |
| | | | Flashing twice per second — Port connection error |

## Fan Assembly

The fan assembly provides cooling for the internal chassis components. The storage router chassis contains four exhaust fans that are located on the left side of the chassis. The fans draw in air from the right side and exhaust air through the left side (see Figure 5).

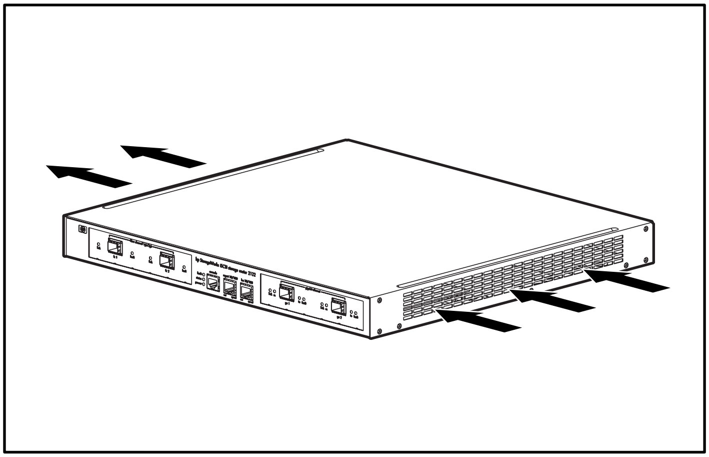


**Figure 5: Chassis Airflow**

## Power Supply

The Storage Router has an internal power supply that monitors its temperature and output voltages. The power supply automatically senses and adjusts to either of these input voltages: 115 VAC/60 Hz or 230 VAC/50 Hz.

If conditions reach critical thresholds, the power supply shuts down to avoid damage from excessive heat or electrical current. The power supply connects to site power through a power cord and the power connector on the rear panel (see Figure 6). The power supply is powered on with a rocker switch next to the power connector. The switch is labeled **I** and **O**. Pressing **I** switches power on. Pressing **O** switches power off.

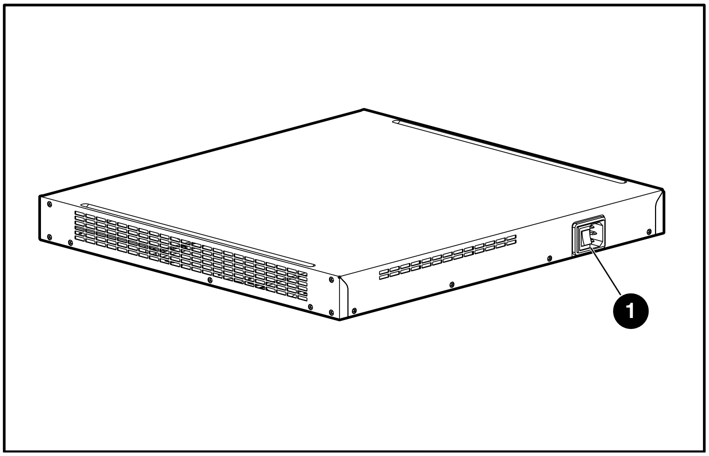


**Figure 6: Rear panel, power connector**

❶ Power Connector

# Installation

2

This chapter describes how to prepare your site for installation, how to prepare and install the Storage Router, how to connect network and Fibre Channel cables, how to connect power, and how to verify correct installation. For first-time installations, perform the procedures in the following sections in the order listed here:

## Site Planning

Planning the proper location and layout of your Storage Router, your equipment rack, or wiring closet is essential for successful Storage Router operation. Equipment placed too close together or in a poorly ventilated area can cause the system to overheat. In addition, poor equipment placement can make system panels inaccessible and difficult to maintain.

To ensure normal operation and to avoid unnecessary maintenance, plan your site configuration and prepare your site before installation.

Table 19 in Appendix A lists the operating and nonoperating environmental site requirements for the Storage Router. Within specified environmental ranges, the system can continue to operate; however, a measurement that approaches the minimum or maximum of a range indicates a potential problem. You can maintain normal operation by anticipating and correcting environmental conditions before they exceed the maximum operating range.

Verify the site power for the type of device you are installing. Power requirements are useful for planning the power distribution system needed to support the Storage Router. Heat dissipation is an important consideration for sizing the air-conditioning requirements for an installation. See Table 19 in Appendix A for power and heat ratings for the Storage Router.

△ **Caution:** To prevent a loss of input power, verify that the total maximum load on the circuit supplying power to the power supply is within the current ratings of the wiring and breakers.

## Installing the Storage Router

You can install the Storage Router on a table or a shelf, or in an equipment rack. The following sections describe the steps required to install the Storage Router:

- Installing on a Table or a Shelf, page 11
- Rack-Mounting the Storage Router, page 11
- Installing SFP Modules, page 15

## Installing on a Table or a Shelf

You can install the Storage Router on a table or a shelf (or another flat, secure surface).

If you are going to install the Storage Router in an equipment rack, skip this section and proceed to the “Rack-mounting the Storage Router” section. To install the chassis on a table or a shelf, follow these steps:

1. Locate the four adhesive-backed rubber feet. They are in the accessory kit that is shipped with the Storage Router.
2. Peel the rubber feet from their backing and place the feet, adhesive-side down, onto the four round recessed areas on the bottom of the chassis.
3. Place the Storage Router on a table or a shelf near an AC power source.

## Rack-Mounting the Storage Router

You can rack-mount the Storage Router in a 19-inch equipment rack with the front panel forward.

The accessory kit shipped with your Storage Router contains two rails, two wing nuts, and various screws.

You need the following tools to install the Storage Router in a rack:

- Phillips screwdriver
- Tape measure

To install the Storage Router in a rack, follow these steps:

1. Prepare for installation:
    a. Place the Storage Router on the floor or on a sturdy table as close as possible to the rack. Leave enough clearance so that you can move around the Storage Router.
    b. Use a tape measure to measure the depth of the rack. Measure from the outside of the front mounting posts to the outside of the rear mounting strip. The depth must be at least 19 inches (48.26 cm) but not more than 32 inches (81.3 cm).
    c. Measure the space between the inner edges of the left-front and right-front mounting posts to ensure that the space is 17.75 inches (45.72 cm) wide.

2. Use the Rack Template provided to mark the center of a 1U mounting location on both sides of the front and rear mounting rails.
3. Install cage nuts in the locations marked in step 2 (see Figure 7).

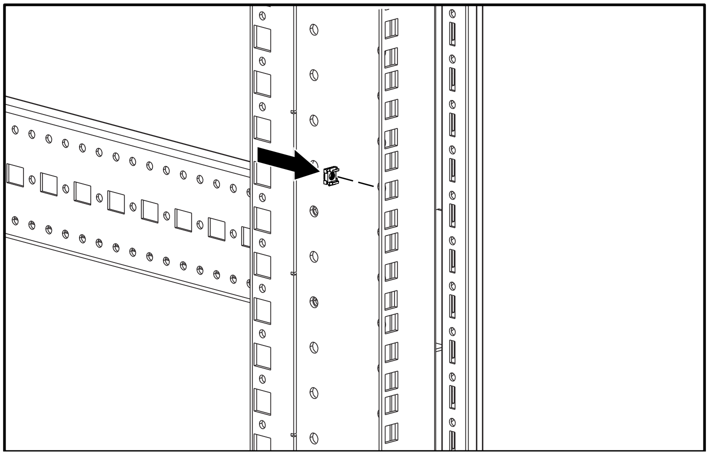


**Figure 7: Installing cage nuts**

4. Assemble the rails using the supplied wing nuts (see Figure 8).

**Note:** Do not tighten the wing nuts completely because the rails will need to be adjusted later in the installation process.

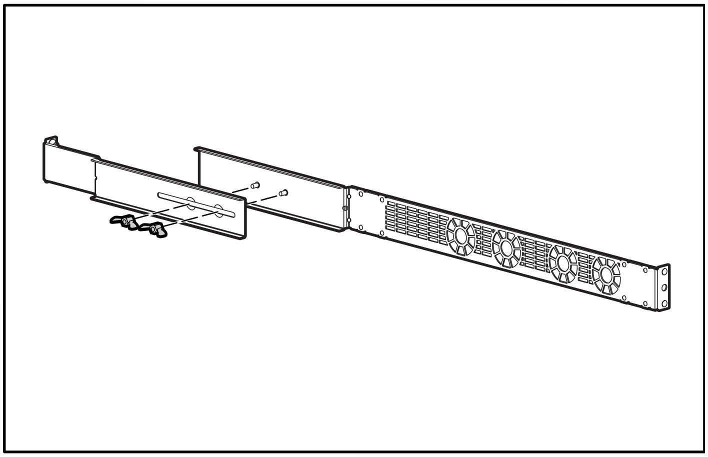


**Figure 8: Rail assembly**

5. Remove all existing screws (6 total) from each side of the chassis (see Figure 9).

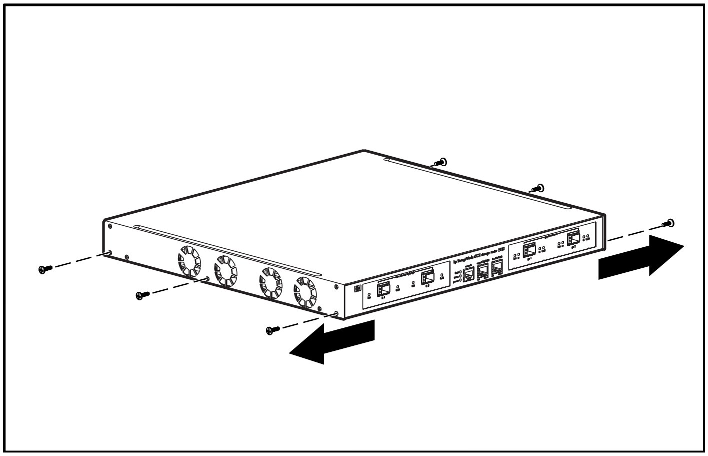


Figure 9: Removing the screws

6. Align and attach the rails to the chassis using the supplied flat-head screws (see Figure 10).

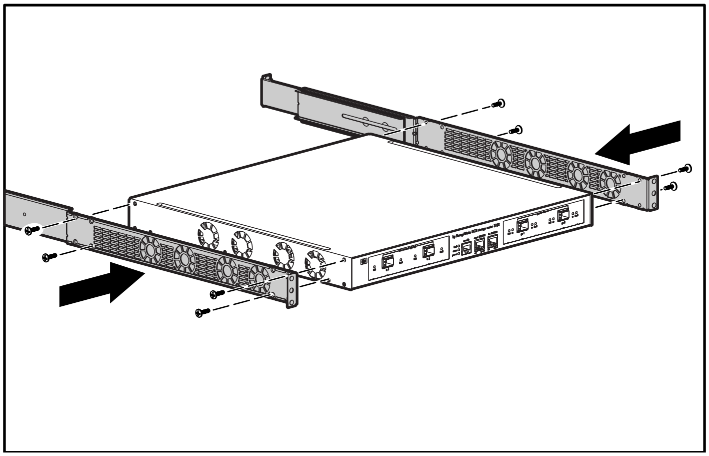


Figure 10: Attaching the rails

7. Slide the Storage Router into the rack and secure the front of the rails using the rack screws (see Figure 11).

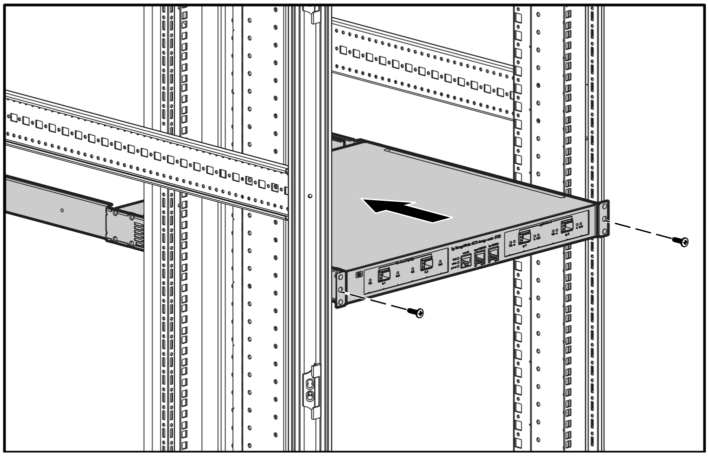


Figure 11:  Installing the Storage Router into the rack

8. Adjust ❶ and secure the rear of the rails using the rack screws ❷ (see Figure 12).
9. Secure ❸ the rail halves by tightening the wing nuts.

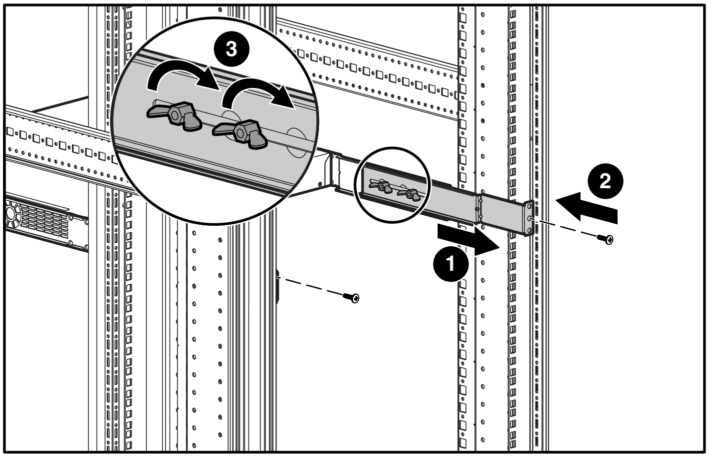


Figure 12:  Securing the rear of the rails

## Installing SFP Modules

Before you install or remove an SFP (small form-factor pluggable) module, read the installation information in this section. For connecting to SFP modules in the Gigabit Ethernet ports and the Fibre Channel ports, read the instructions in the "Connecting Gigabit Ethernet and Fibre Channel Ports."

**Note:** Because of interoperability issues, HP does not support SFPs purchased from third-party vendors. See Appendix B, "Cable and Port Pinouts," for SFP port specifications.

**Note:** When fiber-optic cable plugs and SFP module receptacles are disconnected from each other, place dust covers on them.

**WARNING:** Because invisible radiation may be emitted from the aperture of the port when no fiber cable is connected, avoid exposure to radiation and do not stare into open apertures. To see translated versions of the warning, refer to the Regulatory Compliance and Safety document that accompanied the device.

The Gigabit Ethernet ports use fiber-optic SFP modules with either MT-RJ connectors (see Figure 13) or LC connectors (see Figure 14). The Fibre Channel ports use fiber-optic SFP modules with LC connectors (see Figure 14). See Table 3 to determine what types of SFP modules you can install in the Gigabit Ethernet and Fibre Channel ports. See Appendix B, "Cable and Port Pinouts," for SFP module specifications.

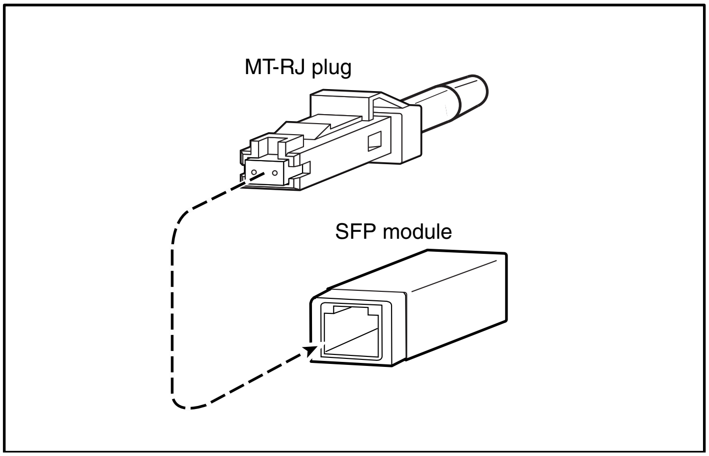


Figure 13: MT-RJ fiber-optic connector and SFP module

**Caution:** Protect your fiber-optic SFP modules by inserting clean dust covers into the SFPs after the cables are extracted from them. Be sure to clean the optic surfaces of the fiber cables before you plug them back into the optical bores of another SFP module. Avoid getting dust and other contaminants into the optical bores of your SFP modules; the optics will not work correctly when obstructed with dust.

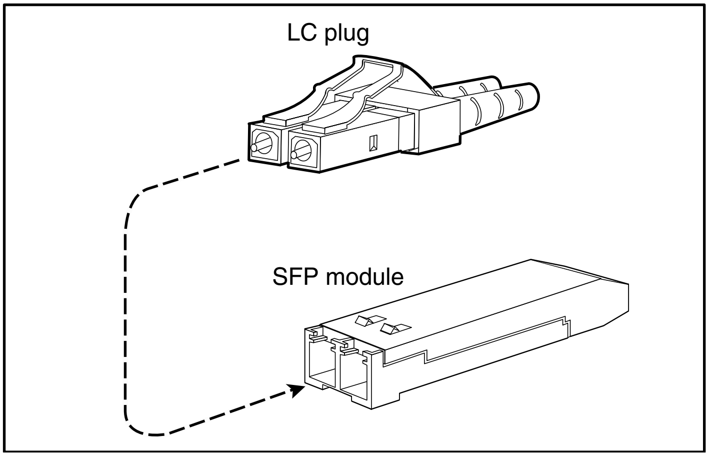


Figure 14: LC connector and fiber-optic SFP module

Table 3: Types of SFP Modules for Gigabit Ethernet and Fibre Channel Ports

| SFP Option Kit Part Number | Connector Type | Port |
|---|---|---|
| 221470-B21 | LC | Gigabit Ethernet or Fibre Channel |

The SFP modules have three different types of latching devices used to secure and detach the SFP module from a port. The three types of SFP modules are described in the following sections:

- Mylar Tab SFP Modules, page 18
- Actuator/Button SFP Modules, page 20
- Bale Clasp SFP Modules, page 22

## Mylar Tab SFP Modules

The Mylar tab SFP module (see Figure 15) has a tab that must be pulled to remove the module from a port.

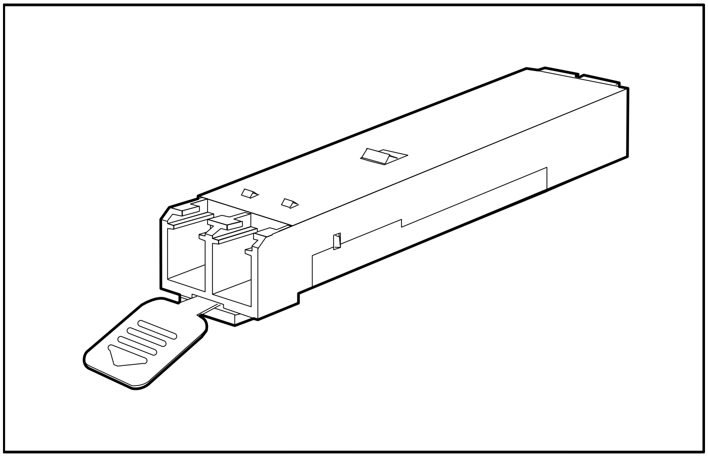


**Figure 15: Mylar tab SFP module**

To insert the Mylar tab SFP module into a port, line up the SFP module with the port, and slide it into place (see Figure 16).

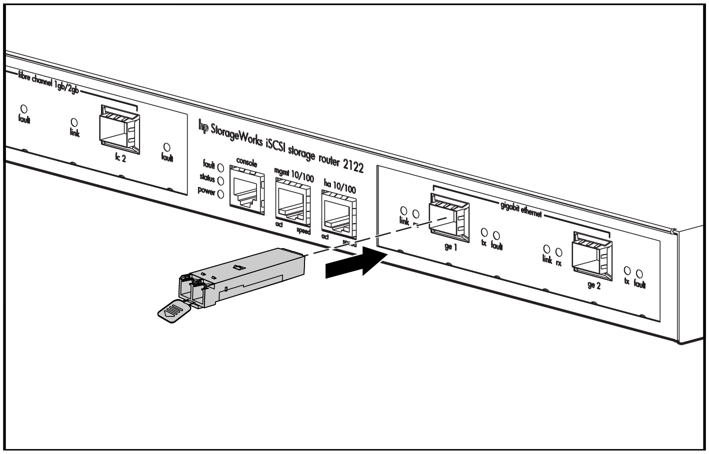


**Figure 16: Inserting a Mylar tab SFP module**

**Caution:** When pulling the tab to remove the SFP module, be sure to pull in a straight outward motion so you remove the SFP module from the port in a parallel direction. Do not twist or pull the tab, you may disconnect it from the SFP module.

To remove the SFP module from the port, pull the tab gently in a slightly downward direction until it disengages from the port and then pull the SFP module out (see Figure 17).

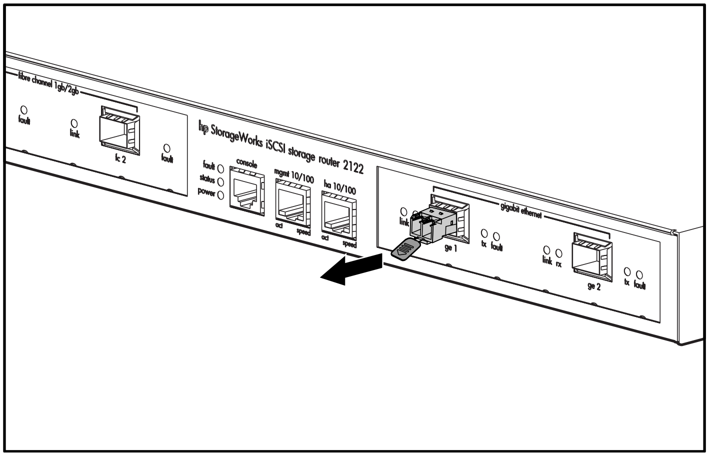


**Figure 17: Removing a Mylar tab SFP module**

## Actuator/Button SFP Modules

The actuator/button SFP module (see Figure 18) has a button that must be pushed to remove the SFP module from a port.

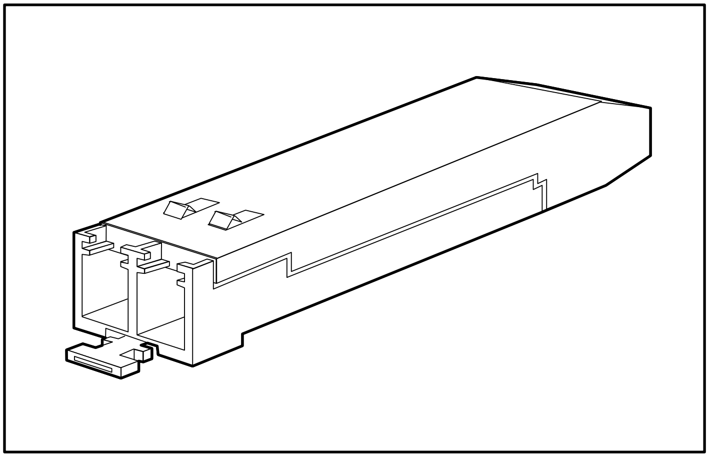


Figure 18: Actuator/button SFP module

To insert the actuator/button SFP module into a port, line up the SFP module with the port and slide it in until the actuator/button clicks into place (see Figure 19). Be sure not to press the actuator/button as you insert the SFP module, you might inadvertently disengage the SFP module from the port.

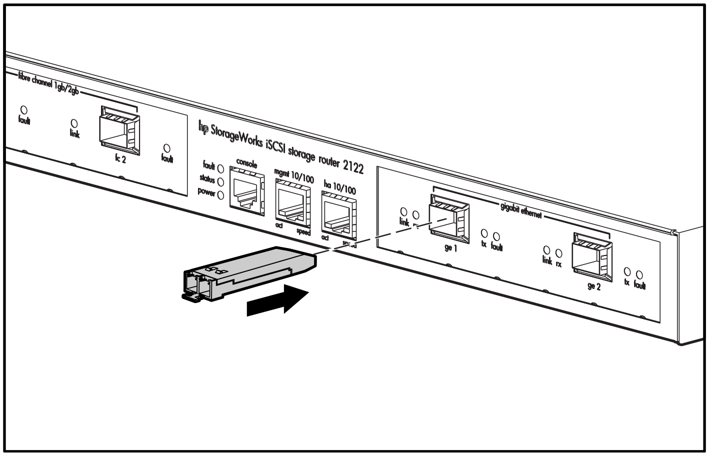


Figure 19: Inserting an actuator/button SFP module

To remove an actuator/button SFP module from a port, perform the following steps:

1. Gently press the actuator/button ❶ on the front of the SFP module until it clicks and the latch mechanism activates, releasing the SFP module from the port (see Figure 20).
2. Grasp the actuator/button between your thumb and index finger and carefully pull the SFP module ❷ from the port (see Figure 20).

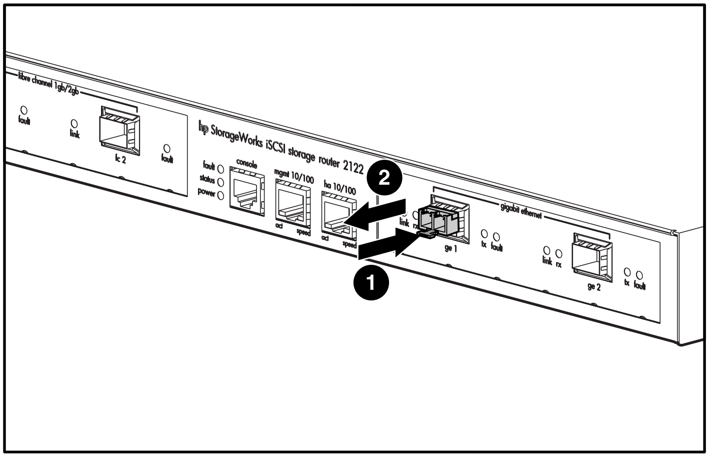


Figure 20: Removing an actuator/button SFP module from a port

## Bale Clasp SFP Modules

The bale clasp SFP module (see Figure 21) has a bale clasp used to secure the SFP module in a port.

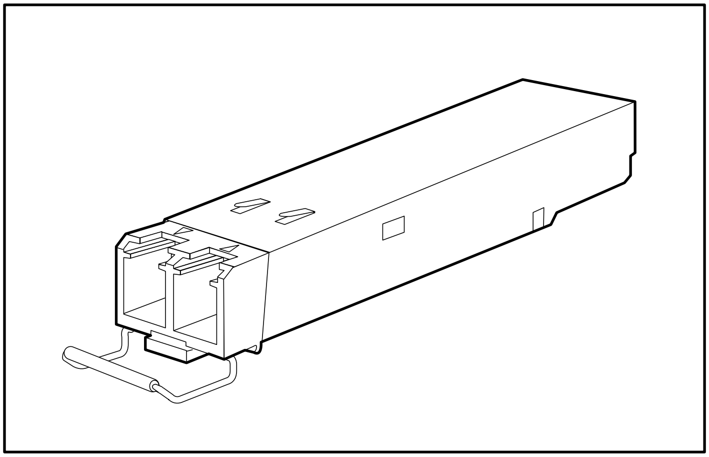


**Figure 21: Bale clasp SFP module**

To insert a bale clasp SFP module into a port:

1. Close the bale clasp before inserting the SFP module.
2. Line up the SFP module with the port and slide it into the port (see Figure 22).

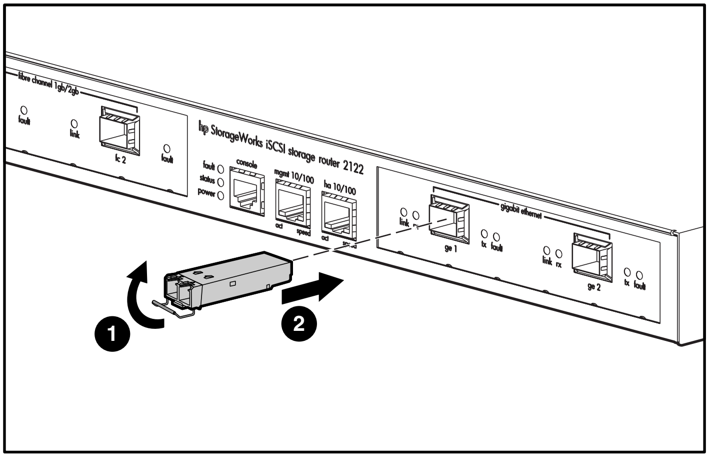


**Figure 22: Inserting a bale clasp SFP module into a port**

To remove a bale clasp SFP module from a port:

1. Open the bale clasp on the SFP module with your index finger in a downward direction, as shown in Figure 23. If the bale clasp is obstructed and you cannot use your index finger to open it, use a small, flat-blade screwdriver or other long, narrow instrument to open the bale clasp as shown in Figure 24.
2. Grasp the SFP module between your thumb and index finger and carefully remove it from the port as shown in Figure 23.

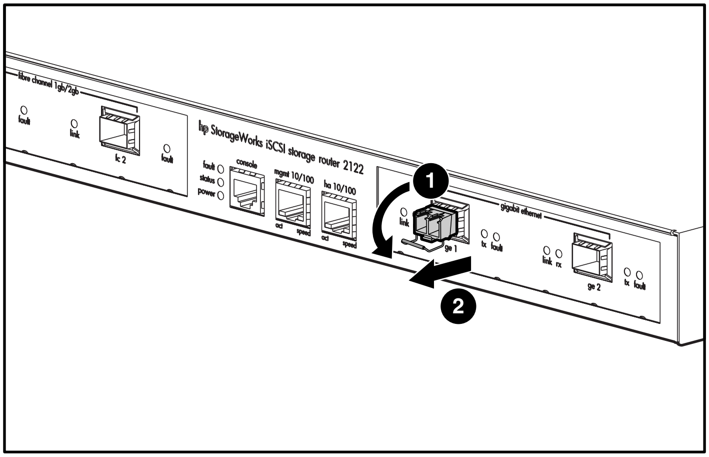


Figure 23: Removing a bale clasp SFP module with your index finger

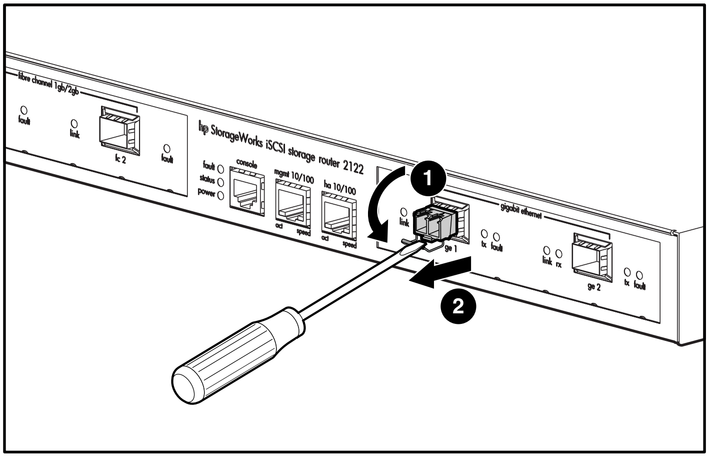


Figure 24: Removing a bale clasp SFP module with a flat-blade screwdriver

# Connecting to Gigabit Ethernet and Fibre Channel Ports

The Gigabit Ethernet ports, GE 1 and GE 2, use MT-RJ-type or LC-type fiber-optic SFP modules and cables. The Fibre Channel ports, FC 1 and FC 2, use LC-type fiber-optic SFP modules and cables. When you are connecting a cable to a fiber-optic SFP module, make sure that you firmly press the cable plug into the socket. The upper edge of the plug must snap into the upper front edge of the socket. You should hear the plug click when it is locked into the socket. To make sure that the plug is locked into the socket, gently pull on it.

To disconnect a plug from a socket, press the trigger on top of the plug, releasing the latch. You should hear a click, which indicates that the latch has released. Carefully pull the plug out of the socket.

**Note:** When you disconnect the fiber-optic cable from the module, grip the body of the connector. Do not grip the connector jacket-sleeve. Gripping the sleeve can, over time, compromise the integrity of the fiber-optic cable termination in the connector.

Dirt or skin oils may have accumulated on an MT-RJ plug faceplate (around the optical-fiber openings), which can generate significant attenuation and reduce the optical power levels below threshold levels so that a link cannot be made. To clean an MT-RJ plug faceplate, follow this procedure:

1. Using a lint-free tissue soaked in 99 percent pure isopropyl alcohol, gently wipe the faceplate.
2. Remove any residual dust from the faceplate with compressed air before installing the cable.

**Note:** When fiber-optic cable plugs and SFP module receptacles are disconnected from each other, place dust covers on them.

The following sections describe how to connect cables to the Gigabit Ethernet and Fibre Channel ports:

- Connecting to a Gigabit Ethernet Port, page 25
- Connecting to a Fibre Channel Port, page 25

## Connecting to a Gigabit Ethernet Port

To connect a cable to a Gigabit Ethernet port:

1. Remove the dust cover from the SFP module in the Gigabit Ethernet port; store the dust cover for future use.
2. Remove the dust cover (or covers) from the plug on the cable; store the cover (or covers) for future use. Insert the cable plug into the Gigabit Ethernet SFP module.
3. Connect the other end of the cable to the external end system, switch, or router.

## Connecting to a Fibre Channel Port

To connect a cable to a Fibre Channel port:

1. Remove the dust cover from the SFP module in the Fibre Channel SFP port; store the dust cover for future use.
2. Remove the dust covers from the cable plug on the fiber-optic cable; store the dust covers for future use. Insert the cable plug into the Fibre Channel SFP module.
3. Connect the other end of the cable to a Fibre Channel port of another system (for example, a storage system, switch, host, or another Storage Router).

## Connecting to the 10/100 Ethernet Management and HA Ports

To connect to the 10/100 management and HA ports:

1. Use modular, RJ-45, straight-through UTP cables to connect the 10/100 management and HA ports to end systems. Use modular, RJ-45 cross-connect cables to connect to external switches and routers.
2. Connect the appropriate modular cables to the 10/100 management and HA ports (see Figure 25).

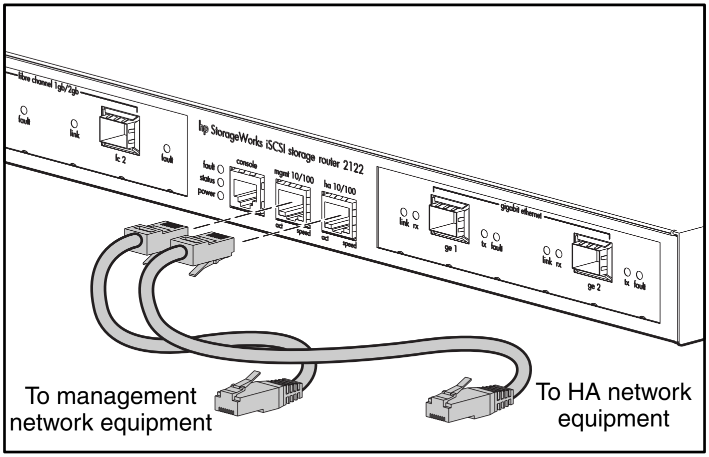


**Figure 25: Connecting to the 10/100 management and HA ports**

3. Connect the other end of the cable to the external end system, switch, or router.

## Connecting to the Console Port

Connect a PC serial port to the console port for local administrative access to the Storage Router. The PC must support VT100 terminal emulation. The terminal-emulation software — frequently a PC application such as HyperTerminal or Procomm Plus — makes communication between the Storage Router and your PC possible during setup and configuration.

To connect to the console port:

1. Configure the PC terminal emulation program to match these console port default characteristics:

**Table 4: Console port default characteristics**

| Console Port Default Characteristics | |
|---|---|
| Bits Per Second | 9600 |
| Data Bits | 8 |
| Parity | None |
| Stop Bits | 1 |
| Flow Control | None |

2. Connect the supplied RJ-45-to-DB-9 female adapter to the PC serial port.
3. Connect one end of the supplied console cable (a rollover RJ-45-to-RJ-45 cable) to the console port. Connect the other end to the RJ-45-to-DB-9 adapter at the PC serial port (see Figure 26).

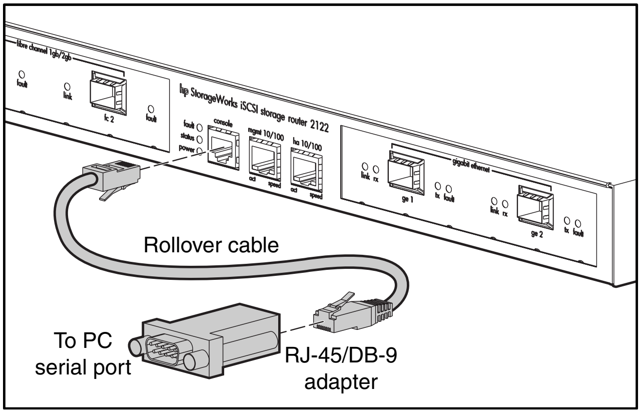


**Figure 26: Connecting the console cable**

# Connecting Power

The Storage Router can be connected to either of two power sources: 115-120 VAC/60 Hz or 230-240 VAC/50 Hz. The power supply automatically senses the source and adjusts to either source.

To connect power to the Storage Router:

1. Make sure the power switch is set to Off (see Figure 27).

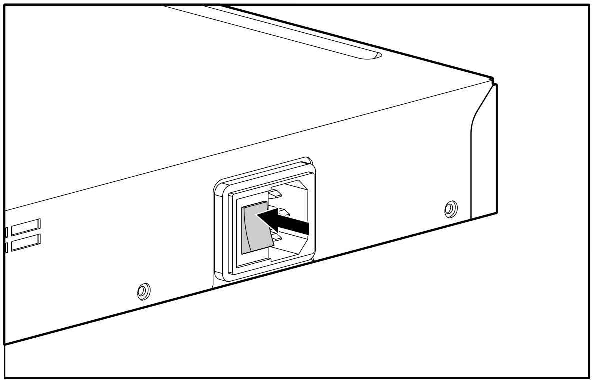


Figure 27: Power set to Off

2. Plug the power cord into the power receptacle located on the rear panel in the chassis (see Figure 28).

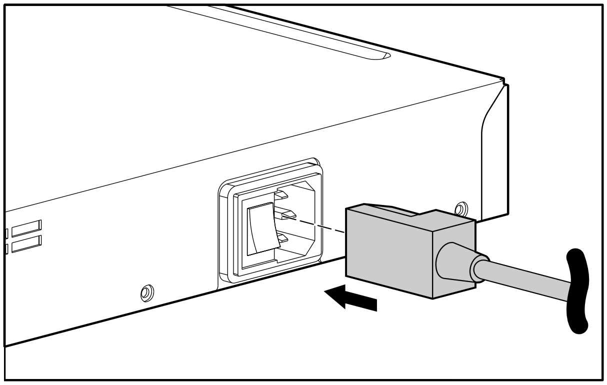


Figure 28: Connecting a power cord to the power connector

3. Connect the other end of the power cord to the power source for the Storage Router.

# Verifying Installation

Verifying installation of the Storage Router consists of making sure that it starts properly and that the network and Fibre Channel connections are operational.

## Verifying Startup Operations

To verify that the Storage Router starts up properly:

1. At the rear of the Storage Router, press the power switch to the on position.
2. At the front of the Storage Router, observe the POWER LED to make sure power is on. Make sure that the FAULT LED is off.
3. Listen and check for air flow to make sure the fan assembly is operating.
4. Observe console output to make sure that the storage router software is booting properly. The boot process may last for three to five minutes and will display boot information and a banner. A successful boot up is indicated by a CLI prompt for user input.
5. If any of these conditions are not met, refer to Chapter 3, “Troubleshooting,” to isolate and, if possible, resolve the problem.

## Verify that Network Connections are Operational

Verifying the network connections consists of making sure that the following ports are operational: Gigabit Ethernet, 10/100 Ethernet management, and 10/100 HA.

To verify that the network connections are operational, perform the following steps:

1. Verify the Gigabit Ethernet port connections by checking the port link status LED. See Table 2 in Chapter 1 page 6 for LED indication descriptions.
2. Verify the 10/100 Ethernet management port connection by checking the port link status LED. See Table 2 in Chapter 1 for LED indication descriptions.
3. Verify the 10/100 HA port connection by checking the port link status LED. See Table 2 in Chapter 1 for LED indication descriptions.
4. If any of these conditions are not met, see Chapter 3, “Troubleshooting,” to isolate and resolve the problem if possible.

## Verify That Fibre Channel Connections are Operational

To verify that the connections are operational, perform the following steps:

1. Verify Fibre Channel port connections by checking Fibre Channel LOG LEDs. See Table 2 in Chapter 1 for LED indication descriptions.
2. If the LOG LEDs for connected ports are flashing, see Chapter 3, “Troubleshooting,” to isolate and, if possible, resolve the problem.

## Where to Go Next

Once you have verified that the storage router hardware is properly installed, it is ready for software configuration. To configure the software, refer to Chapter 4, “Software Overview.”

3

# Troubleshooting

This chapter provides troubleshooting procedures for problems encountered during installation and consists of the following sections:

## Solving Problems at the Component Level

The key to troubleshooting the Storage Router is to isolate the problem on a specific Storage Router component. The first step is comparing what the Storage Router is doing to what it should be doing. Because a startup problem is usually attributed to a single component, it is more efficient to isolate the problem to a subsystem rather than troubleshoot each separate component in the Storage Router.

The Storage Router consists of the following subsystems:

- The power supply operates whenever system power is on (see "Troubleshooting the Power Supply" on page 34).
- The chassis fan assembly operates when the system power is on. The fan may continue to operate even when the power supply shuts down the Storage Router because of an over temperature or over voltage condition (although it does shut down for a power supply shutdown).

  The following are simple checks you can make to determine if there is a fan problem:

  — Listen to the fan assembly to determine if it is operating.

  — Check for any obstructions restricting airflow through the Storage Router.

  If you determine that the fan assembly is not operating properly, contact a customer service representative.

# Identifying Startup Problems

Observe the operation of the Storage Router and its front-panel LEDs to determine startup problems. LEDs indicate Storage Router status in the startup sequence. By checking the LEDs, you can determine when and where the Storage Router failed in the startup sequence.

To power up the Storage Router:

1. Listen for the chassis fan assembly operation. If it does not operate, see “Troubleshooting the Power Supply” on page 34. If you determine that the power supply is functioning normally and that the fan assembly is faulty, contact a customer service representative. If the fan assembly does not function properly at initial startup (there are no installation adjustments that you can make), contact a customer service representative.
2. Check the POWER LED on the front panel. The POWER LED turns on immediately when power is on. The LED remains on during normal Storage Router operation. If the LED is not on, see “Troubleshooting the Power Supply” on page 34.
3. Check the STATUS and FAULT LEDs on the front panel. See “Front-Panel LEDs” in Chapter 1 for LED descriptions.
4. Check the network and Fibre Channel port LEDs on the front panel. See the “Front-Panel LEDs” in Chapter 1 for LED descriptions. If a network or Fibre Channel port LED indicates a problem with the port connection, see “Troubleshooting a Network or Fibre Channel Port Connection” on page 35.
5. Verify that the PC terminal emulation program is set correctly and that the PC is connected properly to the console port. Also, verify at the PC terminal emulation program display that the Storage Router has started up properly (for example, a prompt for starting a configuration wizard or a CLI prompt).
6. Contact a customer service representative for instructions if a status LED indicates a failure or if the PC connected to the console port indicates an incomplete boot-up process.

## Troubleshooting the Power Supply

To help isolate a power problem, follow these steps:

1. Check the POWER LED.
   - If the POWER LED is off, unplug the power cord and then plug the power cord back in.
   - If the POWER LED remains off, check the AC source or the power cable for problems.
2. Connect the power cord to another power source if one is available.
   - If the POWER LED comes on, the problem is the first power source.
   - If the POWER LED is off after you connect the power supply to a new power source, replace the power cord.
   - If the POWER LED still fails to light when the Storage Router is connected to a different power source with a new power cord, the power supply is probably faulty.
3. If you are unable to resolve the problem, contact a customer service representative for instructions.

# Troubleshooting a Network or Fibre Channel Port Connection

If an LED on a network or Fibre Channel port indicates a problem, follow the steps in the next sections to help isolate the problem:

- Troubleshooting a Connection to a Gigabit Ethernet Port, page 35
- Troubleshooting a Connection to a 10/100 Ethernet Management or 10/100 Ethernet HA Port, page 36
- Troubleshooting a Connection to a Fibre Channel Port, page 37

## Troubleshooting a Connection to a Gigabit Ethernet Port

A bad connection to a Gigabit Ethernet (GE 1 or GE 2) port is indicated by the LINK LED not being on. If the LINK LED is not on, follow these steps to help isolate the problem:

1. Verify that the cable is connected properly and is in good operating condition.
   - Disconnect and connect both ends of the cable. If the LINK LED turns on, then the cable was not connected properly.
   - If the LINK LED remains off, replace the cable. If the LINK LED turns on, then the cable was defective.
   - If the LINK LED remains off, the cable is most likely not the problem. Continue to the next step.
2. Check the external end system, switch, or router to which the port is connected.
   - If the external end system, switch, or router is operating properly, continue to the next step.
   - If the external end system, switch, or router is not operating properly, then correct the problem. If the LINK LED turns on, then the problem was with the external end system, switch, or router.
   - If the LINK LED remains off, continue to the next step.
3. Replace the SFP module.
   - If the LINK LED turns on, the problem was the SFP module.
   - If the LINK LED remains off, contact a customer service representative for instructions.

## Troubleshooting a Connection to a 10/100 Ethernet Management or 10/100 Ethernet HA Port

A bad connection to the 10/100 Ethernet Management or the 10/100 Ethernet HA port (MGMT 10/100 or HA 10/100) is indicated by the ACT LED not being on. If the ACT LED is not on, follow these steps to help isolate the problem:

1. Verify that the cable is connected properly and is in good operating condition.
   - Verify that the cable is the correct type of cable. (See Appendix B, “Cable and Port Pinouts.”)
   - Disconnect and connect both ends of the cable. If the ACT LED turns on, then the cable was not connected properly.
   - If the ACT LED remains off, replace the cable. If the ACT LED turns on, then the cable was defective.
   - If the ACT LED remains off, the cable is most likely not the problem. Continue to the next step.
2. Check the external end system, switch, or router to which the port is connected.
   - If the external end system, switch, or router is operating properly, continue to the next step.
   - If the external end system, switch, or router is not operating properly, then correct the problem. If the ACT LED turns on, then the problem was with the external end system, switch, or router.
   - If the ACT LED remains off, contact a customer service representative for instructions.

## Troubleshooting a Connection to a Fibre Channel Port

A bad connection to a Fibre Channel port (FC 1 and FC 2) is indicated by the LOG LED flashing twice per second. If the LOG LED is flashing twice per second, follow these steps to help isolate the problem:

1. Make sure that the Domain ID of the Storage Router is configured properly. If the Domain ID is configured properly, continue to the next step.

   **Note:** When a connection problem is resolved, the LOG LED will turn on after a brief logging-in period that is indicated by the LOG LED flashing once per second.

2. Verify that the cable is connected properly and is in good operating condition.
   - Disconnect and connect both ends of the cable. If the LOG LED turns on, then the cable was not connected properly.
   - If the LOG LED remains off, replace the cable. If the LOG LED turns on, then the cable was defective.
   - If the LOG LED remains off, the cable is most likely not the problem. Continue to the next step.
3. Check the device or switch to which the port is connected.
   - If the device or switch is operating properly, continue to the next step.
   - If the device or switch is not operating properly, then correct the problem. If the LOG LED turns on, then the problem was with the device or switch.
   - If the LOG LED remains off, continue to the next step.
4. Replace the SFP module.
   - If the LOG LED turns on, the problem was the SFP module.
   - If the LOG LED remains off, contact a customer service representative for instructions.

## Contacting Customer Service

If you are unable to solve a startup problem after using the troubleshooting suggestions in this chapter, contact a customer service representative for assistance and further instructions. Before you call, have the following information ready to help your service representative assist you as quickly as possible:

- Date you received the Storage Router
- Chassis serial number (located on the upper-right label on the rear panel of the chassis)
- Type of software and release number
- Maintenance agreement or warranty information
- Brief description of the problem
- Brief explanation of the steps you have taken to isolate and resolve the problem

# Software Overview

4

The Storage Router installation and configuration tasks consist of the following:

- Install the Storage Router according to Chapter 2, “Installation,” or the *hp StorageWorks iSCSI storage router 2122 Installation Card*.
- Configure the storage router software according to the guidelines in this guide.
- Install and configure iSCSI drivers in IP hosts connected to the Storage Router. The iSCSI driver is not required in IP hosts that have a TCP/IP Offload Engine (TOE) with embedded iSCSI protocol installed.

This chapter is the starting point for storage router software configuration. It provides some very basic, abbreviated information to help you understand Storage Router features and the software configuration process. It contains the following topics:

# Storage Router Software Overview

The Storage Router provides universal access to storage over IP networks. Storage router software controls the operation of the Storage Router. The software is configured to provide access to storage over IP networks using SCSI routing.

SCSI routing provides IP hosts with access to Fibre Channel (FC) storage devices, using iSCSI protocol.

**Note:** The iSCSI protocol is an IETF-defined protocol for IP storage (ips). For more information about the iSCSI protocol, refer to the IETF standards for IP storage at http://www.ietf.org.

With SCSI routing, storage device access is managed primarily in the Storage Router (see Figure 29).

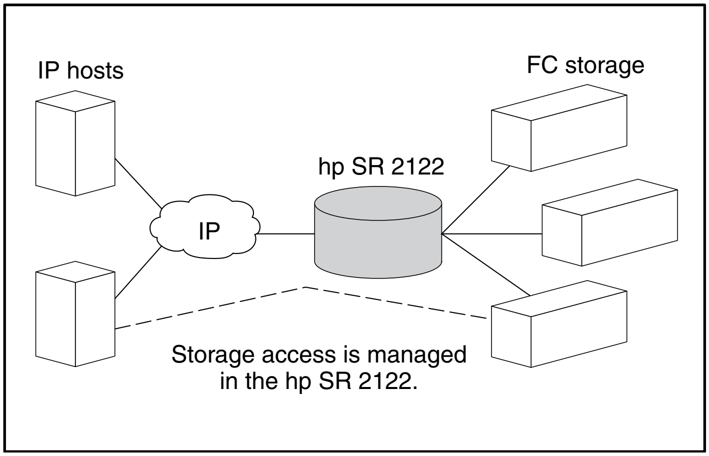


**Figure 29: SCSI routing**

In addition to providing services for accessing storage over IP networks, storage router software provides the following services:

- **VLAN Access Control** provides IP access control to storage based on a VLAN identifier (VID) number (in addition to access control through access lists).
- **Authentication** provides iSCSI authentication using AAA authentication methods.
- **High Availability (HA)** provides the ability to group storage routers in a cluster for failover and other cluster-related functions (for SCSI routing only).
- **SNMP/MIB support** provides network management of the Storage Router through SNMP using selected MIBs.
- **A command line interface (CLI) and a web-based GUI** provides user interfaces for configuration and maintenance of a Storage Router.
- **Secure Sockets Layer Support** provides HTTPS connection for secure access through the web-based GUI.

## SCSI Routing Overview

SCSI routing provides IP hosts with access to FC storage devices as if the storage devices were directly attached to the hosts, with access to devices being managed primarily in the Storage Router. An iSCSI target (also called logical target) is an arbitrary name for a group of physical storage devices. The iSCSI targets are created and mapped to physical storage devices attached to the Storage Router. The Storage Router presents the iSCSI targets to IP hosts (iSCSI initiators) as if the physical storage devices were directly attached to the hosts (see Figure 30). With SCSI routing, storage devices are not aware of each IP host; the storage devices are aware of the Storage Router and respond to it as if it were one FC host.

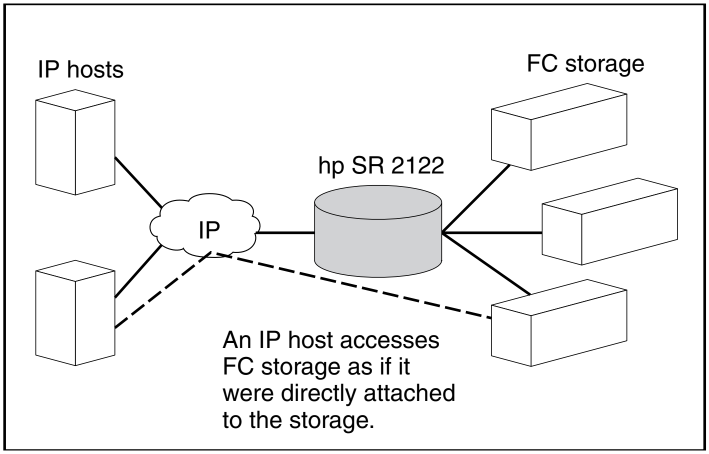

IP hosts
FC storage
hp SR 2122
IP
An IP host accesses FC storage as if it were directly attached to the storage.

**Figure 30: SCSI routing overview**

To configure a Storage Router for SCSI routing, you should have a basic understanding of the following concepts:

- Using iSCSI Protocol to Route SCSI Requests and Responses, page 43
- SCSI Routing Basic Network Structure, page 44
- SCSI Routing Mapping and Access Control, page 45
- Available Instances of SCSI Routing, page 49

**Note:** Along with FC storage, FC host connections and FC switch connections are allowed; however, most of the illustrations in this manual show only storage connections for the purpose of describing the Storage Router features.

## Using iSCSI Protocol to Route SCSI Requests and Responses

SCSI routing consists of routing SCSI requests and responses between hosts in an IP network and FC storage (see Figure 31).

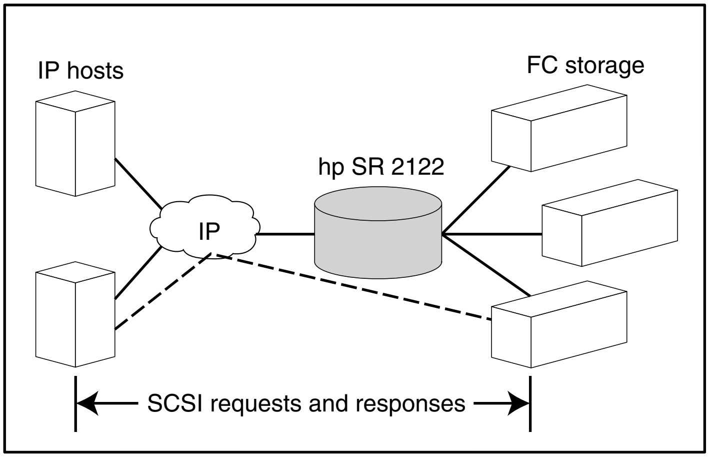


**Figure 31: Routing SCSI requests and responses for SCSI routing**

Each host that requires IP access to storage via a Storage Router needs to have a compatible iSCSI driver installed. Using the iSCSI protocol, the iSCSI driver allows an IP host to transport SCSI requests and responses over an IP network. From the perspective of a host operating system, the iSCSI driver appears to be a SCSI or Fibre Channel driver for a peripheral channel in the host.

SCSI routing consists of the following main actions (see Figure 32):

- Transporting SCSI requests and responses over an IP network between the hosts and the Storage Router
- Routing SCSI requests and responses between hosts on an IP network and FC storage
- Transporting SCSI requests and responses between the Storage Router and FC storage

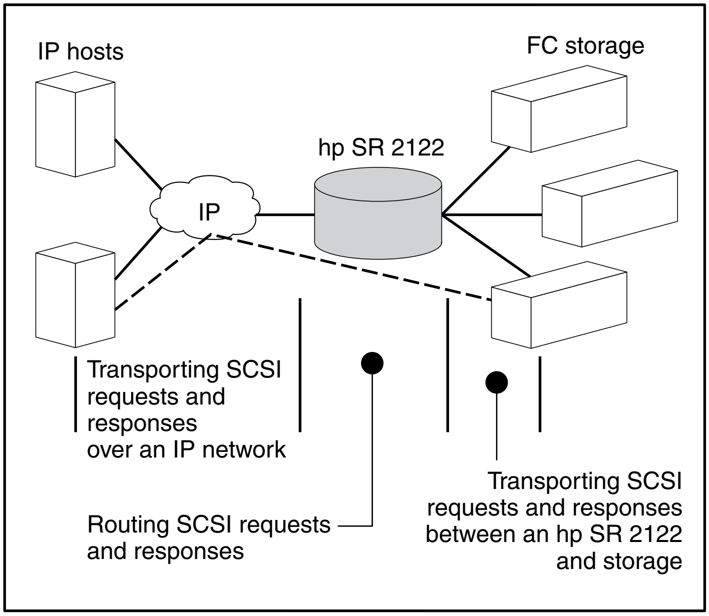

IP hosts
FC storage
hp SR 2122
IP
Transporting SCSI requests and responses over an IP network
Routing SCSI requests and responses
Transporting SCSI requests and responses between an hp SR 2122 and storage

**Figure 32: SCSI routing actions**

## SCSI Routing Basic Network Structure

Figure 33 shows the basic structure of a SCSI routing network. IP hosts with iSCSI drivers access the storage routers through an IP network connected to the Gigabit Ethernet interface of each Storage Router. The storage routers access storage devices connected to the Fibre Channel interfaces of each Storage Router. A management station manages the storage routers through an IP network connected to the management interface of each Storage Router. For high availability (HA) operation, the storage routers communicate with each other over two networks: the HA network connected to the HA interface of each Storage Router and the management network connected to the management interface of each Storage Router.

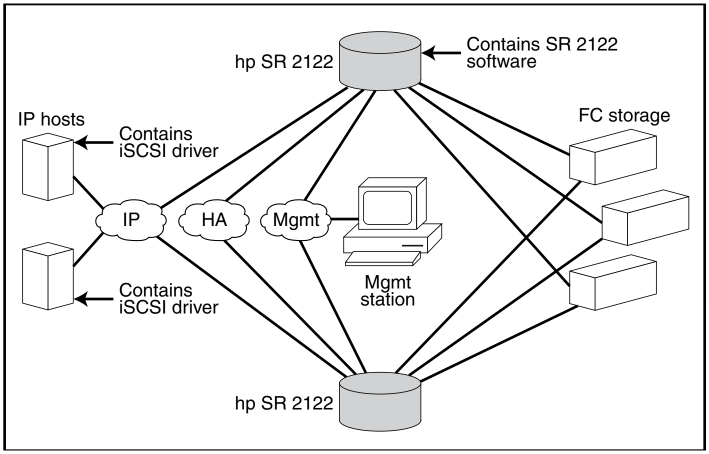


**Figure 33: SCSI Routing basic network structure**

## SCSI Routing Mapping and Access Control

SCSI routing occurs in the Storage Router through the mapping of physical storage devices to iSCSI targets. An iSCSI target (also called logical target) is an arbitrary name for a group of physical storage devices. You can map an iSCSI target to multiple physical devices. An iSCSI target always contains at least one Logical Unit Number (LUN). Each LUN on an iSCSI target is mapped to a single LUN on a physical storage target.

You can choose either of two types of storage mapping: target-and-LUN mapping or target-only mapping. Target-and-LUN mapping maps an iSCSI target and LUN combination to a physical storage target and LUN combination. Target-only mapping maps an iSCSI target to a physical storage target and its LUNs.

With target-and-LUN mapping, an iSCSI target name and iSCSI LUN number are specified and mapped to the physical storage address of one LUN; either a WWPN + LUN (World Wide Port Name + LUN) combination, a LUNWWN (LUN World Wide Name), or a LUN serial number. If the LUN is available, it is made available as an iSCSI LUN and numbered with the iSCSI LUN number specified. For example, if an iSCSI target and iSCSI LUN specified as *Database*, *LUN 9* were mapped to the physical storage address, *WWPN ID*, *LUN 12*, then *LUN 12* would be available as one iSCSI LUN. An iSCSI driver would see the iSCSI target named *Database*, with one iSCSI LUN identified as *LUN 9*. The iSCSI LUN would appear as one storage device to a host (see Table 5).

Table 5: Target and LUN Mapping Example

| Apparent to Host | iSCSI Target | iSCSI LUN Available | Physical Storage Address | Physical LUN Available |
|---|---|---|---|---|
| Local Disk (D:) | Database | LUN 9 | WWPN 070 | LUN 12 |
| Apparent as one locally attached storage device | Database appears as one controller with one LUN available | iSCSI LUN is numbered as specified and can be different than the physical LUN number | Specifies the storage address of the storage controller | The LUN number is specified as the only LUN to be mapped |

With target-only mapping, an iSCSI target name is specified and mapped to the physical storage address of a storage controller only; a WWPN. Any LUNs that are available in the storage controller are made available as iSCSI LUNs and are numbered the same as the LUNs in the storage controller. For example, if an iSCSI target specified as *Webserver2000* were mapped to the physical storage address *WWPN 050*, and *LUNs 0* through *2* were available in that controller, those LUNs would become available as three iSCSI LUNs. An iSCSI driver would see the iSCSI target named *Webserver2000* as a controller with three iSCSI LUNs identified as *LUN 0*, *LUN 1*, and *LUN 2*. Each iSCSI LUN would appear as a separate storage device to a host (see Table 6).

Table 6: Target-only Mapping Example

| Apparent to Host | iSCSI Target | iSCSI LUN Available | Physical Storage Address | Physical LUN Available |
|---|---|---|---|---|
| Local Disk (D:) | Webserver2000 | LUN 0 | WWPN 050 | LUN 0 |
| Local Disk (E:) | Webserver2000 | LUN 1 | WWPN 050 | LUN 1 |
| Local Disk (F:) | Webserver2000 | LUN 2 | WWPN 050 | LUN 2 |
| Apparent as three locally attached storage devices | Webserver2000 appears as one controller with one LUNs 0, 1, and 2 available | iSCSI LUNs are numbered the same as physical LUNs | Specifies the storage address of the storage controller | LUNs 0, 1, and 2 are available for mapping |

Access for SCSI routing is controlled in the IP hosts and the Storage Router. In an IP host, the Gigabit Ethernet IP address of the SCSI routing instance in the Storage Router with which the host is to transport SCSI requests and responses is configured in the iSCSI driver. In a Storage Router, access is controlled through an access list and a VLAN identifier (VID) number of the hosts. Additionally, access can be further controlled in the Storage Router through authentication. For more information about authentication, see the "iSCSI Authentication Overview" section on page 51.

An access list enables access to storage devices attached to the Storage Router with any combination of host IP address(es), CHAP user name(s), or iSCSI name(s). An access list contains these combinations. Host VID enables access to storage devices according to the VID of each host. For more information about VLAN access, see the "VLAN Access Overview" section on page 49.

You can use a combination of access lists and VIDs to configure access in the Storage Router; that is, you can specify that certain hosts according to IP address in a VLAN can access storage devices attached to the Storage Router.

Once the access is configured in the hosts and the Storage Router, and once the storage mapping is configured in the Storage Router, the Storage Router routes SCSI requests and responses between hosts and the mapped storage devices.

Figure 34 represents the concept of storage mapping and access control for SCSI routing. In the figure, the Storage Router provides three IP hosts with IP access to disk drives across four disk controllers. The Storage Router contains two SCSI routing instances: one configured with IP address 10.1.2.3 for the Gigabit Ethernet interface and the other with IP address 10.1.2.4. The iSCSI drivers in each IP host are configured to access those SCSI routing instances by their IP addresses through the Gigabit Ethernet interface. An access list in the Storage Router or VID (or both) specifies that hosts A, B, and C are allowed to access the mapped storage devices. From the perspective of a host, each disk drive mapped to it appears as a locally attached disk drive. Table 7 shows the correlation between an access list and/or VID, the Gigabit Ethernet IP addresses of the SCSI routing instances, and the storage device mapping.

**Note:** The purpose of Figure 34 and Table 7 is only to illustrate the concept of storage mapping and access control. The IP addresses will vary according to each site. Similarly, the type of storage addressing (for example, LUNWWN, WWPN + LUN or LUN serial number) will vary according to the types of storage and the types of storage addressing preferred at each site. In addition, the figure and the table exclude any additional storage routers that could be configured for high availability.

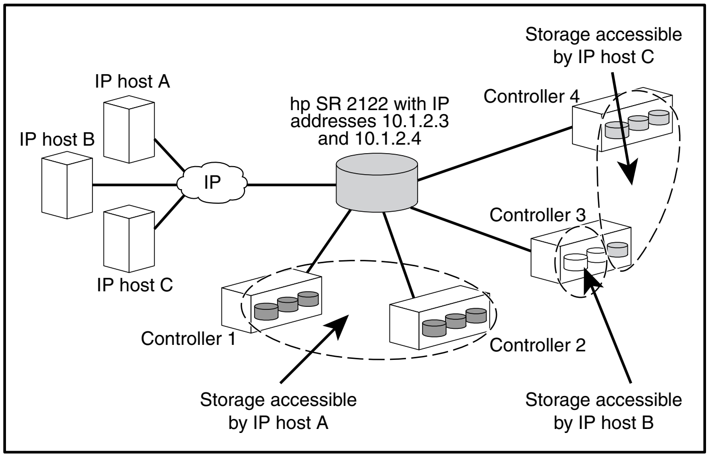


**Figure 34: SCSI routing storage mapping and access control concept**

### Table 7: SCSI Routing Storage Mapping and Access Control Concept

| Hosts allowed access via storage router access list and/or VID | Storage devices apparent to the host as locally attached devices | Via GbE IP addresses of SCSI Routing Instances | Mapped to controller | Mapped to drive |
|---|---|---|---|---|
| Host A | Local Disk (D:) | 10.1.2.3 | 1 | 1 |
| | Local Disk (E:) | 10.1.2.3 | 1 | 2 |
| | Local Disk (F:) | 10.1.2.3 | 1 | 3 |
| | Local Disk (G:) | 10.1.2.3 | 2 | 1 |
| | Local Disk (H:) | 10.1.2.3 | 2 | 2 |
| | Local Disk (I:) | 10.1.2.3 | 2 | 3 |
| Host B | Local Disk (D:) | 10.1.2.3 | 3 | 1 |
| | Local Disk (E:) | 10.1.2.3 | 3 | 2 |
| Host C | Local Disk (D:) | 10.1.2.4 | 4 | 1 |
| | Local Disk (E:) | 10.1.2.4 | 4 | 2 |
| | Local Disk (F:) | 10.1.2.4 | 4 | 3 |
| | Local Disk (G:) | 10.1.2.4 | 3 | 3 |

## Available Instances of SCSI Routing

You can configure a Storage Router with up to 12 SCSI routing services. Each service needs to be configured with a Gigabit Ethernet IP address, mapping between iSCSI target names and physical storage addresses, and access control.

When an Storage Router is part of a cluster, an instance of SCSI routing can run on only one Storage Router in a cluster at any given time. For more information about instances of SCSI routing in a cluster, see the “Storage Router Cluster Management Overview” section on page 51. For more information about configuring a Storage Router, see the appropriate configuration chapters in this document.

## VLAN Access Overview

Storage Router VLAN access provides IP hosts with access to storage devices according to the VLAN to which each host belongs.

Figure 35 shows a sample network that employs Storage Router VLAN access. In the figure, a Storage Router Gigabit Ethernet interface is connected to an IP network through an IEEE 802.1Q trunk; the Storage Router Fibre Channel interfaces are connected to storage devices 1, 2, and 3. The Storage Router is configured with two SCSI routing instances named *SR100* and *SR200*. The IP network contains two VLANs: VLAN 100 and VLAN 200. The SCSI routing instance, SR100, is configured to allow the hosts in VLAN 100 to access storage devices 1 and 2. The SCSI routing instance, SR200, is configured to allow the hosts in VLAN 200 to access storage device 3.

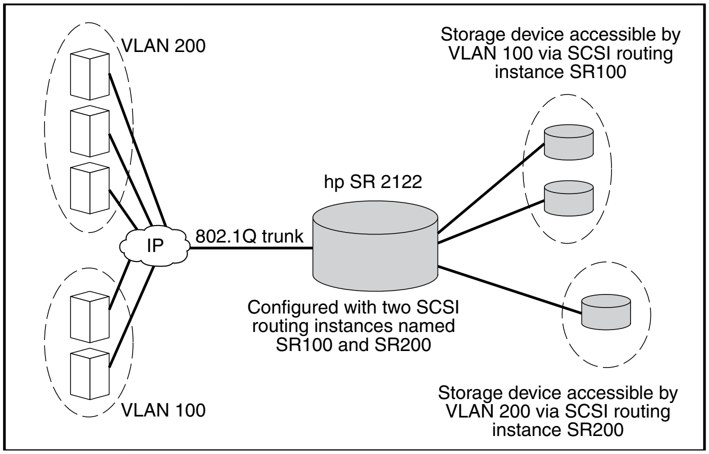

VLAN 200
Storage device accessible by VLAN 100 via SCSI routing instance SR100
hp SR 2122
IP
802.1Q trunk
Configured with two SCSI routing instances named SR100 and SR200
VLAN 100
Storage device accessible by VLAN 200 via SCSI routing instance SR200

**Figure 35: VLAN access overview**

If the Storage Router is used in a switched network environment, configure the Storage Router using the proprietary VLAN Trunking Protocol (VTP). With VTP, the Storage Router will exchange VTP packets with an externally attached switch to dynamically learn about the VLANs that are accessible in the IP network. The Storage Router then uses VTP to propagate VLAN information around the switched network using layer 2 multicast packets.

If the Storage Router is used in a non-switched network environment, configure the Storage Router for VLAN without using VTP. The Storage Router does not exchange VTP packets to learn about the VLANs in the network. Instead, you must manually assign VLANs in the network with a VLAN identifier (VID) number. You can optionally assign each VLAN with a unique name and manually set the MTU size.

If the Storage Router participates in a cluster, the VLAN information configured for the Storage Router is propagated to all storage routers in the cluster.

The Storage Router uses IEEE 802.1Q standard for VLAN encapsulation. With 802.1Q encapsulation, VLAN information is carried in packets sent and received through the Storage Router Gigabit Ethernet interface. These packets contain the VID and other VLAN information needed for VLAN members to participate in a VLAN.

A VLAN is granted access to storage devices via a SCSI routing instance configured in the Storage Router. The iSCSI targets assigned to the SCSI routing instance determine which storage devices the VLAN can access.

## iSCSI Authentication Overview

iSCSI authentication is a software service available in each Storage Router. It authenticates IP hosts that request access to storage. iSCSI authentication is provided by an AAA (authentication, authorization, and accounting) subsystem configured in each Storage Router. AAA is Cisco's architectural framework for configuring a set of three independent security functions in a consistent and modular manner: authentication, authorization, and accounting. The Storage Router software implements the authentication function.

Authentication provides a method of identifying users (including login and password dialog, challenge and response, and messaging support) prior to receiving access to the requested object, function, or network service. AAA authentication is configured by defining a list of authentication services. iSCSI authentication, which uses the AAA authentication services list, can be enabled for specific SCSI routing instances in a Storage Router.

When iSCSI authentication is enabled, IP hosts (with iSCSI drivers) must provide user name and password information each time an iSCSI TCP connection is established. iSCSI authentication uses the iSCSI CHAP (Challenge Handshake Authentication Protocol) authentication method.

## Storage Router Cluster Management Overview

You can configure storage routers in a cluster to allow the storage routers to back each other up in case of failure.

A storage router cluster consists of two storage routers connected as follows:

- Connected to the same hosts
- Connected to the same storage systems
- Connected to each other through their management and high availability (HA) interfaces

In a cluster, storage routers continually exchange HA information to propagate configuration data to each other and to detect failures in the cluster. The storage routers exchange HA information through two separate networks: one connected to the management interface of each Storage Router and the other connected to the HA interface of each Storage Router. To make sure that HA information is exchanged reliably between storage routers, the storage routers balance the transmission of HA information between the management and the HA interfaces.

A storage router cluster supports up to 12 active instances of SCSI routing. At any given time, an instance of SCSI routing can run on only one Storage Router in a cluster. The instance continues running on the Storage Router where it was started until one of the following actions occurs:

- The instance is explicitly stopped or failed over to the other Storage Router in the cluster.
- The instance automatically fails over to another Storage Router because an interface is unavailable or another software or hardware problem occurs.

Each Storage Router in a cluster can run up to 12 instances of SCSI routing. For example, if one Storage Router is already running two instances, it is eligible to run up to ten additional instances.

## Interface Naming

Configuring the storage router software requires that you understand hardware interface naming. This section describes the interface naming system used with the storage router hardware.

Each storage router interface is assigned a three-character name consisting of two lower case letters followed by a number. The letters designate the interface type; the number designates the chassis slot occupied by the interface (see Figure 36).

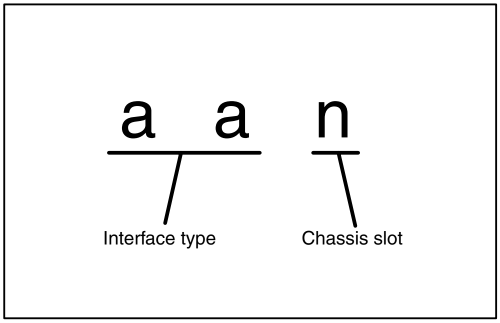


**Figure 36: Storage router interface naming system**

Table 8 shows valid interface type designators for the Storage Router; Figure 37 shows each interface location and interface name on the Storage Router.

Table 8:  Interface Type Designators

| Interface Type | Description |
|---|---|
| FC | Fibre Channel |
| GE | Gigabit Ethernet |

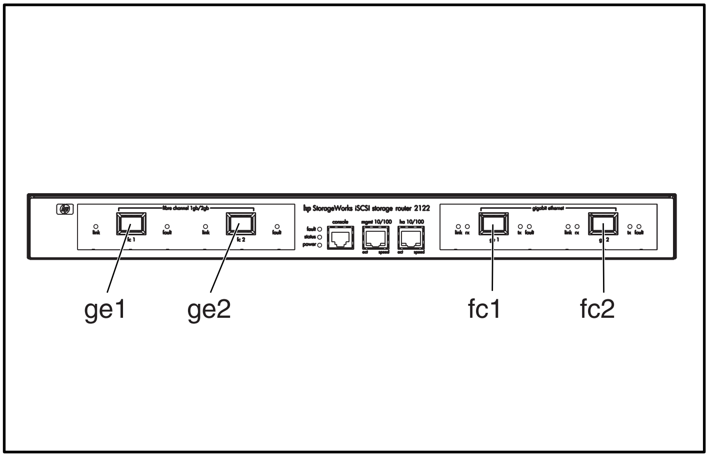


Figure 37:  Storage router chassis-slot numbering

## Where to Go Next

When you are ready to configure the storage router software, proceed to one of the following chapters in this configuration guide according to your needs:

- Chapter 5, “Configuring the Storage Router” — For initial setup or after configuration has been reset to factory default configuration
- Chapter 6, “Configuring System Parameters” — Using the CLI for setting up and modifying system parameters
- Chapter 7, “Configuring VLAN” — Using the CLI for setting up and modifying VLAN configurations
- Chapter 8, “Configuring SCSI Routing” — Using the CLI for setting up and modifying SCSI routing configurations
- Chapter 9, “Configuring Authentication” — Using the CLI for setting up and modifying authentication configurations
- Chapter 10, “Configuring a High Availability Cluster” — Using the CLI for setting up and modifying cluster configurations
- Chapter 11, “Maintaining and Managing the Storage Router” — Downloading software, backing up and restoring configurations, and other related maintenance and management tasks

# Configuring the Storage Router

5

This chapter describes the configuration information to gather and explains the initial system configuration script and setup configuration wizard for the first-time configuration of the Storage Router. This chapter also introduces the command line interface (CLI) and web-based GUI, which can be used for subsequent configuration tasks.

This chapter contains the following sections:

# Prerequisite Tasks

Before configuring the Storage Router for the first time, make sure you have completed the hardware installation according to Chapter 2, “Installation.”

# Collecting Configuration Information

Use the Storage Router First-Time Configuration Checklist (see Table 10) to help you gather the system and network information is needed for the first-time configuration of your Storage Router. The items in the checklist are based on the information requested by the initial system configuration script and the setup configuration wizard. Refer to Table 9 for information on the configuration items needed for first-time configuration.

**Table 9: Collecting Configuration Information**

| Configuration Item | Description | Required or Optional |
|---|---|---|
| Configuration deployment | **SCSI routing** (Storage Router enables iSCSI hosts to access Fibre Channel storage. Storage Router manages access to the Fibre Channel storage.) | Required |
| Management interface IP address and subnet mask | The IP address and subnet mask of the storage router management interface.<br>**Note:** The management interface for each Storage Router in a cluster must be on the same IP subnet. | Required |
| Static route for management interface | The destination IP address with subnet mask and then the gateway IP address. | Required if the Storage Router is managed from a subnet other than the one to which it is physically attached |
| System name | The name you want to use for the Storage Router. If you use the services of a domain name server (DNS), the system name is the same name you will enter and associate with the management interface. Maximum length is 19 characters. | Required |
| GE Interface | The Gigabit Ethernet interface used to communicate to the IP network, either **ge1** or **ge2**. The default is **ge1**. | Required for SCSI routing only |

| Configuration Item | Description | Required or Optional |
|---|---|---|
| High availability (HA) configuration | The Storage Router can run in either **standalone** or **clustered** mode. The default is **clustered**. Standalone mode is recommended if the Storage Router is not intended to provide high availability along with other storage routers. | Required for SCSI routing only |
| High availability (HA) cluster name | The name of the cluster in which the Storage Router is to participate. Clusters are multiple storage routers that back each other up in case of hardware or software failure. All storage routers that participate in a cluster must have the same cluster name. | Required only if clustered was specified for the HA configuration |
| High availability (HA) IP address and subnet mask | The IP address and subnet mask of the storage router HA interface. The HA interface and management interface must be on unique IP networks. If the Storage Router is to participate in a cluster, the HA IP address is required; if the Storage Router is a standalone machine, it is optional.<br>**Note:** The HA interface for each Storage Router in a cluster must be on the same IP subnet. | Required only if clustered was specified for the HA configuration |
| Primary DNS IP address | The IP address of the primary domain name server to be accessed by the Storage Router. Required if you refer to any other server via name rather than IP address. | Optional |
| Secondary DNS IP address | A backup domain name server from which the Storage Router can request services when the primary DNS is unavailable. | Optional |
| NTP server IP address | The IP address of the NTP server available to the Storage Router. This allows the Storage Router to keep the date and time synchronized with the rest of the network. | Optional |
| Time zone, current date and time | The format for the date is mm/dd/yyyy, and the time is hh:mm:ss. | Optional |
| Enable Telnet on all interfaces | Enable Telnet access on all interfaces. By default, Telnet access is enabled on only the management interface. | Optional |
| SNMP read community name | The name of the community having read-only access to the storage router network. The Storage Router will respond to this community's `GET` commands. The default is **public**. | Optional |
| SNMP write community name | The name of the community having write access to the storage router network. The Storage Router will respond to this community's `SET` commands. The default is **private**. | Optional |
| First SNMP trap manager IP address | The IP address of the first destination host used for SNMP notifications (traps). Required if you wish to use SNMP traps. | Optional |

| Configuration Item | Description | Required or Optional |
|---|---|---|
| Trap version for first SNMP IP address | The version number of the traps that are to be sent to the first SNMP trap manager IP address. The default is **1**. | Optional |
| Second SNMP trap manager IP address | An optional IP address of the second destination host used for SNMP notifications (traps). | Optional |
| Trap version for second SNMP IP address | The version number of the traps that are to be sent to the second SNMP trap manager IP address. The default is **1**. | Optional |
| Send authentication failure option | Enable an authentication failure trap to be sent when a user specifies an incorrect community. | Optional |
| Send link up/down traps option | Enable link up/down traps to be sent for the Management, HA, Gigabit, and/or Fibre Channel interfaces when the link goes up and when it goes down. | Optional |
| Monitor-level password | A password for users who will only monitor storage router operations. The default password is **hp**. | Optional |
| Administrator-level password | A password for users who will configure and administer the Storage Router. The default password is **hp**. | Optional |

| Configuration Item | Description | Required or Optional |
|---|---|---|
| Password applied to EIA/TIA-232 console interface (yes/no) | Choose whether or not the user is required to enter the monitor and administrator password when accessing the Storage Router via the EIA/TIA-232 console interface. The default is **no**. | Optional |
| System administrator contact information | The name, e-mail address, phone number, and pager number of the system administrator of the Storage Router. Usage is completely site-specific. | Optional |
| Name of SCSI routing instance | A unique name for a SCSI routing instance. Names of instances can be up to 32 characters in length. A maximum of 12 unique SCSI routing instances are allowed. Only one instance can be named in the **setup configuration** wizard.<br>**Note:** If the Storage Router is going to be a member of a cluster, do not define more than 12 SCSI routing instances across all storage routers in the cluster. For additional information about HA, cluster configuration and failover, see Chapter 10, “Configuring a High Availability Cluster“ and Chapter 11, “Maintaining and Managing the Storage Router.“<br>**Note:** Do not name the SCSI routing instance with the setup configuration wizard if you are using the VLAN service with your Storage Router. See Chapter 7 “Configuring for VLAN” before naming and configuring SCSI routing instances. | Required |

Once you have completed the first-time configuration checklist, you are ready to continue with the first-time configuration of the Storage Router using the initial system configuration script and the setup configuration wizard.

Table 10: Storage Router First-Time Configuration Checklist

| Configuration Item | Value |
|---|---|
| Configuration deployment option (1 or 2) | |
| Management interface IP address and subnet mask | |
| Static route for management interface | |
| System name | |
| GE Interface | |
| High availability (HA) configuration (standalone or clustered) | |
| HA cluster name | |
| HA interface IP address and subnet mask | |
| Primary DNS IP address | |
| Secondary DNS IP address | |
| NTP server IP address | |
| Enable Telnet on all interfaces (yes/no) | |
| SNMP read community name (default public) | |
| SNMP write community name (default private) | |
| First SNMP trap manager IP address | |
| Trap version for first SNMP IP address | |
| Second SNMP trap manager IP address | |
| Trap version for second SNMP IP address | |
| Send authentication failure trap when incorrect community specified (yes/no) | |
| Modify link up/down traps for one or more interfaces (yes/no) | |
| Send link up/down traps for Management interface (yes/no) | |
| Send link up/down traps for HA interface (yes/no) | |
| Send link up/down traps for Gigabit Ethernet interface (yes/no) | |
| Send link up/down traps for Fibre Channel interface (yes/no) | |
| Monitor-level password | |
| Administrator-level password | |
| Apply passwords to EIA/TIA-232 console interface (yes/no) | |
| System administrator name | |
| System administrator e-mail address | |

| Configuration Item | Value |
|---|---|
| System administrator phone number | |
| System administrator pager number | |
| Name of SCSI routing instance (if using the VLAN service, do not configure a SCSI routing instance with the setup configuration wizard) | |
| Configuration deployment option (1 or 2) | |
| Management interface IP address and subnet mask | |

# Connecting a Console

To begin configuration of your Storage Router, use the command line interface (CLI), by connecting a PC with a terminal emulation program to the EIA/TIA-232 console interface according to the Storage Router Hardware Installation Guide. Then make sure that the terminal emulation program is configured for a CLI session with the values provided in Table 11.

**Table 11: Terminal Emulation Configuration**

| Setting | Value |
|---|---|
| Terminal Mode | VT-100 |
| Baud | 9600 |
| Parity | No parity |
| Stop bits | 1 stop bit |

## Initial System Configuration Script

The initial system configuration script runs on the CLI and ensures that a few required values are entered to make the Storage Router operational. When you first power up the Storage Router and after the initial boot process, the script will run automatically on the CLI session running on the terminal emulation program via an EIA/TIA-232 console connection.

After the first running of the script, the script will run automatically whenever the Storage Router is not configured with an IP address for the management interface, due most likely to a `clear conf` command, which requires the system to be configured again.

The initial system configuration script provides explanatory text before prompting you to enter configuration values. There are two versions of the script. The values asked for by the script are determined by the configuration deployment option entered for the first prompt.

Table 12 lists the configuration items in the order they will appear in the script.

**Table 12: Configuration items in Initial System Configuration Script**

| Configuration Item | Configuration Deployment |
|---|---|
| Management interface IP address and subnet mask in CIDR style (for example: 10.1.10.244/24) | |
| The destination IP address with subnet mask and then the gateway IP address (for example: 1.0.1.0/24 10.0.1.2) (Optional) | |
| Storage router system name (maximum length allowed is 19 characters) | |
| HA configuration (standalone or clustered) | |
| Cluster name (asked for only when HA configuration is set to clustered) | |
| HA interface IP address and subnet mask in CIDR style (for example: 10.1.20.56/24; asked for only when HA configuration is set to clustered) | |
| Gigabit Ethernet interface used to communicate to IP network, select either ge1 or ge2 | |
| Gigabit Ethernet interface IP address and subnet mask in CIDR style (for example: 10.1.0.45/24) | |

When the script completes, the system automatically reboots. When the command prompt returns, continue configuration with the setup configuration wizard.

# Running the Setup Configuration Wizard

The Setup Configuration Wizard is available from the CLI and is a script that consists of a series of prompts asking you to enter values to provide a basic system configuration for your Storage Router. You will be asked to enter values to configure the following:

- Management interface (this includes primary and secondary DNS servers)
- Time zone, NTP server, current date and time
- Network management access (this includes SNMP)
- Monitor and administrator passwords
- Console interface password
- System administrator contact information
- SCSI routing (this section of the wizard only appears if SCSI routing was the configuration deployment selected in the initial system configuration script; if you are using the VLAN service, do not configure SCSI routing with the Setup Configuration Wizard)

You can run the Setup Configuration Wizard through an EIA/TIA-232 console interface connection, or through a Telnet session using the management interface if the IP address is already configured in the Storage Router. If you choose to complete the configuration using the management interface, use the default password, `hp`, to establish your CLI session.

The values entered for the Setup Configuration Wizard are saved at the end of the wizard's script. To quit the configuration wizard at any time without saving changes, press **Ctrl-C**, and reboot the Storage Router to restore previous values.

**Note:** The factory default listening port used for iSCSI traffic is 3260. This is a port number assigned by IANA. You can change this value for your network configuration if needed.

Use the following procedure to start the Setup Configuration Wizard:

1. `enable` — Enter Administrator mode. If prompted for an Administrator password, use the default password, **hp**.
2. `setup` — Start the setup configuration wizard. The wizard can run in either of two modes: **novice** or **expert**. The novice level provides information before the prompt explaining what is being requested. The expert level does not provide the explanatory text. The wizard will ask you to choose one of the two levels. Respond to the prompts using your "Storage Router First-Time Configuration Checklist" table on page 60. For multiple choice questions, the choices are shown in square brackets. For values requiring a specific format, the required format is shown in square brackets. If values have already been entered (for instance, via the initial system configuration script), the current value saved in the system are shown in square brackets. Default values are shown in parentheses within the square brackets. If you want to accept the current or default value, press **Enter**. If there is no default and you want to bypass the question (that is, you do not want to change or provide a value), simply press **Enter**.

If you configured any interfaces or identified any servers to the Storage Router that are outside the storage router management subnet, you must update the storage router route table with the appropriate gateways that will provide access to these interfaces or servers (use the `ip route` command).

You can use the `setup` command again to change these basic configuration parameters. You can also use the command line interface (CLI) or the web-based GUI to make changes to the basic storage router configuration or to configure the Storage Router more extensively. To access the web-based GUI, point your browser to the storage router management interface IP address.

## Introducing the CLI

The CLI is available via a Telnet session to the management interface. It is also available via a direct EIA/TIA-232 connection on the console interface. The CLI provides commands to perform all necessary storage router management functions, including software upgrades and maintenance.

All CLI commands are capable of prompting for further information as the user types. Pressing the Tab key completes the current command word at any point after it is unique. Pressing the question mark (`?`) key lists all of the options available at that point in the command syntax. Each word can be truncated at any point after it is unique.

## Character Case Sensitivity in the CLI

CLI commands, keywords, and reserved words are not case-sensitive. Commands, keywords, and reserved words can be entered in upper and lower case. User-defined text strings can be defined in both upper and lower case (including mixed cases) and is preserved in the configuration.

## Command Modes

The storage router management interface is password protected. You must enter passwords when accessing the Storage Router via Telnet (for the CLI) or web-based GUI.

There are two levels of authority:

- **Monitor mode** allows view-only access to the storage router status and system configuration information.
- **Administrator mode** allows the user to configure and actively manage the Storage Router, its access lists and SCSI routing instances, and the storage router cluster.

Passwords for Monitor and Administrator mode can be initially configured through the Setup Configuration Wizard (see "Running the Setup Configuration Wizard" on page 63). The factory default password for both modes is `hp`.

## Command Prompt

The CLI command prompt includes the storage router system name. An asterisk ( `*` ) appears at the beginning of the prompt if the system configuration has been modified but not saved.

## Reserved Words

Reserved words cannot be used as values or names in CLI commands. Words that are used as commands or as keywords in commands are reserved words. The following are additional reserved words in the CLI.

- `acl`
- `canonical`
- `iprouter`
- `iptan`
- `loglevel`

## Show CLI Command

Use the `show cli` command to display the complete CLI command syntax tree, along with helpful information about command parameters and arguments. Only valid commands will display for the current command mode of your Storage Router.

You can choose specific commands to display by specifying desired commands with the `show cli` command. For example, `show cli aaa debug scsirouter` displays the syntax tree for all aaa commands, all debug commands, and all scsirouter commands.

## Special Keys

The CLI supports the use of special keyboard keys. Table 13 lists the special keys and describes their function.

**Table 13: Special Keys**

| Key | Function |
|---|---|
| `?` | List choices |
| `Backspace` | Delete character backwards |
| `Tab` | Command word completion |
| `Ctrl-A` | Go to the beginning of the line |
| `Ctrl-B or Left Arrow` | Go backwards one character |
| `Ctrl-D` | Delete current character |
| `Ctrl-E` | Go to the end of the line |
| `Ctrl-F or Right Arrow` | Go forward one character |
| `Ctrl-K` | Delete from current position to the end of the line |
| `Ctrl-N or Down Arrow` | Go to the next line in the history buffer |
| `Ctrl-P or Up Arrow` | Go to the previous line in the history buffer |
| `Ctrl-T` | Transpose the current and previous character |
| `Ctrl-U` | Delete the line |
| `Ctrl-W` | Delete the previous word |

## Starting a CLI Management Session

Follow these steps to start a CLI management session via a Telnet connection to the Storage Router.

1. Establish a Telnet session to the Storage Router.
2. Enter the appropriate password at the logon prompt.
3. Enter `enable` to change to Administrator mode. (Optional)

**Note:** If you need to make changes to the configuration of the Storage Router, you need to enable the Administrator mode.

4. Enter the Administrator password at the prompt. (Optional)
5. Issue the appropriate CLI commands to complete the desired task.

# Introducing the Web-Based GUI

As an alternative to the CLI, you can configure your Storage Router using the web-based GUI. You can use the GUI for configuration after completing the initial system configuration script, which assures that the storage router management interface is configured with an IP address.

To access the GUI, enter the URL for the Storage Router by pointing your browser to the storage router management interface IP address using the HTTP protocol (for example, type `http://10.1.10.244`).

## Logging In

After entering the URL for your Storage Router, a login page appears. You can log in as monitor or as admin, and you will be asked for your user name and password. See Table 14 for the user name and factory default password to use for the two login options. If you already configured new passwords for the monitor and/or the administrator mode, use them when logging in.

**Table 14: Logging into the Web-Based GUI**

| Login Options | User Name | Factory Default Password |
|---|---|---|
| Monitor | monitor | hp |
| Admin | admin | hp |

## Monitor Mode

Monitor mode in the web-based GUI will only allow you to monitor the Storage Router. You cannot configure, maintain, or troubleshoot the Storage Router in monitor mode. If you click on the Configuration, Maintenance, and Troubleshooting menu items in the GUI, a login dialog box will appear asking for a user name and password for administrator mode.

## Administrator Mode

In administrator mode, you can configure, maintain, and troubleshoot the Storage Router. If you click the Monitor menu item, a login dialog box will appear asking for a user name and password for monitor mode.

## Menu Items and Links

The GUI's menu items and links appear horizontally at the top of the browser page. Table 15 lists the menu items and links, the action that takes place when they are clicked, and the login modes from which they are available.

**Table 15: Menu and Item Links**

| Menu Items and Links | Action | Login Mode |
|---|---|---|
| Monitor | Lists menu options in left frame to be displayed in main frame. | Monitor only |
| Configuration | Lists menu options in left frame to be displayed in main frame. | Admin only |
| Maintenance | Lists menu options in left frame to be displayed in main frame. | Admin only |
| Troubleshooting | Lists menu options in left frame to be displayed in main frame. | Admin only |
| Support | Opens the HP.com "Service & Support" page in a new browser window. | Monitor and Admin |
| Home | Returns to the GUI's login page where you select to log in as either Monitor or Admin. | Monitor and Admin |
| Help | Opens the GUI's online help in a new browser window. | Monitor and Admin |

# Installing the iSCSI Drivers

The following section decides the procedure for installing the iSCSI drivers for Linux and for the Cisco initiator.

## Installing the iSCSI driver for Linux

This section provide instructions fir installing the iSCSI drivers for Linux and contains the following topics:

### Pre-requisites

The kernel source must be installed for the iSCSI driver to compile properly.

If you are upgrading from a previous installation of the iSCSI driver, hp recommends that you remove the file */etc/initiatorname.iscsi* before installing the new driver.

### Installing the Driver

1. Use `tar(1)` to decompress the source archive into a directory of your choice. The archive will contain a subdirectory corresponding to the archive name.

```
cd /usr/src
tar xvzf /path/to/linux-iscsi-<version>.tgz
cd linux-iscsi-<version>
```

2. Compile the iSCSI driver. If your kernel sources are not in the usual place, add 'TOPDIR=/path/to/kernel' or edit the definition of TOPDIR in the Makefile.

```
make
```

3. As root, install the driver. If you are currently using the iSCSI driver, first unmount all iSCSI devices and unload the old iSCSI driver. If your Linux distribution includes an iSCSI driver, it may be necessary to uninstall that package first.

```
make install
```

4. Update */etc/iscsi.conf* to include the IP addresses for your iSCSI targets. A sample configuration file might include entries like this:

   ```
   DiscoveryAddress=192.168.10.94
   ```

   The *iscsi.conf* man page has a more detailed description of the configuration file format. To read the man page, type:

   ```
   man iscsi.conf
   ```

5. Manually start iSCSI services to test your configuration. On Red Hat systems, run:

   ```
   /etc/rc.d/init.d/iscsi start
   ```

   If there are problems loading the iSCSI kernel module, diagnostic information will be placed in */var/log/iscsi.log*.

   The iSCSI initialization will report information on each detected device to the console or in `dmesg(8)` output. For example:

   ```
   Vendor: SEAGATE Model: ST39103FC Rev: 0002
   Type: Direct-Access              ANSI SCSI revision: 02
   Detected scsi disk sda at scsi0, channel 0, id 0, lun 0
   SCSI device sda: hdwr sector= 512 bytes.
                      Sectors= 17783240 [8683 MB] [8.7 GB]
   sda: sda1
   scsi singledevice 0 0 0 1
   ```

   Normal disk commands like fdisk, mkfs, and fsck will work on the iSCSI devices like a local drive.

   */proc/scsi/iscsi* will contain a file (the controller number) that contains information about the iSCSI devices.

   To manually stop the iSCSI driver enter:

   ```
   /etc/rc.d/init.d/iscsi stop
   ```

6. Modify your init scripts to manage iSCSI. If you are using a non-Red Hat Linux distribution you may need to edit your boot scripts to properly run the iSCSI setup script. You may also need to change the order of the boot script to ensure that iSCSI services are started after the network has been initialized.

7. List your iSCSI partitions in */etc/fstab.iscsi*. It has the same format as */etc/fstab*. The init scripts will mount and unmount these partitions automatically. Refer to the readme file that comes with the iSCSI driver source archive for more details on how to do this correctly.

## Uninstalling the Driver

1. Change to the driver source directory from installation step 1.
2. While logged in as root, run:

   ```
   make remove
   ```

   This deletes the appropriate files from */lib/modules* and */usr/local/sbin*. The configuration files in */etc* are not deleted, since they will be needed if another driver version is installed later.
3. Back up one directory and delete the source code:

   ```
   cd ..
   rm -fr linux-iscsi-<ver>
   ```

## Cisco Initiator Installation Sequence in a Microsoft Windows 2000 Environment

1. Go to the directory where the initiator software resides and run *Setup.exe.*

   ```
   C:\SR2122\Initiator\Setup.exe
   ```
2. Follow the prompts on the screen and accept the license agreement.
3. At the appropriate screen, enter the required Target IP addresses.
4. Reboot the File Server when prompted.
5. After the system restarts, log in to your test domain, and go to Control Panel */iSCSI Config*. Double-click the icon in Control Panel.
6. To ensure network connectivity, press the “Rescan” or “Re-Login” button. You should see the IP address(es) you added in Step 3.
7. Exit the iSCSI Config Screen.
8. Start an Internet browser and open the SR2122 GUI as Admin.
9. Go to “Configuring SCSI Targets and Access List Entries” to complete the storage configuration.

## Where to Go Next

If you did not run the complete Storage Router Setup Configuration Wizard, or if you want to make system configuration additions, changes, or corrections, continue with the procedures described in Chapter 6, “Configuring System Parameters.”

If you are using the VLAN service with the Storage Router and you entered all desired parameters — except for SCSI routing — with the Setup Configuration Wizard (see “Running the Setup Configuration Wizard” on page 63 for details), configure for VLAN using the procedures described in Chapter 7, “Configuring for VLAN.”

If you do not need to configure for VLAN or zoning, go directly to Chapter 8, “Configuring SCSI Routing,” to configure SCSI routing more extensively.

**Note:** If you are going to add the Storage Router to an existing storage router cluster, review the information and procedures in Chapter 10, “Configuring a High Availability Cluster,” before configuring SCSI routing.

# Configuring System Parameters

6

This chapter explains how to configure system parameters on your Storage Router and contains the following sections:

System parameters can be configured or changed using CLI commands, as described in this chapter, or via the web-based GUI. To access the web-based GUI, point your browser to the Storage Router's management interface IP address. After logging on, click the Help link to access online help for the GUI.

## Prerequisite Tasks

Before configuring system parameters, make sure you have finished the following tasks:

- Completed the hardware installation according to the Storage Router Hardware Installation Guide
- Entered values as requested by the initial system configuration script (for more information, see the "Initial System Configuration Script" in Chapter 5 page 62)

**Note:** You do not need to perform the configuration tasks in this chapter if you ran the complete Storage Router Setup Configuration Wizard (using the `setup CLI` command with no keyword), or if you ran the wizards separately using all the `setup CLI` commands except `setup scsi`.

## Configuration Tasks

To configure system parameters on your Storage Router, perform the following steps:

1. Configure the management interface.
2. Configure the time and date.
3. Configure network management access. (Optional)
4. Configure passwords.
5. Configure administrator contact information.
6. Configure the high-availability (HA) interface. (Optional)
7. Verify and save configuration.

**Note:** You can verify and save the configuration (by using the `save system bootconfig` or `save all bootconfig` command) at any point in the process of performing the configuration tasks.

Figure 38 illustrates the example configuration used in this chapter.

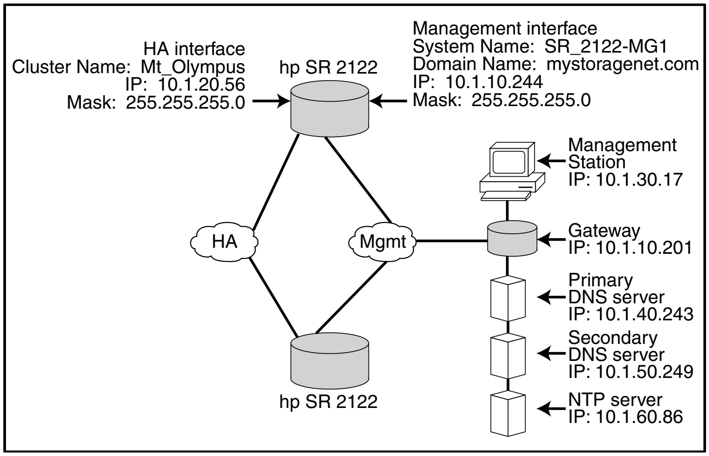


**Figure 38: System parameters example configuration**

# Configuring the Management Interface

Configuring the management interface consists of tasks for setting the system name, IP address and mask, gateway, and DNS servers. Use the following procedure to configure the management interface:

**Note:** The purpose of Figure 38 is an example system configuration only. The IP addresses and all names given below are examples only.

1. `enable` — Enter Administration mode.
2. `hostname` *`SR_2122-MG1`* — Specify or change the system name. The system name identifies the Storage Router through the management interface and appears immediately in the prompt.
3. `interface mgmt ip-address` *`10.1.10.244/24`* — Specify or change the IP address and subnet mask for the management interface.

**Note:** If this Storage Router is to participate in a cluster, the management interface for all storage routers in the cluster must be on the same IP subnet.

4. `ip route` *`10.1.30.0/24 10.1.10.201`* — Configure a gateway IP address if the Storage Router is to be managed from a management station outside the storage router management subnet. The second IP address specifies a gateway on the storage router management network that will provide access to a management station. (Optional)

**Note:** In this configuration example, the mask is set to **24 255.255.255.0** to allow any host on subnet **10.1.30.0** to be a management station.

5. `ip name-server` *`10.1.40.243 10.1.50.249`* — Set the primary and secondary DNS IP addresses. Specifies the IP address of the primary DNS server if the management interface IP address is to be correlated with a DNS host name. If there is a secondary DNS, the second IP address specifies the IP address of the secondary DNS server. (Optional)
6. `ip domain-name` *`mystoragenet.com`* — Specify the domain name of the Storage Router. Use this command in conjunction with the `ip name-server` command. (Optional)
7. `ip route` *`10.1.40.243/32 10.1.10.201`* — Configure a gateway IP address if the primary DNS server is outside the storage router management subnet. The second IP address specifies a gateway on the storage router management network that will provide access to a primary DNS server. (Optional)

**Note:** In this configuration example, the mask is set to **32 255.255.255.255** to specify the host with IP address **10.1.40.243** (the primary DNS server).

8. `ip route` *`10.1.50.249/32 10.1.10.201`* — Configure a gateway IP address if the secondary DNS server is outside the storage router management subnet. The second IP address specifies a gateway on the storage router management network that will provide access to a secondary DNS server. (Optional)

**Note:** In this configuration example, the mask is set to **32 255.255.255.255** to specify the host with IP address **10.1.50.249** (the secondary DNS server).

## Configuring Time and Date

Configuring time and date parameters consists of specifying the time, date, time zone, and time server. Use the following procedure to configure the time and date parameters:

1. `enable` — Enter Administration mode.
2. `Clock set` *`08:20:00 02 15 2002`* — Set time and date (for example: time, **8:20 A.M.**; date, **April 15, 2002**).
3. `Clock set` *`08:20:00 02 15 2002`* — Identify the time zone where the Storage Router is located. If a time zone is not identified, the default is GMT.

   To use the `clock timezone` command, you must use a valid time-zone string. For a list of valid time-zone strings, use the `clock timezone ?` command.
4. `NTP peer` *`10.1.60.86`* — Specify the name or IP address of the network time protocol (NTP) server with which the Storage Router will synchronize the date and time. (Optional)
5. `IP route` *`10.1.60.86/32 10.1.10.201`* — Specify the gateway IP address if the time server is outside the storage router management subnet. The second IP address specifies the gateway on the storage router management network that provides access to the time server. (Optional)

**Note:** In this configuration example, the mask is set to **32 255.255.255.255** to specify the host with IP address **10.1.60.86**.

# Configuring Network Management Access

Configuring network management access consists of tasks for configuring SNMP. Use the following procedure to configure SNMP for network management access:

1. `enable` — Enter Administration mode.
2. `no restrict` *`all`* `telnet` — Enable Telnet access on **all** interfaces. By default, Telnet access is enabled on only the management interface. (Optional)
3. `snmp-server community` *`world`* `ro` — Specify the name of the community having read-only access of the storage router network (that is, to which community's `GET` commands the Storage Router will respond). The default read community is **public**. (Optional)
4. `snmp-server community` *`mynetmanagers`* `rw` — Specify the name of the community having write access to the storage router network (that is, to which community's `SET` commands the Storage Router will respond). The default write community is **private**. (Optional)
5. `snmp-server host` *`10.1.30.17`* `version` *`2`* `traps` — Specify the IP address for the first destination host used for a specified version of notifications (traps). Version 1 traps is the default version.

**Note:** In this configuration example, the trap hosts have IP addresses that are outside the storage router management subnet. In an earlier step in the "Configuring the Management Interface" section, a gateway was already specified providing access to hosts on the **10.1.30.0** subnet.

6. `snmp-server host` *`10.1.30.18`* `traps` — Specify the IP address for the second destination host used for notifications (traps). Version 1 traps is the default version. (Optional)
7. `snmp-server` *`sendauthtraps`* — Enable sending of authentication failure traps. (Optional)
8. `no snmp-server` *`linkupdown all`* — By default, the SNMP agent is enabled to generate link up/down traps for all interfaces. In this configuration example, the command disables this setting for all interfaces. (Optional)

# Configuring Passwords

Configuring passwords consists of setting the monitor-mode and administrator-mode passwords for access to the 10/100 Ethernet management interface (used for the CLI via Telnet and the web-based GUI via HTTP). You can enable these passwords to restrict access to the EIA/TIA-232 console interface. Use the following procedure to configure passwords:

**Note:** The factory default password for both Monitor and Administrator modes is **hp**.

1. `enable` — Enter Administration mode.
2. `Monitor password` *`janu$01`* — No snmp-server linkupdown all.
3. `Admin password` *`electr@50`* — Set the administrator password (for system administrators, allowing configuration changes).
4. `Restrict console` — Enable the Monitor-mode and Administrator-mode passwords to be required when accessing the Storage Router via a console connected to the EIA/TIA-232 console interface. (Optional)

# Configuring Administrator Contact Information

Configuring administrator contact information consists of tasks for specifying the name, e-mail address, phone number, and pager number of the system administrator for the Storage Router. Use the following procedure to configure administrator contact information:

1. `enable` — Enter Administration mode.
2. `Admin contactinfo name` *`Pat J. Smith`*`, email` *`pjsmith@mystoragenet.com`* `phone` *`763-555-1117`*`, and pager` *`763-555-7766`* — Provide contact name, e-mail address, phone number, and pager number. Enclose each string that contain spaces in single or double quotes.

**Note:** The `admin contactinfo` command requires that you specify either one parameter or all four parameters.

## Configuring the High-Availability Interface

When the Storage Router is part of a storage router cluster, you will need to configure the high availability (HA) interface. Use the following procedure to configure the HA interface parameters:

1. `enable` — Enter Administration mode.
2. `Show cluster` — Display cluster information and refer to the HA Configuration field to verify if the Storage Router is running as standalone or clustered. Also, verify if the HA interface is configured with a correct IP address.
3. `setup cluster` — Run the Setup Cluster Wizard. The wizard prompts you to do the following:
   - Select the appropriate HA configuration mode (standalone or clustered).
   - Specify HA interface IP address and subnet mask. (The HA and management interfaces must not be on the same network; each interface must be on a unique IP network. In a cluster, the HA interfaces for all storage routers must be on the same IP subnet.)
   - Change cluster name (if necessary).
   - You will be asked if you want to retain or delete the current configuration of the Storage Router:
     - Retaining means that the configuration of this Storage Router (including SCSI routing instances) is propagated to the other Storage Router in the same cluster.
     - Deleting means that the existing configuration (including SCSI routing instances) will be deleted from the Storage Router.

   If you are joining an existing cluster, any access lists that you have previously defined will be overwritten by the access lists available to the cluster. This occurs regardless of your decision to retain or delete configuration information. If you wish to make your current access lists available to the cluster, you must save them to a file before joining the cluster, then restore them. See Chapter 10, “Configuring a High Availability Cluster,” for complete details.

   As prompted, type `yes` to confirm your choice to retain or delete the current configuration of the Storage Router. The system will then automatically reboot.

# Verifying and Saving Configuration

Verify the system parameters using the following procedure. You can save the configuration at any time using either the `save system bootconfig` or `save all bootconfig` commands. You must save the running configuration to the bootable configuration for it to be retained in the Storage Router when it is rebooted.

Use the following procedure to verify configuration information.

1. `enable` — Enter Administration mode.
2. `Show system` — Display system information, such as system name, software version, date and time (including time zone), NTP server, DNS (name server), and management and HA interface IP addresses.
3. `Show IP route` — Display the system route table, if you added any routing information. (Optional)
4. `Show SNMP` — Display SNMP management configuration information for the Storage Router, if set. (Optional)
5. `Show admin` — Display contact information for the system administrator of the Storage Router, if set. (Optional)
6. `Show cluster` — Display cluster name and other cluster information, if you configured the Storage Router as a member of a cluster. (Optional)
7. `Show bootconfig` — Display the current boot configuration of the Storage Router. (Optional)
8. `Show runningconfig` — Display the current running configuration of the Storage Router. (Optional)

# Configuring VLAN

7

This chapter explains how to configure your Storage Router for a virtual local area network (VLAN) and contains the following sections:

You can configure for VLAN using CLI commands, as described in this chapter, or via the web-based GUI. To access the web-based GUI, point your browser to the Storage Router's management interface IP address. After logging on, click the Help link to access online help for the GUI.

## Prerequisite Tasks

Before configuring for VLAN, make sure you have configured all system parameters as described in Chapter 5, "Configuring the Storage Router" or Chapter 6, "Configuring System Parameters."

## VLAN Encapsulation

The Storage Router uses the IEEE 802.1Q standard for VLAN encapsulation.

**Note:** If the Storage Router is connected to a switch, the switch port must be configured as a trunk port and the encapsulation set to 802.1Q, not Inter-Switch Link (ISL), which is the default setting for trunk ports.

## Configuration Tasks

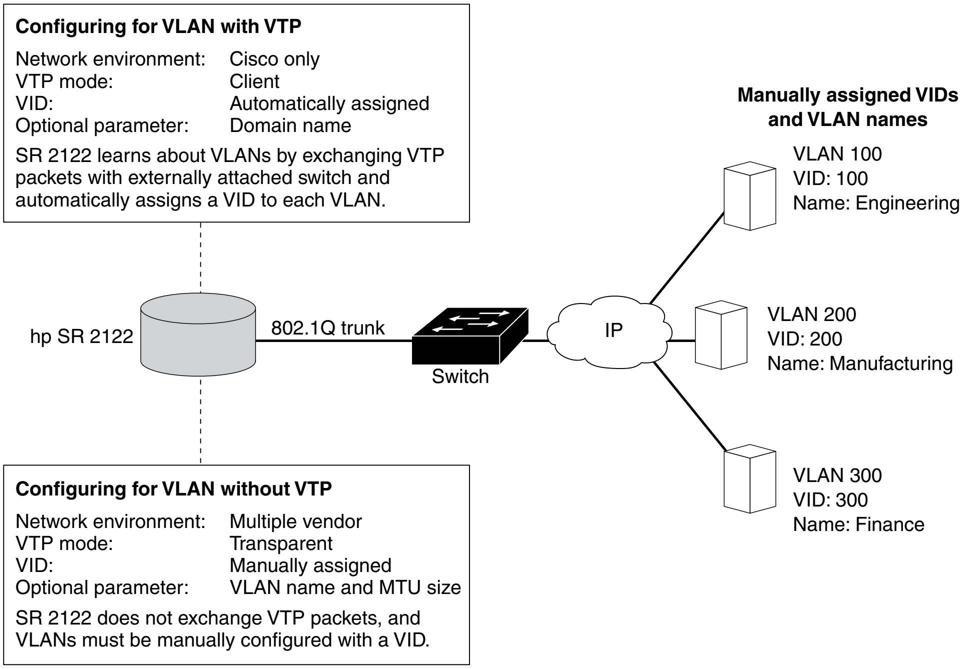
To configure for VLAN on the Storage Router:

1. Configure for VLAN using the VLAN Trunking Protocol (VTP) or Configure for VLAN without using VTP.
2. Configure an IP route.
3. Verify and save configuration.

**Note:** You can verify and save the configuration at any point in the process of performing the configuration tasks. Save your configuration by using the `save all bootconfig` CLI command. This command saves all configuration data to the bootable configuration, which is then used when the Storage Router is rebooted.

4. Proceed to Chapter 8, "Configuring SCSI Routing," to configure SCSI routing and to assign a VLAN to a SCSI routing instance.

Figure 39 contrasts configuring the Storage Router for VLAN with VTP and without VTP.



**Configuring for VLAN with VTP**

| | |
|---|---|
| Network environment: | Cisco only |
| VTP mode: | Client |
| VID: | Automatically assigned |
| Optional parameter: | Domain name |

SR 2122 learns about VLANs by exchanging VTP packets with externally attached switch and automatically assigns a VID to each VLAN.

**Configuring for VLAN without VTP**

| | |
|---|---|
| Network environment: | Multiple vendor |
| VTP mode: | Transparent |
| VID: | Manually assigned |
| Optional parameter: | VLAN name and MTU size |

SR 2122 does not exchange VTP packets, and VLANs must be manually configured with a VID.

Figure 39: Contrast of configuring for VLAN with VTP and without VTP

## Configuring for VLAN with VTP

Configuring for VLAN using the VLAN Trunking Protocol (VTP) consists of assigning the VTP domain name and setting the VTP mode to client. VTP, a proprietary protocol of Cisco Systems, is used to propagate VLAN information around a switched network.

Use the following procedure to configure VLAN using VTP:

**Note:** VTP can only be used in a Cisco network environment.

1. `enable` — Enter Administrator mode.
2. `vtp domain` *`opus`* — Assign a VTP domain name opus to which the Storage Router belongs. If a domain name is not specified, the Storage Router will assign itself to the first domain from which it receives a VTP message. The default setting is **none**.
3. `vtp mode` *`client`* — The default setting for the VTP mode is **client**. Set the VTP mode to **client** if the current setting is **transparent**.

   In client mode, the Storage Router will exchange VTP packets with an externally attached switch to learn about the VLANs that are accessible in the network.

**Note:** The VTP mode is a cluster-wide configuration item. When set by the user and saved, the mode setting becomes active on all storage routers in the cluster.

# Configuring for VLAN without VTP

Configuring for VLAN without using VTP consists of setting the VTP mode to transparent, assigning a VID, and optionally assigning a name and maximum transmission unit (MTU) size to the VLAN.

Use the following procedure to configure VLAN without using VTP:

1. `enable` — Enter Administrator mode.
2. `vtp mode` *`transparent`* — Set the VTP mode for the Storage Router to **transparent**. In transparent mode, the Storage Router does not exchange VTP packets, and VLANs must be manually configured. The default setting is **client**.

**Note:** The VTP mode is a cluster-wide configuration item. When set by the user and saved, the mode setting becomes active on all storage routers in the cluster.

3. `vlan` *`100`* `or vlan` *`100`* `name` *`Engineering`* `and mtusize` *`9000`* — Assign a VLAN identifier VID number that uniquely identifies the VLAN. The VID can be any integer from 1 to 4095.

   Optionally, a VLAN can be assigned a unique name **Engineering** up to 32 characters in length. If a name is not specified, a default name is **automatically assigned**. The default name has VLAN as the prefix followed by the VID, left padded to four bytes (for example, **VLAN0100**).

   Optionally, an MTU size can be specified using a value from 1500 to 9000. The default value is **1500**.

**Note:** VLANs are a cluster-wide configuration item. When set by the user and saved, the VLAN information is propagated to all storage routers in the cluster.

# Configuring an IP Route

Configuring an IP route to access the VLAN consists of specifying a static route that uses a gateway attached to the desired VLAN. Use the following procedure to configure an IP route.

1. `enable` — Enter Administration mode.
2. `ip route` *`10.2.90.285/32 10.2.10.233`*`, interface` *`ge2`*`, and VLAN` *`100`* — Specify the IP address and subnet mask 10.2.90.285/32 of the destination. Set the subnet mask to 255.255.255.255. In this example, the subnet mask was set using CIDR style /32.

   In addition, specify the gateway IP address 10.2.10.233, the interface name ge2, and the VID 100.

**Note:** To find the desired VID number, use the `show vlan` command. VIDs are listed in the VLAN column.

# Verifying and Saving Configuration

Verify VTP and VLAN operational and configuration information using the procedures that follow. You can save the configuration at any time by using the `save all bootconfig` command. You must save the running configuration to the bootable configuration for it to be retained in the Storage Router when it is rebooted. Once you have saved the configuration, you can verify that the configuration to be used when the Storage Router is rebooted matches the currently running configuration.

Use the following procedure to verify VTP operational information:

1. `enable` — Enter Administration mode.
2. `show vtp` — Display VTP operational information (Example 1).

   **Example 1: Verifying VTP Operational Information**

```
➔ [Storage Router]# show vtp
  Configuration Revision    : 8
  Number of existing VLANs : 4
  VTP Operating Mode        : Client
  VTP Domain Name           : opus
```

Use the following procedure to verify VTP configured settings.

1. `enable` — Enter Administration mode.
2. `show vtp config` — Display VTP configured settings (Example 2).

**Example 2: Verifying VTP Configured Settings**

```
➔ [Storage Router]# show vtp config
  vtp mode client
  vtp domain opus
```

Use the following procedure to verify current operational information for all VLANs either learned from the network using VTP in client mode or configured locally while in transparent mode.

1. `enable` — Enter Administration mode.
2. `show vtp` — Display current VLAN operational information (Example 3).

**Example 3: Verifying VLAN Operational Information**

```
➔ [Storage Router]# show vlan
  VLAN Name                             Status    Ports
  ---- -------------------------------- --------- -----
  100  Engineering                      active    ge2
  200  Manufacturing                    active    ge2

  VLAN Type  MTU   Interfaces
  ---- ----- ----- -------------------------------
  100  enet  1500  ge2VLAN100
  200  enet  1500  ge2VLAN200
```

Use the following procedure to verify configured VLAN information.

1. `enable` — Enter Administration mode.
2. `show vtp config` — Display VTP configured information (Example 4).

**Example 4: Verifying VLAN Configuration Information**

```
➔ [Storage Router]# show vlan config
  vlan 100 name Engineering mtu 1500
  vlan 200 name Manufacturing mtu 1500
```

## Assigning a VLAN to a SCSI Routing Instance

Assigning a VLAN to a SCSI routing instance is achieved with the `scsirouter serverif vlan` command. This procedure is provided in the "Configuring a Server Interface" section of Chapter 8, "Configuring SCSI Routing." HP recommends that you follow the configuration tasks to configure SCSI routing in the order given in that chapter at the time you are ready to configure SCSI routing.

# Configuring SCSI Routing

8

This chapter explains how to configure your Storage Router for SCSI routing and contains the following sections:

SCSI routing can be configured using CLI commands, as described in this chapter, or via the web-based GUI. To access the web-based GUI, point your browser to the Storage Router’s management interface IP address. After logging on, click the Help link to access online help for the GUI.

# Prerequisite Tasks

Before configuring SCSI routing, make sure you have configured all system parameters as described in Chapter 5, “Configuring the Storage Router” or Chapter 6 “Configuring System Parameters.”

If the VLAN service is to be used with the Storage Router, configure VLANs as described in Chapter 7, “Configuring for VLAN,” before proceeding.

# Configuration Tasks

To configure SCSI routing on your Storage Router:

1. Create a SCSI routing instance. Once an instance is created, you will configure that instance with parameters for a server interface, iSCSI targets, and access by IP hosts.
2. Configure the server interface with or without VLAN.
3. Configure iSCSI targets.
4. Configure an access list that identifies which IP hosts can access iSCSI targets configured as part of a SCSI routing instance. An access list is necessary if you want to specify access to iSCSI targets on a per-IP host basis. An access list is not necessary if you want to specify that all IP hosts have access to the iSCSI targets configured in a SCSI routing instance. (Optional)
5. Configure access. This identifies which IP hosts can access the iSCSI targets configured as part of a SCSI routing instance.
6. Verify and save configuration.

**Note:** Although this is shown as the last step, you can verify and save the configuration at any point in the process of performing the configuration tasks. Save your configuration by using the `save all bootconfig` CLI command. This command saves all configuration data to the bootable configuration, which is then used when the Storage Router is rebooted.

**Caution:** When making changes to a SCSI routing instance (such as adding or deleting targets or changing access) be sure to make the complementary changes to the iSCSI driver configuration of IP hosts that use that SCSI routing instance to access the storage resources. See the "Installing the iSCSI Drivers" section of Chapter 5, or the readme files for the appropriate iSCSI drivers for additional details. (You can access the latest iSCSI drivers and readme and example configuration files from http://www.hp.com/support).

Figure 40 illustrates SCSI routing configuration elements and Figure 41 illustrates the example configuration used in this chapter. Figure 42 illustrates how the configuration of SCSI routing instances determines VLAN access to storage devices.

**Note:** Configuring the SCSI routing instance does not include configuring the FC interfaces. Once the SCSI routing instance is configured, all the FC interfaces are available. For more information on the FC interfaces default characteristics, see the "Default Values For FC Interfaces" section on page 108.

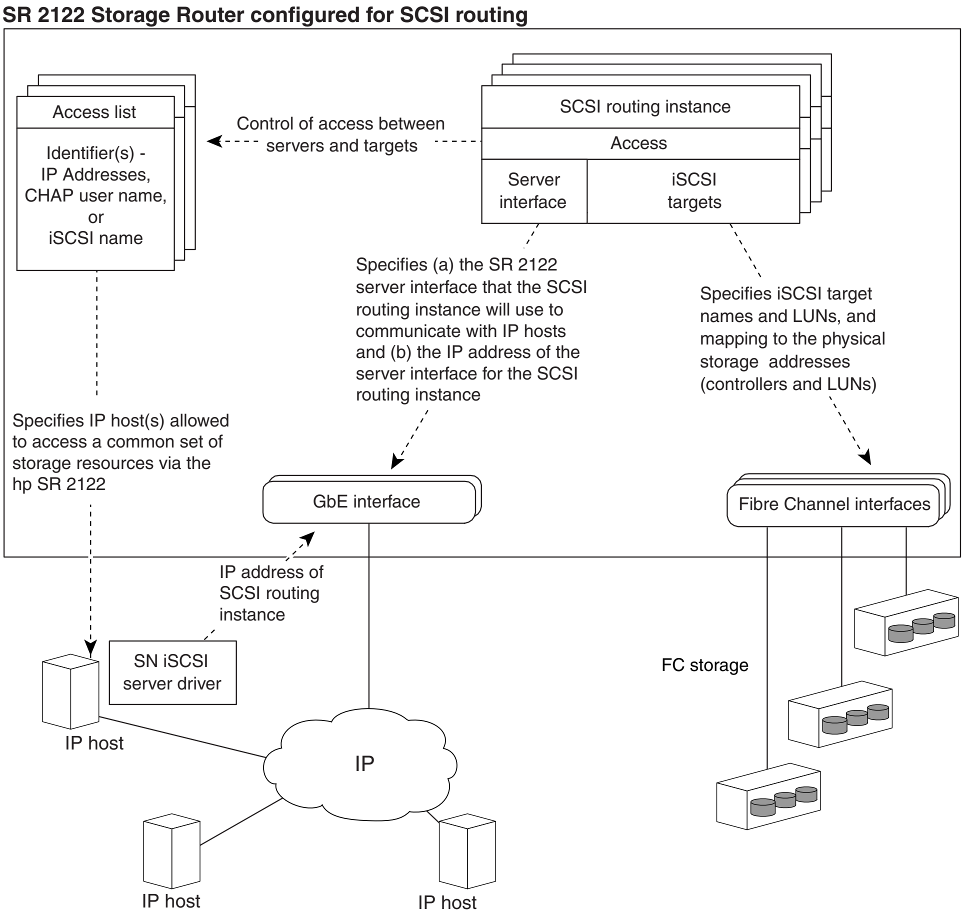

SR 2122 Storage Router configured for SCSI routing
Access list
Identifier(s) - IP Addresses, CHAP user name, or iSCSI name
Control of access between servers and targets
SCSI routing instance
Access
Server interface
iSCSI targets
Specifies (a) the SR 2122 server interface that the SCSI routing instance will use to communicate with IP hosts and (b) the IP address of the server interface for the SCSI routing instance
Specifies iSCSI target names and LUNs, and mapping to the physical storage addresses (controllers and LUNs)
Specifies IP host(s) allowed to access a common set of storage resources via the hp SR 2122
GbE interface
Fibre Channel interfaces
IP address of SCSI routing instance
SN iSCSI server driver
FC storage
IP host
IP
IP host
IP host

Figure 40: Configuration elements for SCSI routing

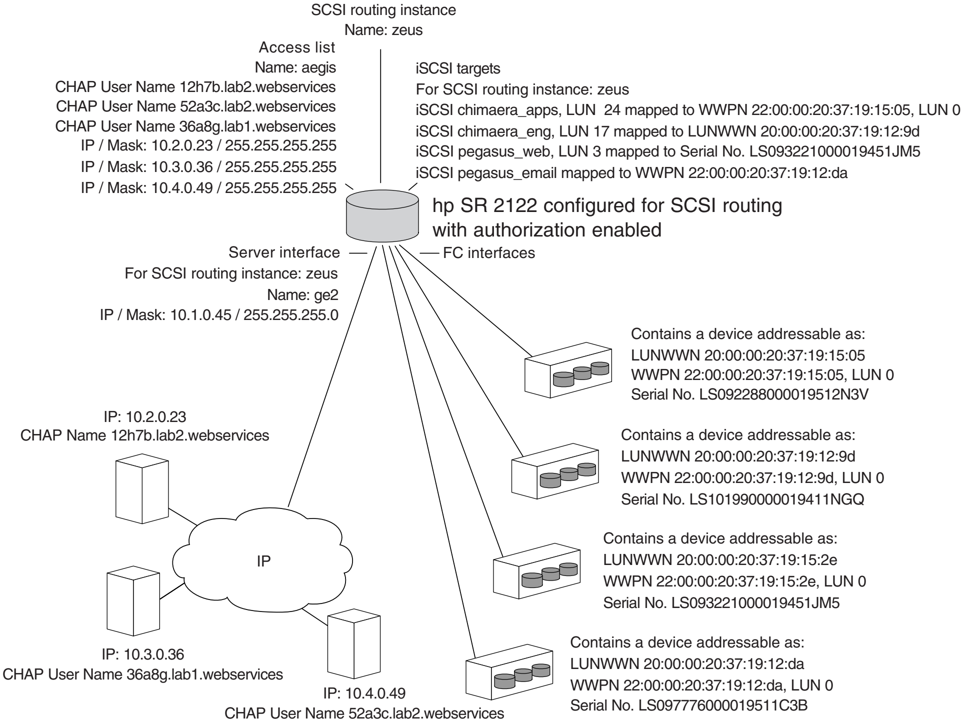

SCSI routing instance
Name: zeus
Access list
Name: aegis
CHAP User Name 12h7b.lab2.webservices
CHAP User Name 52a3c.lab2.webservices
CHAP User Name 36a8g.lab1.webservices
IP / Mask: 10.2.0.23 / 255.255.255.255
IP / Mask: 10.3.0.36 / 255.255.255.255
IP / Mask: 10.4.0.49 / 255.255.255.255
iSCSI targets
For SCSI routing instance: zeus
iSCSI chimaera_apps, LUN 24 mapped to WWPN 22:00:00:20:37:19:15:05, LUN 0
iSCSI chimaera_eng, LUN 17 mapped to LUNWWN 20:00:00:20:37:19:12:9d
iSCSI pegasus_web, LUN 3 mapped to Serial No. LS093221000019451JM5
iSCSI pegasus_email mapped to WWPN 22:00:00:20:37:19:12:da
hp SR 2122 configured for SCSI routing
with authorization enabled
Server interface
For SCSI routing instance: zeus
Name: ge2
IP / Mask: 10.1.0.45 / 255.255.255.0
FC interfaces
Contains a device addressable as:
LUNWWN 20:00:00:20:37:19:15:05
WWPN 22:00:00:20:37:19:15:05, LUN 0
Serial No. LS092288000019512N3V
IP: 10.2.0.23
CHAP Name 12h7b.lab2.webservices
Contains a device addressable as:
LUNWWN 20:00:00:20:37:19:12:9d
WWPN 22:00:00:20:37:19:12:9d, LUN 0
Serial No. LS101990000019411NGQ
Contains a device addressable as:
LUNWWN 20:00:00:20:37:19:15:2e
WWPN 22:00:00:20:37:19:15:2e, LUN 0
Serial No. LS093221000019451JM5
IP
Contains a device addressable as:
LUNWWN 20:00:00:20:37:19:12:da
WWPN 22:00:00:20:37:19:12:da, LUN 0
Serial No. LS097776000019511C3B
IP: 10.3.0.36
CHAP User Name 36a8g.lab1.webservices
IP: 10.4.0.49
CHAP User Name 52a3c.lab2.webservices

**Figure 41: SCSI routing parameters example configuration**

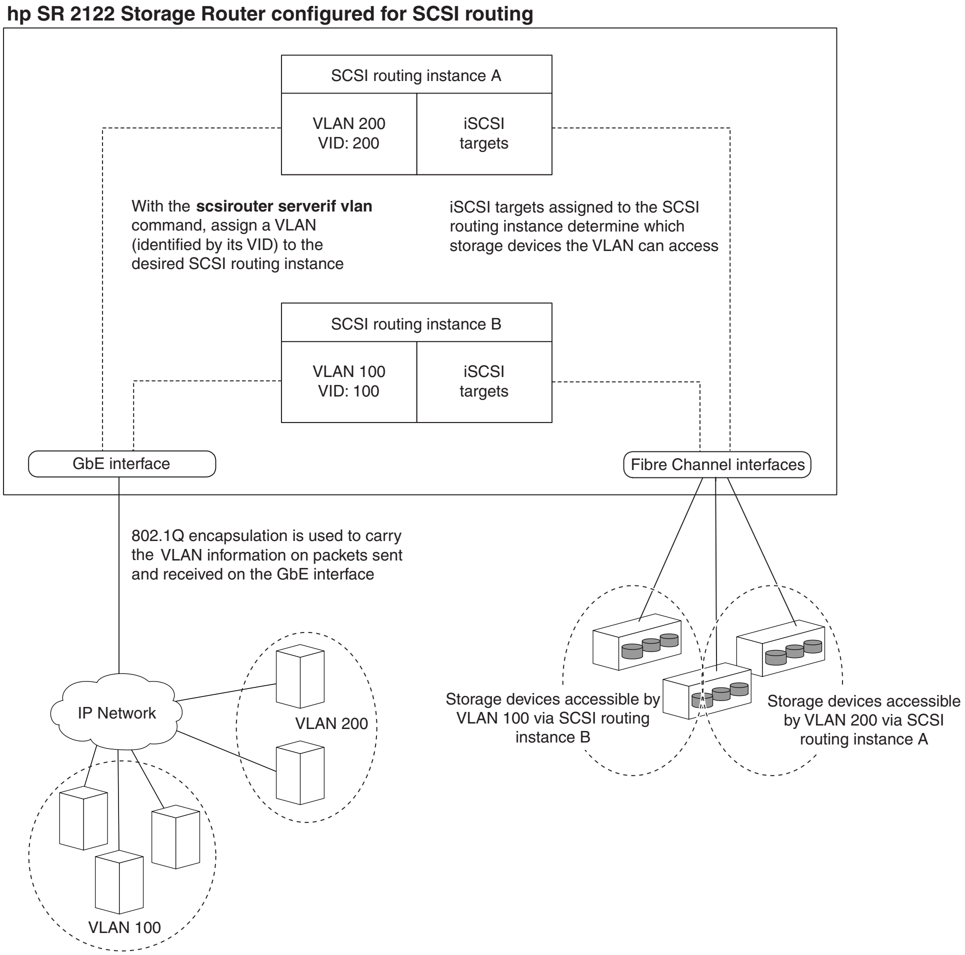

hp SR 2122 Storage Router configured for SCSI routing
SCSI routing instance A
VLAN 200
VID: 200
iSCSI
targets
With the **scsirouter serverif vlan** command, assign a VLAN (identified by its VID) to the desired SCSI routing instance
iSCSI targets assigned to the SCSI routing instance determine which storage devices the VLAN can access
SCSI routing instance B
VLAN 100
VID: 100
iSCSI
targets
GbE interface
Fibre Channel interfaces
802.1Q encapsulation is used to carry the VLAN information on packets sent and received on the GbE interface
IP Network
VLAN 200
VLAN 100
Storage devices accessible by VLAN 100 via SCSI routing instance B
Storage devices accessible by VLAN 200 via SCSI routing instance A

**Figure 42: Configuration of SCSI routing determines VLAN access to storage**

# Creating a SCSI Routing Instance

Creating a SCSI routing instance consists of naming the new instance. Use the following procedure to create a SCSI routing instance:

1. `enable` — Enter Administration mode.
2. `SCSIRouter` *`zeus`* — Create a SCSI routing instance by naming the new instance **zeus**.

---

**Note:** You can define up to 12 instances on a single Storage Router or across a cluster. For additional details about configuring storage router clusters for high availability, see Chapter 10, "Configuring a High Availability Cluster."

---

# Configuring a Server Interface

Configuring a server interface consists of assigning a server interface along with an IP address and subnet mask to the desired SCSI routing instance. If the Storage Router is to be used with VLAN, specify the VLAN by its VID.

## Without VLAN

Use the following procedure to configure a server interface for a SCSI routing instance:

1. `enable` — Enter Administration mode.
2. `SCSIRouter` *`zeus`* `serverif` *`ge2`* `VLAN` *`100 10.1.0.45/24`* — Assign a server interface `ge2` to the desired SCSI routing instance **zeus**. Specify the IP address and subnet mask **10.1.0.45/24** that IP hosts will use to access the SCSI routing instance. In this example, the subnet mask of **255.255.255.0** was set using CIDR style **/24**.

## With VLAN

Use the following procedure to assign a server interface and VLAN to a SCSI routing instance:

1. `enable` — Enter Administration mode.
2. `SCSIRouter` *`zeus`* `serverif` *`ge2`* `VLAN` *`100 10.1.0.45/24`* — Assign a VLAN, identified by its VID **100**, to the desired SCSI routing instance **zeus**. Specify the server interface **ge2** and the IP address and subnet mask **10.1.0.45/24** that the VLAN will use to access the SCSI routing instance. In this example, the subnet mask of **255.255.255.0** was set using CIDR style **/24**.

**Note:** To look up the VID, use the `show vlan` command. VIDs are listed in the VLAN column.

# Configuring iSCSI Targets

Configuring iSCSI targets consists of specifying the SCSI routing instance to which an iSCSI target is to be assigned, specifying the iSCSI target, and mapping the iSCSI target to a physical storage device. When assigning an iSCSI target, you can specify the physical storage device either by physical storage address, serial number, or by an index number assigned to the device.

**Note:** When a new iSCSI target is configured, IP hosts do not have access to it. You need to configure access to newly created iSCSI targets according to the "Configuring Access" section later in this chapter.

Use the procedures that follow according to mapping type and storage addressing type:

- Target-and-LUN mapping using WWPN addressing, page 99
- Target-and-LUN mapping using LUNWWN addressing, page 100
- Target-and-LUN mapping using Serial Number addressing, page 101
- Target-only mapping using WWPN addressing, page 101

### Example 5: Indexed List of Storage Devices

```
id interface lunwwn           wwpn             tgtid lun vendor  product    serial number
1  fc4       20000020371912d5 22000020371912d5 n/a   0   DEC     HSG80      LS099969000019511C2H
2  fc4       20000020371912da 22000020371912da n/a   0   DEC     HSG80      LS097776000019511C3B
3  fc4       200000203719129d 220000203719129d n/a   0   DEC     HSG80CCL   LS101990000019411NGQ
4  fc4       2000002037191505 2200002037191505 n/a   0   COMPAQ  MSA1000    LS101990000019451JM5
5  fc4       20000020371912b2 22000020371912b2 n/a   0   COMPAQ  MSA1000    LS099843000019430RC7
6  fc4       200000203719152e 220000203719152e n/a   0   COMPAQ  MSA1000    LS093221000019451JM5
```

## Target-and-LUN mapping using WWPN addressing

Use the following procedure to map iSCSI targets to storage devices by physical storage address:

1. `enable` — Enter Administration mode.
2. `SCSIRouter` *`zeus`* `target` *`chimaera_apps`* `LUN` *`24`* `WWPN` *`22:00:00:20:37:19:15:05`* `LUN` *`0`* — Specify desired SCSI routing instance **zeus**. Specify iSCSI target **chimaera_apps** and LUN **24**, and map it to the desired physical address WWPN **22:00:00:20:37:19:15:05** LUN **0**.

Use the following procedure to map iSCSI targets to storage devices by an index number:

1. `enable` — Enter Administration mode.
2. `SCSIRouter` *`zeus`* `target` *`chimaera_apps`* `LUN` *`31`* `WWPN` *`#?`* — Specify desired SCSI routing instance **zeus**. Specify iSCSI target **chimaera_apps** and LUN **31**, and prompt for an indexed list of available storage addresses using the number sign and a question mark **#?**.
3. `SCSIRouter` *`zeus`* `target` *`chimaera_apps`* `LUN` *`31`* `WWPN` *`#4`* — Choose a physical address designated by an index number (see index number 4 in Example 5) to map the iSCSI target **chimaera_apps** and LUN **31** combination to the desired physical address WWPN **22:00:00:20:37:19:15:05**, LUN **0**.

## Target-and-LUN mapping using LUNWWN addressing

Use the following procedure to map iSCSI targets to storage devices by physical storage address:

1. `enable` — Enter Administration mode.
2. `SCSIRouter` *`zeus`* `target` *`chimaera_apps`* `LUN` *`17`* `LUNWWN` *`22:00:00:20:37:19:12:9d`* — Specify desired SCSI routing instance **zeus**. Specify iSCSI **target chimaera_apps** and LUN **17**, and map it to the desired physical address LUNWWN **22:00:00:20:37:19:12:9d**.

Use the following procedure to map iSCSI targets to storage devices by an index number:

1. `enable` — Enter Administration mode.
2. `SCSIRouter` *`zeus`* `target` *`chimaera_apps`* `LUN` *`17`* `WWPN` *`#?`* — Specify desired SCSI routing instance **zeus**. Specify iSCSI target **chimaera_apps** and LUN **17**, and prompt for an indexed list of available storage addresses using the number sign and a question mark **#?**.
3. `SCSIRouter` *`zeus`* `target` *`chimaera_apps`* `LUN` *`17`* `LUNWWN` *`#3`* — Choose a physical address designated by an index number (see index number 3 in Example 5) to map the iSCSI target **chimaera_apps** and LUN **17** combination to the desired physical address LUNWWN **22:00:00:20:37:19:12:9d**.

## Target-and-LUN mapping using Serial Number addressing

Use the following procedure to map iSCSI targets to storage devices by serial number:

1. `enable` — Enter Administration mode.
2. `SCSIRouter` *`zeus`* `target` *`pegasus_web`* `LUN` *`3`* `serial number` *`LS093221000019451JM5`* — Specify desired SCSI routing instance **zeus**. Specify iSCSI target **pegasus_web** and LUN **3**, and map it to the desired serial number **LS093221000019451JM5**.

Use the following procedure to map iSCSI targets to storage devices by an index number:

1. `enable` — Enter Administration mode.
2. `SCSIRouter` *`zeus`* `target` *`pegasus_web`* `LUN` *`3`* `serial number` *`#?`* — Specify desired SCSI routing instance **zeus**. Specify iSCSI target **pegasus_web** and LUN **3**, and prompt for an indexed list of available storage addresses using the number sign and a question mark **#?**.
3. `SCSIRouter` *`zeus`* `target pegasus_web LUN` *`3`* `serial number` *`#6`* — Choose a physical address designated by an index number (see index number 6 in Example 5) to map the iSCSI target **pegasus_web** and LUN **3** combination to the desired physical address serial number **LS093221000019451JM5**.

## Target-only mapping using WWPN addressing

Use the following procedure to map iSCSI targets to storage devices by physical storage address:

1. `enable` — Enter Administration mode.
2. `SCSIRouter` *`zeus`* `target` *`pegasus_email`* `WWPN` *`22:00:00:20:37:19:12:da`* — Specify desired SCSI routing instance **zeus**. Specify iSCSI target **pegasus_email**, and map it to the desired physical address WWPN **22:00:00:20:37:19:12:da** and any LUNs available as part of that WWPN.

Use the following procedure to map iSCSI targets to storage devices by index numbers:

1. `enable` — Enter Administration mode.
2. `SCSIRouter` *`zeus`* `target` *`pegasus_email`* `WWPN` *`#?`* — Specify desired SCSI routing instance **zeus**. Specify iSCSI target **pegasus_email** and prompt for an indexed list of available storage addresses using the number sign and a question mark **#?**.
3. `SCSIRouter` *`zeus`* `target` *`pegasus_email`* `WWPN` *`#2`* — Choose a physical address designated by an index number (see index number 2 in Example 5) to map the iSCSI target **pegasus_email** to the desired physical address WWPN **22:00:00:20:37:19:12:da**.

## Configuring an Access List

Configuring an access list consists of creating an access list by naming it and identifying the IP hosts that have permission to access storage devices via iSCSI target names. IP hosts can be identified by:

- IP address
- CHAP user name (used for iSCSI authentication)
- iSCSI name of the IP host - The iSCSI name is a UTF-8 character string based on iSCSI functional requirements. It is a location-independent permanent identifier for an iSCSI node, and is generated when a target is initially created.

An access list can contain one or more types of identification entries. If an identification entry type exists in the access list, the IP host attempting to access the associated storage target must have a matching entry defined in the access list. For example, if an access list contains both IP address and iSCSI name identification entry types, then every IP host that requires access to the associated set of storage resources must have a matching IP address and iSCSI name entry in the access list.

An access list is necessary if you want to specify access to iSCSI targets on a per-IP host basis. An access list is not necessary if you want to specify that all IP hosts have access to the iSCSI targets configured in a SCSI routing instance.

**Note:** If there is a CHAP user name entry in the access list, the SCSI routing instance used to access the storage target must also have iSCSI authentication enabled. See Chapter 9, "Configuring Authentication," for additional information about AAA and iSCSI authentication.

Use the following procedure to create an access list. In this procedure, the access list is called **aegis** and the IP host identifiers include three IP addresses (**10.2.0.23**, **10.3.0.36**, and **10.4.0.49**) and a CHAP-username (**12h7b.lab2.webservices**):

1. `enable` — Enter Administration mode.
2. `accesslist` *`aegis`* — Create an access list by naming it **aegis**. There is a 31 character limit.
3. `accesslist` *`aegis`* `description` *`"Access to zeus SCSI routing service"`* — Add a string as a description for the access list. Enclose the string using single or double quotes. (Optional)
4. `accesslist` *`aegis 10.2.0.23/32 10.3.0.36/32 10.4.0.49/32`* — Add IP addresses of IP hosts to the access list. Separate multiple IP addresses with a space. To limit the access to each IP address, set the subnet mask to **255.255.255.255**. In this example, the subnet mask was set using CIDR style **/32**.
5. `accesslist` *`aegis`* `CHAP-username` *`12h7b.lab2.webservices`* — Add CHAP-usernames in the access list. To limit the access to each CHAP-username. The password it supplies must be successfully validated using the AAA method configured.

**Note:** Authentication must be enabled when using CHAP-usernames in the access list.

**Note:** In a cluster environment, all access lists must be created and maintained on the first Storage Router to join the cluster. If you issue the `accesslist` commands from another Storage Router in the cluster, the CLI displays an informational message with the IP address of the Storage Router that is currently handling all access list functions. For more information on operating the Storage Router in a cluster, see Chapter 11, "Maintaining and Managing the Storage Router."

# Configuring Access

Configuring access consists of specifying which iSCSI targets can be accessed by IP hosts. When configuring access, you can specify one iSCSI target at a time or all iSCSI targets. Similarly, you can specify one access list at a time or all IP hosts using a SCSI routing instance. In addition, you can deny access to iSCSI targets one at a time or all at once.

The default for access to newly configured iSCSI targets is none. You must configure access according to the information provided in this section.

Use the procedures that follow according to the type of access:

- Access an iSCSI target by IP hosts identified in an access list, page 104
- Access an iSCSI target by all IP hosts, page 105
- Access all iSCSI targets by IP hosts identified in an access list, page 105
- Access all iSCSI targets by all IP hosts, page 105
- Access denied to one iSCSI target, page 105
- Access denied to all iSCSI targets, page 106

## Access an iSCSI target by IP hosts identified in an access list

Use the following procedure to specify one iSCSI target at a time to be accessible by IP hosts listed in an access list:

1. `enable` — Enter Administration mode.
2. `SCSIRouter` *`zeus`* `target` *`chimaera_email`* `accesslist` *`aegis`* — Specify that an iSCSI target **chimaera_email**, configured as part of a SCSI routing instance **zeus**, can be accessed by IP hosts listed in an access list **aegis**.

## Access an iSCSI target by all IP hosts

Use the following procedure to specify one iSCSI target at a time to be accessible by all IP hosts.:

1. `enable` — Enter Administration mode.
2. `SCSIRouter` *`zeus`* `target` *`chimaera_apps`* `accesslist` *`all`* — Specify that an iSCSI target **chimaera_apps**, configured as part of a SCSI routing instance **zeus**, can be accessed by **all** IP hosts.

## Access all iSCSI targets by IP hosts identified in an access list

Use the following procedure to specify all iSCSI targets to be accessible by IP hosts listed in an access list:

1. `enable` — Enter Administration mode.
2. `SCSIRouter` *`zeus`* `target` *`all`* `accesslist` *`aegis`* — Specify that **all** iSCSI targets that were configured as part of a SCSI routing instance **zeus**, can be accessed by IP hosts listed in an access list **aegis**.

## Access all iSCSI targets by all IP hosts

Use the following procedure to specify all iSCSI targets to be accessible by all IP hosts:

1. `enable` — Enter Administration mode.
2. `SCSIRouter` *`zeus`* `target` *`all`* `accesslist` *`all`* — Specify that **all** iSCSI targets that were configured as part of a SCSI routing instance **zeus** can be accessed by **all** IP hosts.

## Access denied to one iSCSI target

Use the following procedure to deny access by IP hosts to one iSCSI target at a time:

1. `enable` — Enter Administration mode.
2. `SCSIRouter zeus target` *`chimaera_apps`* `accesslist` *`none`* — Specify that **no** IP host can access the iSCSI target **chimaera_apps**, configured as part of the specified SCSI routing instance **zeus**.

## Access denied to all iSCSI targets

Use the following procedure to deny access by all IP hosts to all iSCSI targets at once:

1. `enable` — Enter Administration mode.
2. `SCSIRouter` *`zeus`* `target` *`all`* `accesslist` *`none`* — Specify that **no** IP hosts can access **any** iSCSI targets that were configured as part of the specified SCSI routing instance **zeus**.

## Verifying and Saving Configuration

Verify the access list configuration and the SCSI routing configuration using the procedures that follow. You can save the configuration at any time by using the `save all bootconfig` command. You must save the running configuration to the bootable configuration for it to be retained in the Storage Router when it is rebooted. Once you have saved the configuration, you can verify that the configuration to be used when the Storage Router is rebooted matches the currently running configuration.

Use the following procedure to verify access list configuration:

1. `enable` — Enter Administration mode.
2. `Show accesslist` — Display a list of all existing access lists (Example 6).
3. `Show accesslist` *`aegis`* — Display the IP host identifies in an access list (Example 7).

### Example 6: Verifying Existence of an Access List

```
➔ [SR2122]# show accesslist
aegis
hris-mgmt
```

### Example 7: Verifying IP Addresses in an Access List Named aegis

```
➔ [SR2122]# show accesslist aegis
accesslist aegis description "Access to zeus SCSI routing service"
accesslist aegis 10.2.0.23/255.255.255.255
accesslist aegis 10.3.0.36/255.255.255.255
accesslist aegis 10.4.0.49/255.255.255.255
accesslist aegis chap-username 12h7b.lab2.webservices
```

Use the following procedure to verify the configuration of a SCSI routing instance:

1. `enable` — Enter Administration mode.
2. `Show scsirouter` *`zeus`* — Display the parameters configured for the specified SCSI routing instance (Example 8).

### Example 8:  Verifying Configuration for a SCSI Routing Instance

```
➔ [SR2122]# show scsirouter zeus
zeus description "(not set)"
zeus authenticate "none"
zeus primary "none"
zeus proxy server disabled
zeus failover primary "none"
zeus failover secondary "none"
zeus target naming authority "none"
zeus target log level is not available
zeus target chimaera_apps description "(not set)"
zeus target chimaera_apps Name "iqn.1987-05.com.hp.00.d3f8a650c7deacecd97e1812d.chimaera_"
zeus target chimaera_apps enabled "TRUE"
zeus target chimaera_apps accesslist "all"
zeus target chimaera_apps lun 24 wwpn "22:00:00:20:37:19:15:05" lun "0" I/F fci1
zeus target chimaera_eng description "(not set)"
zeus target chimaera_eng enabled "TRUE"
zeus target chimaera_eng accesslist "all"
zeus target chimaera_eng lun 17 lunwwn "22:00:00:20:37:19:12:9d" I/F fci1
zeus target pegasus_web description "(not set)"
zeus target pegasus_web Name
"iqn.1987-05.com.hp.00.d6bf2b11ed9c88ce9299ea3f0961ad94.pegasus_web"
zeus target pegasus_web enabled "TRUE"
zeus target pegasus_web accesslist "all"
zeus target pegasus_web lun 3 serial "LS0932210000019451JM5" I/F fci1
```

## Default Values For FC Interfaces

The following are the default operational characteristics for the Fibre Channel interfaces 1 and 2:

- Fairness disabled (switch has priority)
- Fabric Address Notification (FAN) enabled
- Automatically negotiated transfer rate (linkspeed auto)
- Multi-Frame sequence bundling enabled
- Automatic selection of port type as:
  - auto - Port type is gl-port
  - e-port - Port type is switch to switch
  - f-port - Port type is Fabric
  - fl-port - Port type is Fabric Loop (public loop)
  - g-port - Port type is Generic either f-port or e-port
  - gl-port - Port type is Generic Loop either fl-port, e-port, or g-port
  - tl-port - Port type is Translated Loop

# Configuring Authentication

9

This chapter explains how to configure the authentication portion of HP authentication, authorization and accounting (AAA) methods on the Storage Router, and how to enable iSCSI authentication, which uses the AAA authentication methods.

The following tasks are covered:

The AAA authentication function is always enabled for the Storage Router; it cannot be disabled.

Authentication parameters can be configured using CLI commands, as described in this chapter, or via the web-based GUI. To access the web-based GUI, point your browser to the Storage Router's management interface IP address. After logging on, click the Help link to access online help for the GUI.

## Prerequisite Tasks

Before performing AAA and iSCSI authentication configuration tasks on the Storage Router, make sure you have configured system parameters as described in Chapter 5, "Configuring the Storage Router," or Chapter 6, "Configuring System Parameters." If the Storage Router is deployed for SCSI routing, you should also configure SCSI routing instances as described in Chapter 8, "Configuring SCSI Routing," before proceeding.

**Note:** AAA and iSCSI authentication configuration settings are system-wide parameters and are not shared across a cluster. However, you may prefer to configure all storage routers in a cluster with the same authentication settings.

## Using iSCSI Authentication

iSCSI authentication provides a mechanism to authenticate all IP hosts that request access to storage via a SCSI routing instance. When enabled, iSCSI drivers provide user name and password information each time an iSCSI TCP connection is established. iSCSI authentication uses the iSCSI CHAP (Challenge Handshake Authentication Protocol) authentication method. Authentication services are provided by the AAA subsystem configured for each Storage Router.

Authentication, authorization and accounting (AAA) is Cisco's architectural framework for configuring a set of three independent security functions in a consistent, modular manner. The Storage Router implements the authentication function.

Authentication provides a method of identifying users (including login and password dialog, challenge and response, and messaging support) prior to receiving access to the requested object, function, or network service. AAA authentication is configured by defining a list of authentication services. iSCSI authentication, which uses the AAA authentication services list, can be enabled for specific SCSI routing instances.

# AAA Security Services

iSCSI authentication uses AAA security services to administer its security functions. If you are using remote security servers, AAA is the means through which you establish communications between the Storage Router and the remote RADIUS or TACACS+ security server.

This chapter describes how to configure the following AAA security services:

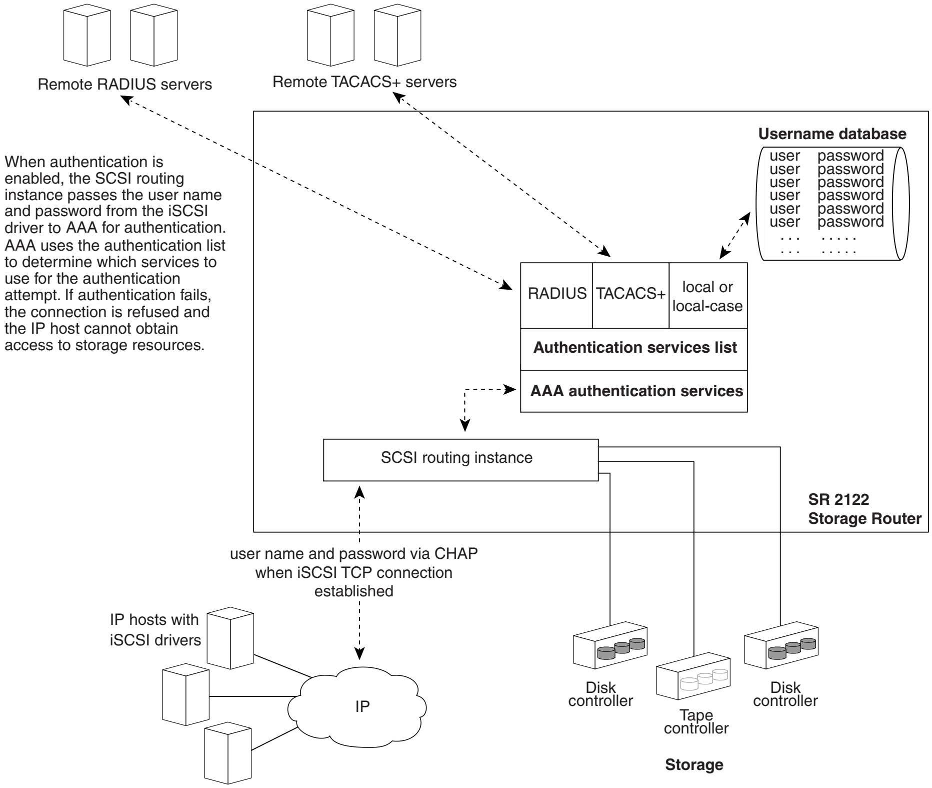
- RADIUS is a distributed client/server system implemented through AAA that secures networks against unauthorized access. In this implementation, the Storage Router sends authentication requests to a central RADIUS server that contains all user authentication and network service access information.
- TACACS+ is a security application implemented through AAA that provides centralized validation of users attempting to gain access to storage targets through specified SCSI routing instances. TACACS+ services are maintained in a database on a TACACS+ daemon running, typically, on a UNIX or Windows NT workstation. TACACS+ provides for separate and modular authentication, authorization, and accounting facilities.
- Local or local-case uses a local username database on the Storage Router for authentication. Local-case indicates that the user name authentication is case-sensitive. Password authentication is always case-sensitive.

# Configuration Tasks

To configure iSCSI authentication and the associated AAA authentication services on the Storage Router:

1. Configure the desired security services, such as RADIUS, TACACS+, or the local username database.
2. Build the AAA authentication list.
3. Test the iSCSI authentication services.
4. Enable iSCSI authentication for individual SCSI routing instances.
5. Verify and save AAA and iSCSI authentication configuration.

Figure 43 illustrates AAA authentication configuration elements and Figure 44 illustrates the example configuration of iSCSI authentication and AAA authentication services used in this chapter.



When authentication is enabled, the SCSI routing instance passes the user name and password from the iSCSI driver to AAA for authentication. AAA uses the authentication list to determine which services to use for the authentication attempt. If authentication fails, the connection is refused and the IP host cannot obtain access to storage resources.

**Figure 43: iSCSI authentication configuration elements**

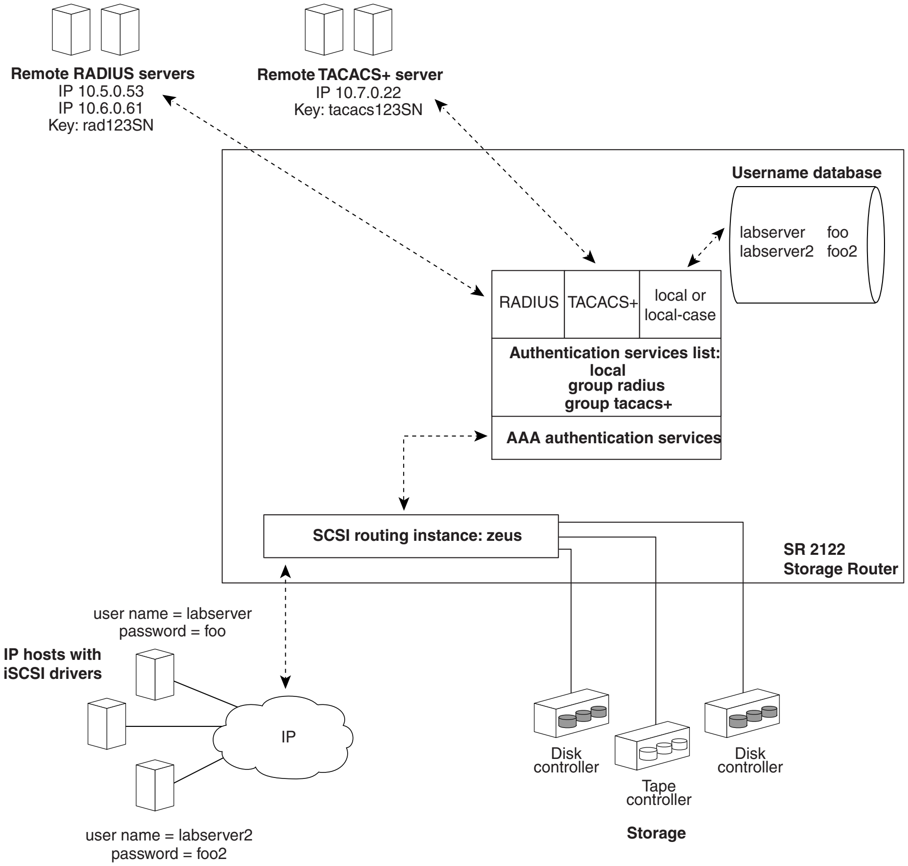


**Figure 44: iSCSI authentication example configuration**

# Configuring Security Services

Configuring security services consists of setting the appropriate parameters for the various service options that can be used by the Storage Router. The Storage Router can use any or all of the supported security services.

Use the procedures that follow to configure the Storage Router to use the appropriate security services:

- RADIUS Servers, page 114
- TACACS+ Hosts, page 115
- Local Username Database, page 115

## RADIUS Servers

Use the commands in the following procedure to configure RADIUS security services:

1. `enable` — Enter Administrator mode.
2. `radius-server host` *`10.5.0.53`* — Specify the RADIUS server to be used for AAA authentication services. For example, specify the RADIUS server at **10.5.0.53** for use by the Storage Router. Because no port is specified, the authentication requests use the default UDP port 1645. Global timeout and retransmit values are also used.
3. `radius-server host` *`10.6.0.61`* — Specify a secondary RADIUS server. RADIUS servers are accessed in the order in which they are defined. For example, specify the RADIUS server at **10.6.0.61** as the second RADIUS server to be used for AAA authentication services.
4. `radius-server key` *`rad123SN`* — Configure the global authentication and encryption key to be used for all RADIUS communications between the Storage Router and the RADIUS daemon. For example, set the key to **rad123SN**. This key must match the key used on the RADIUS daemon.

## TACACS+ Hosts

Use the commands in the following procedure to configure TACACS+ security services:

1. `enable` — Enter Administrator mode.
2. `tacacs-server host` *`10.7.0.22`* — Specify the TACACS+ server to be used for AAA authentication services. For example, specify the TACACS+ server at **10.7.0.22** for use by the Storage Router. Because no port is specified, the authentication requests use the default port **49**. The global timeout value is also used.
3. `tacacs-server key` *`tacacs123SN`* — Configure the global authentication and encryption key to be used for all TACACS+ communications between the Storage Router and the TACACS+ server. For example, set the key to **tacacs123SN**. This key must match the key used by the TACACS+ daemon.

## Local Username Database

Use the commands in the following procedure to configure a local username database:

**Note:** Passwords are entered in clear text, but are changed to "XXXXX" in the CLI command history cache, and are stored in the local username database in encrypted format.

1. `enable` — Enter Administrator mode.
2. `username` *`labserver`* `password foo username` *`labserver2`* `password` *`foo2`* — Enter a user name and password for each device requiring authentication prior to access to storage. For example, add the following user name and password combinations:
   - `labserver` and `foo`
   - `labserver2` and `foo2`

   User name and password pairs must match the user name and password pairs configured for the iSCSI drivers that require access to storage via the SCSI routing instances that have iSCSI authentication enabled. If other authentication services are also used (such as RADIUS or TACACS+), these user name and password pairs must also be configured within the databases those services use for authentication purposes.

The following rules apply to passwords:

- Passwords are entered in clear text. However, they are stored in an encrypted format.
- If the password contains embedded spaces, enclose it with single or double quotes.
- After initial entry, passwords display in their encrypted format. Use the `show aaa` command to display the local username database entries. The following is an example display:

  ```
  username "foo" password "9 ea9bb0c57ca4806d3555f3f78a4204177a"
  ```

---

**Note:** The first *"9"* in the example display indicates that the password is encrypted.

---

- You can re-enter an encrypted password using the normal `username password` command. Enter the encrypted password in single or double quotes, starting with 9 and a single space. For example, copying and pasting password `"9 ea9bb0c57ca4806d3555f3f78a4204177a"` from the example above into the `username pat` command would create an entry for `pat` in the username database. The user named `pat` would have the same password as the user named `foo`. This functionality allows user names and passwords to be restored from saved configuration files.
- When entering a password, a zero followed by a single space indicates that the following string is not encrypted; 9 followed by a single space indicates that the following string is encrypted. To enter a password that starts with 9 or zero, followed by one or more spaces, enter a zero and a space and then enter the password string. For example, to enter the password "`0 123`" for the user named `pat`, enter this command:

  ```
  username pat password "0 0 123"
  ```

  To enter the password "`9 73Zjm 5`" for user name `lab1`, use this command:

  ```
  username lab1 password "0 9 73Zjm 5"
  ```

# Building the AAA Authentication List

iSCSI authentication uses a list of defined AAA authentication services to administer its security functions. The list that is created must be named *default*.

Use the commands in the following procedure to build a list of AAA authentication services to be used for iSCSI authentication:

1. `enable` — Enter Administrator mode.
2. `aaa authentication iscsi` *`default`* `local group radius group tacacs+` — Create a list (named **default**) of authentication services. For example, build a list so that AAA first tries to perform authentication using the local username database. If AAA fails to find a user name match, an attempt is made to contact a RADIUS server. If no RADIUS server is found, RADIUS returns an error and AAA tries to use a TACACS+ server. If no TACACS+ server is found, TACACS+ returns an error and AAA authentication fails. If a RADIUS or TACACS+ server does not find a user name and password match, authentication fails and no other methods are attempted.

**Note:** If local or local-case is the first service in the authentication list and a user name match is not found, the next service in the list will be tried. If local or local-case is not the first service, authentication fails if a user name match is not found. Authentication always fails if a RADIUS or TACACS+ server fails to find a user name match.

# Testing iSCSI Authentication

Before enabling iSCSI authentication for a SCSI routing instance, you can test iSCSI authentication from the Storage Router. The user name and password are passed to AAA authentication, which performs authentication using the iSCSI default authentication list. The command response indicates a pass or fail status.

Use the commands in the following procedure to test iSCSI authentication:

1. `enable` — Enter Administrator mode.
2. `aaa test authentication iscsi default` *`labserver foo`* and `aaa test authentication iscsi default` *`labserver2 foo2`* — Test the user names and passwords listed in the username database. AAA authentication uses the services in the default list for authentication (Example 9).

**Example 9: Testing Authentication**

```
➔ *[SR2122-MG1]# aaa test authentication iscsi default labserver foo

  Sep 02 14:37:00:aaa:AS_NOTICE :Auth test request being queued

  Sep 02 14:37:00:aaa:AS_NOTICE :Auth test request complete, status = pass
```

# Enabling iSCSI Authentication

iSCSI authentication is enabled for specific SCSI routing instances. By default, iSCSI authentication is not enabled.

Use the commands in the following procedure to enable iSCSI authentication using the AAA authentication methods configured in the default AAA authentication list:

1. `enable` — Enter Administrator mode.
2. `scsirouter` *`zeus`* `authenticate` *`yes`* — Enable authentication for the named SCSI routing instance. For example, enable authentication for the SCSI routing instances named **zeus**.

## Verifying and Saving Configuration

You can save the configuration at any time using either the `save aaa bootconfig` or `save all bootconfig` commands. You must save the authentication configuration for it to be retained in the Storage Router when it is rebooted.

Use the following procedure to verify and save authentication settings.

1. `enable` — Enter Administrator mode.
2. `show aaa` — Display AAA authentication configuration (Example 10).
3. `show scsirouter` *`zeus`* — Verify that iSCSI authentication is enabled for SCSI routing instances **zeus** (Example 11).
4. `save aaa bootconfig` — Save authentication settings.
5. `save scsirouter` *`zeus`* `bootconfig` — Save the SCSI routing instances.
6. `save all bootconfig` — Save all configuration settings. This command may be used in place of individual `save aaa bootconfig` and `save scsirouter bootconfig` commands described in Steps 4 and 5 (Optional).

**Example 10: Display AAA Authentication Configuration**

```
➔ [SR2122-MG1]# show aaa
aaa new-model
aaa authentication iscsi default local group radius group tacacs+
username "LabServer" password "9 3b7e1560943b2c3df73ae16dd8c21406ad"
username "LabServer2" password "9 5a034dba7085f7628852db4637787b3f9e"
radius-server key "9 4f5e3deda858731566fa8c7fa23d8a5b4d"
radius-server timeout 100
radius-server retransmit 3
radius-server host 10.5.0.53 auth-port 1645
radius-server host 10.6.0.61 auth-port 1645
tacacs-server key "9 10d2a453d607e75f36ca96dfc5d36b4495"
tacacs-server host 10.7.0.22 auth-port 49
```

### Example 11: Verify iSCSI Authentication for SCSI Routing Instance

```
➔ [SR2122-MG1]# show scsirouter zeus
zeus description "(not set)"
zeus authentication "yes"
zeus primary "none"
zeus target naming authority "none"
zeus serverif ge2 10.1.0.45/24
zeus target chimaera_apps description "(not set)"
zeus target chimaera_apps WWUI
"iqn.1987-05.com.hp.00.0b1aaa415a4146aa2d899c47070c3c06.chimaera_apps"
zeus target chimaera_apps enabled "TRUE"
zeus target chimaera_apps accesslist "none"
zeus target chimaera_apps lun 24 wwpn "22:00:00:20:37:19:15:05" lun "0"
zeus target chimaera_eng description "(not set)"
zeus target chimaera_eng WWUI
"iqn.1987-05.com.hp.00.0b1aaa415a4146ab2d799c45070c3d06.chimaera_eng"
zeus target chimaera_eng enabled "TRUE"
zeus target chimaera_eng accesslist "aegis"
zeus target chimaera_eng lun 17 wwnn "22:00:00:20:37:19:12:9d"
zeus target pegasus_email description "(not set)"
zeus target pegasus_email WWUI
"iqn.1987-05.com.hp.00.0b1aca415a6146ea2d809c44070c2c06.pegasus_email"
zeus target pegasus_email enabled "TRUE"
zeus target pegasus_email accesslist "all"
zeus target pegasus_email wwpn "22:00:00:20:37:19:12:da"
```

# Configuring a High Availability Cluster

# 10

This chapter explains how to configure storage routers in a cluster to allow the storage routers to back each other up in case of failure. The following tasks are covered:

High availability clusters can be configured using CLI commands, as described in this chapter, or via the web-based GUI. To access the web-based GUI, point your browser to the Storage Router's management interface IP address. After logging on, click the Help link to access online help for the GUI.

## Prerequisite Tasks

Before performing any high availability cluster configuration tasks, make sure you have configured system parameters, including the HA interface, as described in Chapter 5, "Configuring the Storage Router," or Chapter 6, "Configuring System Parameters."

When you configure SCSI routing instances to run in a high availability cluster, follow these guidelines:

- If you map targets using WWPN, be sure to specify both the primary WWPN (the WWPN associated with the storage resource as known to the primary Storage Router in the cluster) and the secondary WWPN (the WWPN associated with the storage resource as known to the second Storage Router in the cluster).
- Automatic failover of a SCSI routing instance occurs if the Gigabit Ethernet interface is unavailable or if all mapped targets are unavailable. If some targets are available and others are not, the SCSI routing instance will not automatically fail over. All SCSI routing instances will failover if the Storage Router running the instances fails to exchange heartbeats within the high availability cluster.

  To maximize the potential for automatic failover in case of target unavailability, map the targets associated with a single SCSI routing instance to storage that is available through one Fibre Channel interface. Do not map the targets associated with a single SCSI routing instance to storage that is available through multiple FC interfaces.

  This type of mapping minimizes the potential for a mixed target availability condition, which prevents IP hosts from accessing some storage but does not cause an automatic failover of the SCSI routing instance.

## Adding the Storage Router to a Cluster

In most situations, you will completely configure a principal Storage Router (including all cluster-wide settings), and then add a new, unconfigured Storage Router or a minimally configured Storage Router to the cluster. A high availability cluster is composed of two storage routers.

The following Storage Router configuration settings are shared cluster-wide, and when configured on the first Storage Router in the cluster, will be shared with the other Storage Router that joins the cluster.

- Access lists
- Cluster name
- SCSI routing instances
- VLAN information (VID, VTP mode, domain name, and so on)

**Note:** A minimally configured Storage Router is one in which the management IP address, system name, and optional network management interfaces have been configured. Other system information, such as HA IP address, administrator and monitor passwords, may also have been configured. A minimally configured Storage Router, however, must not have had any cluster-wide settings configured.

## Adding an Unconfigured Storage Router

To add a new, unconfigured Storage Router to an existing cluster:

1. Respond to the prompts from the Storage Router initial system configuration script. This script configures the following settings:

   - Management IP address
   - System name
   - HA configuration mode
   - Cluster name
   - HA IP address

   When prompted to select HA configuration mode, choose clustered. When prompted for cluster name, enter the name of the existing cluster. At the end of the initial system configuration script, the Storage Router automatically reboots.

2. When the Storage Router restarts, it communicates with the other member of the cluster to obtain current cluster configuration information. Once the Storage Router is completely restarted, verify the new cluster configuration. Issue the `show cluster` command to verify the cluster name and confirm that the Storage Router is exchanging heartbeats with the other member of the cluster.

3. To verify that both storage routers in the cluster include the same configuration, issue the following commands from the principal Storage Router in the cluster:
   - `show accesslist all from bootconfig`
   - `show scsirouter all from bootconfig`
   - `show vlan`
   - `show vtp`

   Issue the same commands from the Storage Router just added to the cluster. The displays should be the same.
4. Use the Setup Configuration Wizard, CLI commands, or the GUI to complete Storage Router configuration. See Chapter 5, “Configuring the Storage Router,” or Chapter 6, “Configuring System Parameters,” for complete details.
5. Save any changes made to the configuration by issuing the appropriate `save` command with the **bootconfig** keyword, which updates the bootable configuration for the Storage Router and notifies all storage routers in the cluster of the configuration changes. (Optional)
6. To divide the workload between the storage routers in the cluster, you can manually failover selected SCSI routing instances using the `failover scsirouter` command. For additional information about failing over SCSI routing instances, see the section “Controlling SCSI Routing Instances in a Cluster” in Chapter 11, “Maintaining and Managing the Storage Router.” (Optional)

## Adding a Minimally Configured Storage Router

To add a minimally configured Storage Router to an existing cluster, perform the following steps:

1. Run the Setup Cluster Configuration Wizard:
   - When prompted to select HA configuration mode, choose clustered.
   - When prompted for cluster name, enter the name of the existing cluster.
   - When prompted to retain or delete scsirouter instances, enter delete. Deleting means that any existing SCSI routing instances will be deleted from this Storage Router.
   - Enter yes to confirm your changes. The Storage Router automatically reboots.

2. When the Storage Router restarts, it communicates with other member of the cluster to obtain current cluster configuration information. Once the Storage Router is completely restarted, verify the new cluster configuration. Issue the `show cluster` command to verify the cluster name and confirm that the Storage Router is exchanging heartbeats with the other member of the cluster.
3. To verify that both storage routers in the cluster include the same configuration, issue the following commands from the principal Storage Router in the cluster:
   - `show accesslist all from bootconfig`
   - `show scsirouter all from bootconfig`
   - `show vlan`
   - `show vtp`

   Issue the same commands from the Storage Router just added to the cluster. The displays should be the same.
4. Complete additional system configuration of the Storage Router just added to the cluster, as needed. For example:
   - Use the Setup Access Configuration Wizard to configure passwords for the Storage Router.
   - Use the Setup Netmgmt Configuration Wizard to configure the Storage Router for network management via SNMP.
   - Use the Setup Time Configuration Wizard to configure the storage router date and time, and optional NTP server information.
   - Use the CLI or GUI to configure AAA authentication. See Chapter 9, “Configuring Authentication,” for additional information.
5. Save any changes to the configuration by issuing the appropriate `save` command with the **bootconfig** keyword, which updates the bootable configuration for the Storage Router and notifies all storage routers in the cluster of the configuration changes.
6. To divide the workload between the storage routers in the cluster, you can manually failover selected SCSI routing instances using the `failover scsirouter` command. For additional information about failing over SCSI routing instances, see the section “Controlling SCSI Routing Instances in a Cluster” in Chapter 11, “Maintaining and Managing the Storage Router.” (Optional)

## Adding Completely Configured Storage Routers

In some cases you may prefer to completely configure both storage routers (including SCSI routing instances and access lists) as standalone systems before joining them into a cluster.

The following example explains the steps required to create a cluster named *Cluster1*, composed of two storage routers named *StorageRouterSys1* and *StorageRouterSys2*. This example assumes that both storage routers are fully configured with SCSI routing instances and access lists. (See Chapter 8, "Configuring SCSI Routing," for details.) Use the `scsirouter primary` command to assign a preferred Storage Router to any or all of the SCSI routing instances, if desired.

**Note:** A cluster supports up to 12 active SCSI routing instances.

To create a cluster from fully configured storage routers, perform the following steps:

1. Use the *setup cluster configuration* wizard to define *StorageRouterSys1* as a member of the cluster *Cluster1*. When prompted, enter retain to keep the access list and SCSI routing instance information already defined.
2. Use the `show cluster` command to verify the cluster name after *StorageRouterSys1* reboots. Verify that all instances and access lists are still available, using `show scsirouter` and `show accesslist` commands.
3. On *StorageRouterSys2*, save any access list information that you want to make available in the cluster to a file, using the `save accesslist` command. (Optional)

   For example, to save all access lists to a file named *StorageRouterSys2_AccessLists.xml*:

   ```
   save accesslist all SR2122Sys2_AccessLists.xml
   ```

4. Because access lists can only be manipulated from the first Storage Router in a cluster, the saved configuration file from *StorageRouterSys2* must be made available to *StorageRouterSys1*. See Chapter 11, "Maintaining and Managing the Storage Router," for information on managing Storage Router saved configuration files using either the `copy savedconfig` command or `FTP`. (Optional)

5. Add *SvSys2* to the new cluster named *Cluster1*, using the Setup Cluster Configuration Wizard. When prompted, enter retain to share the existing SCSI routing instances across the cluster.
6. Use the `show cluster` command to verify the cluster name after *StorageRouterSys2* reboots. Verify that the defined SCSI routing instances were retained, using `show scsirouter` command.
7. Restore any access lists saved in Step 3 using the `restore accesslist from` command. Access lists can only be manipulated from the first Storage Router in a cluster, so these commands must be issued from the system *StorageRouterSys1*. (Optional)
8. Save all configuration information on system *StorageRouterSys1* by issuing a `save all bootconfig` command, which updates the bootable configuration of all storage routers in the cluster. (Optional)
9. Verify that all SCSI routing instances are active using the `show scsirouter stats` command on both storage routers.

## Changing Clusters

In some situations, you may need to move the Storage Router from one cluster to another cluster. Moving a fully configured Storage Router from one cluster to another is more complex than simply adding the Storage Router to a cluster. Advanced planning is required.

To successfully move the Storage Router from one cluster to another:

1. Verify that the Storage Router to be moved has the same hardware configuration as the other storage routers in the cluster you are planning to join. Each Storage Router in the cluster must have connectivity to the same IP hosts and Fibre Channel storage. All management interfaces for the storage routers within a cluster must be on the same IP subnet, and all HA interfaces for the storage routers within a cluster must be on the same IP subnet. However, the management interfaces must be on a different IP network than the HA interfaces.
2. Decide if you need to retain any SCSI routing instances defined on the Storage Router joining the cluster. Retaining data means all SCSI routing instances existing on the Storage Router joining the cluster will be added to those already defined for the cluster. If the existing instances are not retained, they are deleted.

3. If you are going to retain data, determine if you have any duplicate SCSI routing instance names. When the Storage Router is added to the cluster, the data in the cluster will overwrite the existing data. You may prefer to change the configuration in the Storage Router before it joins the cluster to prevent this situation.
4. If you are going to retain data, determine if you need to save existing access list information. Access lists are not retained. Any access lists on the Storage Router will be discarded when it joins the new cluster. You can save the access list information and then restore it to the cluster. Access list information can be restored before or after the Storage Router joins the cluster by transferring the saved configuration file to the first Storage Router in the cluster and performing the restore.
5. Use the Setup Cluster Configuration Wizard to join the new cluster. Respond to the prompts to retain or delete configuration as required. The Storage Router will automatically reboot at the end of the configuration wizard.
6. Perform any additional configuration that may be needed. You can fail over SCSI routing instances to this new cluster member to balance traffic load between all storage routers in the cluster.
7. Use the `save all` command with the **bootconfig** keyword to copy and save the Storage Router configuration, thereby updating the cluster.

# Maintaining and Managing the Storage Router

# 11

This chapter explains how to perform normal maintenance and management tasks associated with the Storage Router. The following tasks are covered:

Storage router maintenance and management tasks can be performed using CLI commands, as described in this chapter, or via the web-based GUI. To access the web-based GUI, point your browser to the Storage Router's management interface IP address. After logging on, click the Help link to access online help for the GUI.

**Note:** Not all maintenance and management tasks are appropriate for all storage routers. For example, tasks related to high availability clusters (such as failover of SCSI routing instances) are not necessary for storage routers configured as standalone systems.

# Prerequisite Tasks

Before performing any storage router maintenance tasks, make sure you have configured system parameters as described in Chapter 5, “Configuring the Storage Router,” or Chapter 6, “Configuring System Parameters.”

**Note:** Certain configuration tasks, such as identifying a location from which to download software, are optional and may not have been performed during initial configuration. You may perform these tasks at any time, via the CLI or the GUI. Where necessary, this chapter will identify the relevant tasks and commands.

# Installing Updated Software

The Storage Router is designed to run on a continual basis without significant maintenance. However, from time to time, you may need to install updated software. The Storage Router stores software images (along with configuration files, log files, and other information) on a local file system. This file system is stored on an internal, non-volatile Flash disk. The `show software version all` command displays a list of all software versions stored on the Storage Router and the amount of disk space available for additional software.

http://www.hp.com provides registered users access to storage router software updates. You can download updated software directly to the Storage Router from HP.com via standard HTTP, or via HTTP using a proxy server. You can also use a standard browser to download software updates and associated readme files from http://www.hp.com to a location of your choosing. Using the CLI or the web-based GUI, you can then make software available from this location (known as the “download location”) to the Store Router via HTTP, HTTP using a proxy server, or Trivial File Transport Protocol (TFTP).

**Note:** Always review the readme file before making updated software available to the Storage Router.

If you plan to use the CLI `download software http` or `download software proxy` commands to make the updated software available to the Storage Router, the machine hosting the download location must be running a web server. If you plan to use the CLI `download software tftp` command, the machine must be accessible using the Trivial File Transport Protocol. If the machine is not running a web server or accessible via TFTP, use the storage router web-based GUI to make the updated software available to the Storage Router. (See the online Help for details.)

The download location used for retrieving updated storage router software is set using the `software http url`, `software proxy url`, or the `software tftp` commands. To view the download location currently specified, use the `show software version all` command (Example 12). The `show software version all` command identifies the HTTP URL, Proxy URL, and TFTP host name and other information used to identify the download location, the current version of software running on the Storage Router, and the version that will be used at system restart. In the example, all default locations and related user names and passwords are set.

**Note:** If you are a registered HP.com user, you can download a TFTP server tool for Microsoft Windows 95, Microsoft Windows 98, and Microsoft Windows NT. You can reach the TFTP server tool on HP.com at the Software Center under Service & Support: http://www.hp.com/support.

### Example 12: Results of "show software version all" Command

```
[SR2122_A01]# show software version all
Version    Boot  Hash  Sign  Crash  Size     Date
---------  ----  ----  ----  -----  -----    ----------
2.3.0.49   OK    OK    N/A   0      18585600 Mar 21 18:08 CST 2002
2.3.1      OK    OK    N/A   0      18616320 Mar 22 16:35 CST 2002

Http Url: http://www.HP.com
Http Username: SWAdmin01
Http Password: *********

Proxy Address: 10.1.12.32
Proxy Port: 3122
Proxy Url: http://www.hp.com
Proxy Username: SWAdmin01
Proxy Password: *********

Tftp Hostname: 10.1.1.122
Tftp Directory: SR2122/v2.3/

Disk Space Available: 13357.0 KB
Current Version: 2.3.1
Boot Version: 2.3.1
```

To update storage router software:

1. Identify the location from which to retrieve the updated storage router software. (This is either http://www.hp.com or another download location of your choosing, as previously described.) (Optional)
2. Make the selected version of software available on the storage router local file system.
3. Set the new version as the version to be booted during the next system restart, and reboot the Storage Router. (Optional)

## Specifying the Location to Retrieve Updated Software

You must specify the location from which to retrieve updated software. If the current download location is not appropriate, you can reset it. Use the following procedures to specify the desired download location:

- Using HTTP, page 132
- Using Proxy Services, page 133
- Using TFTP, page 134

When you are finished, verify the new settings using the `show software version all` command, then save them using the `save system bootconfig` or `save all bootconfig` command.

### Using HTTP

Use the following procedure to specify the HTTP download location:

1. `enable` — Enter Administrator mode.
2. `show software version` *`all`* — List the software versions currently available for booting, along with the current download locations. Verify that the version of software required is not already available. Verify that the current download location information for HTTP is correct.
3. `software http url` *`http://10.1.11.32/~software/SR2122`* — If the current download location is not the one from which you would normally retrieve updated software, reset the current download location. For example, reset your current download location to **http://10.1.11.32/~software/SR2122**. (Optional)

4. `software http username` *`webadmin`* `password` *`webword`* — Use this command to define the user name and password needed to access the selected location. For example, specify user name **webadmin** and password **webword**. If no user name and password are required, use the keyword **none** (for example, `software http username none`). (Optional)

**Note:** If you are using the default URL, http://www.hp.com, the username and password must be the same as your hp.com login ID and password.

## Using Proxy Services

Use the following procedure to specify a download location via proxy services:

1. `enable` — Enter Administrator mode.
2. `show software version` *`all`* — List the software versions currently available for booting, along with the current download locations. Verify that the version of software required is not already available. Verify that the current download location information for HTTP via proxy server is correct.
3. `software proxy url` *`default`* — If the current download location is not the one from which you would normally retrieve updated software, reset the current download location. For example, reset your current download location to the **default** (http://www.hp.com). (Optional)
4. `software proxy address` *`http://10.1.10.126`* `port` *`32`* — This is the address and port number of the proxy server that will be used to access the URL specified in Step 3 (for example, **http://10.1.10.126**, port **32**). (Optional)
5. `software proxy username` *`HPuser`* `password` *`HPpswd`* — Use this command to define the user name and password needed to access the selected download location. For example, specify user name **HPuser** and password **HPpswd**. If no user name and password are required, use the keyword none (for example, software proxy username none). (Optional)

**Note:** If you are using the default URL, http://www.hp.com, the username and password must be the same as your hp.com login ID and password.

## Using TFTP

Use the following procedure to specify the TFTP download location:

1. `enable` — Enter Administrator mode.
2. `show software version all` — List the software versions currently available for booting, along with the current download locations. Verify that the version of software required is not already available. Verify that the current download location information for TFTP is correct.
3. `software tftp hostname` *`TFTPHost1`* `directory` *`/tftpboot`* — If the current host name and base directory location are not the ones from which you would normally retrieve updated software, reset the host and optional base directory. For example, set the host name to **TFTPHost1** and the base directory to `/tftpboot`. If a DNS is not defined for the Storage Router, enter the IP address of the TFTP host.

# Downloading Updated Software

The `download software` command makes a new version of software available to the Storage Router for boot purposes. You can store two versions of software on the Storage Router. Before attempting to download updated software, verify that only a single version of software exists on the Storage Router.

Use the following procedures to make a new version of software available to the Storage Router:

- Using HTTP, page 135
- Using Proxy Services, page 135
- Using TFTP, page 136

## Using HTTP

Use the following procedure to make a new version of software available to the Storage Router via HTTP:

1. `enable` — Enter Administrator mode.
2. `show software version` *`all`* — Verify that there is only one version of software on the Storage Router. If two versions exist, use the `delete software version` command to delete the old version of software to make room for the new version.
3. `download software http version` *`2.3.1`* — Download a new software version to the Storage Router (for example, **2.3.1**).

**Note:** There may be times when you need to make special software available to the Storage Router, for example, under the guidance of a HP Technical Support professional. If you isolate this software from standard updates by placing it in another location (not the default download location), you could change the default download location, download the software, and then reset the default download location. An easier way, however, is to specify the download location via the URL parameter on the `download software http` command. For example, to download a file named **231.tar** containing version 2.3.1 software from `http://your.website.com/StorageRouter`, issue this command: `download software http url http://your.website.com/StorageRouter/231.tar`.

## Using Proxy Services

Use the following procedure to make a new version of software available to the Storage Router via proxy services:

1. `enable` — Enter Administrator mode.
2. `show software version` *`all`* — Verify that there is only one version of software on the Storage Router. If two versions exist, use the `delete software version` command to delete the old version of software to make room for the new version.
3. `download software proxy version` *`2.3.1`* — Make a new software version available to the Storage Router (for example, **2.3.1**).

**Note:** There may be times when you need to make special software available to the Storage Router, for example, under the guidance of a HP Technical Support professional. If you isolate this software from standard updates by placing it in another location (not the default download location), you could change the default download location, download the software, and then reset the default download location. An easier way, however, is to specify the download location via the URL parameter on the `download software proxy` command. For example, to download a file named **231.tar** containing version 2.3.1 software from `http://your.website.com/StorageRouter` using the services of a proxy server, issue this command:
`download software proxy url http://your.website.com/ StorageRouter/231.tar`.

## Using TFTP

Use the following procedure to make a new version of software available to the Storage Router via TFTP:

1. `enable` — Enter Administrator mode.
2. `show software version` *`all`* — Verify that there is only one version of software on the Storage Router. If two versions exist, use the `delete software version` command to delete the old version of software to make room for the new version.
3. `download software tftp version` *`2.3.1`* — Make a new software version available to the Storage Router (for example, **2.3.1**).

**Note:** There may be times when you need to make special software available to the Storage Router, for example, under the guidance of a HP Technical Support professional. If you isolate this software from standard updates by placing it in another location (not the default download location), you could change the default download location, download the software, and then reset the default download location. An easier way, however, is to specify the download location via the hostname and filename parameters on the `download software tftp` command. For example, to download a file named **231.tar** containing version 2.3.1 software from my_tftpHost using TFTP, issue this command:
`download software tftp hostname my_tftp Host` filename **231.tar**. The **231.tar** file must reside in the default base directory defined for the TFTP host.

## Setting Updated Software as Boot Version

Downloading updated software to the Storage Router does not change the currently running version of the software, nor does it automatically set the new version to be booted at next system restart. You must take specific action to make the new software version bootable.

Setting software as the bootable version consists of verifying the software integrity and performing internal checks to ensure that the Storage Router can boot the specified version of software.

Use the following procedure to set the new software as the version to be booted:

1. `enable` — Enter Administrator mode.
2. `software version` *`2.3.1`* — Select the software to be booted when the system next starts (for example, boot **2.3.1** when the system restarts). The system checks the integrity of the specified software version to be sure that it is bootable.
3. `show software version boot` — Verify that the correct version is shown as the bootable version (identified as Boot Version).
4. `reboot` — Restart the Storage Router to run the new software. (Optional)

When you set a new software version as the bootable version, internal checks are made to ensure that the new software can be run.

## Precautions for Cluster Environments

In a cluster environment, the `software version` command may temporarily suspend normal HA communications, while internal checks are made to ensure that the new software can be run. A suspension will cause a failover of any SCSI routing instances active on the Storage Router.

Any instances with the primary attribute set to the name of the Storage Router will resume running on the Storage Router after it is rebooted. If you are not going to reboot the Storage Router immediately, use the `failover scsirouter` command to return the desired SCSI routing instances to the Storage Router.

If the Storage Router is running in a cluster environment, issuing the `reboot` command will attempt failover for all SCSI routing instances to another Storage Router in the cluster. The iSCSI drivers handle reconnection of users to the appropriate storage resources, minimizing the effects of the reboot sequence on those users.

# Backing Up System Configuration

Backing up the system configuration consists of saving selected storage router configuration information to XML files that can be stored both locally and remotely. Should problems occur, AAA authentication information, SCSI routing instances, access lists, VLANs, and other storage router system configuration information can be restored from these files.

While you can issue a `save` command at any time during a CLI command session, best practices suggest that you should back up the storage router system configuration to a file on a regular basis.

Configuration files are normally maintained in the `savedconfig` directory on the Storage Router. You can use the `copy` command to copy the configuration file to a server running TFTP, allowing you to integrate the storage router backups with other software archives. By accessing the web-based GUI from a remote server, you can create storage router backup files directly on that server. See the GUI online help for details.

## Creating Local Backups

Local backups allow you to store the resulting XML configuration file in the `savedconfig` directory on the Storage Router.

Use the following procedure to perform a local backup that saves the configuration of all the current SCSI routing instances to a file named *backup1* in the `savedconfig` directory:

1. `enable` — Enter Administrator mode.
2. `save scsirouter all` *`backup1`* — Save all defined SCSI routing instances to a file named *backup1*.

## Storing Backups to a Remote TFTP Server

Use the following procedure to create a backup configuration file named *backup1* and to copy that backup file to another file named *back1.xml*, located on the TFTP host, tftpserver1, in the default directory, `/tftpboot`:

1. `enable` — Enter Administrator mode.
2. `save all` *`backup1`* — Save the current running configuration to a file called *backup1* in the `savedconfig` directory.
3. `copy savedconfig:` *`backup1 tftp://tserver1/ back1.xml`* — Copy the saved configuration file, *backup1*, to a file called *back1.xml*, located on the TFTP server, tserver1, in the default directory.

**Note:** The **back1.xml** file must already exist in the `default` directory with the appropriate permissions that allow it to be overwritten. You cannot create a new file using TFTP.

# Restoring from Backups

AAA authentication information, SCSI routing instances, access lists, VLANs, and selected system configuration data can be restored from previously saved configuration files. You may choose to restore selected data such as a specific SCSI routing instance, or all data, using the `restore` command with the `from` keyword.

The file from which configuration is restored must reside in the `savedconfig` directory (`/ata3/savedconfig`). If you need to restore configuration data from a backup file existing elsewhere in the network, use the `copy` command to make the desired file available in the `savedconfig` directory.

Restoring configuration data copies all or part of the contents of the specified file into persistent memory; it does not always change the Storage Router's running configuration. For example, the configuration of a restored SCSI routing instance may only be completely visible via the `show scsirouter` command using the `from bootconfig` keywords, until the instance has been restarted.

## Restoring a Deleted SCSI Routing Instance

For example, suppose the SCSI routing instance, **scsi1**, was inadvertently deleted. Use the following procedure to restore **scsi1** from a configuration file that was saved to a URL:

1. `enable` — Enter Administrator mode.
2. `copy` *`http://10.1.1.44/~s1/back1.xml`* `savedconfig:`*`scsi1_restore.xml`* — Copy the specified configuration file from the designated URL and place it in the `savedconfig` directory, using the file name, *scsi1_restore.xml*.
3. `show savedconfig` — Verify that the imported file now exists in the `savedconfig` directory.
4. `show scsirouter all from` *`scsi1_restore.xml`* — Restores SCSI routing instance, **scsi1**, from the specified file.
5. `show scsirouter` *`scsi1`* `from` *`bootconfig`* — Display the restored SCSI routing instance, **scsi1**, to verify configuration is as expected.
6. `scsirouter` *`scsi1`* `enable` — Start the restored SCSI routing instance, updating the running configuration of the Storage Router. Once the instance has been restored and restarted, modifications to its configuration can also be made.
7. `save scsirouter` *`scsi1`* `bootconfig` — If changes are made to the SCSI routing instance configuration, save the SCSI routing instance to the storage router bootable configuration. (Optional)

## Restoring an Existing SCSI Routing Instance

If you need to restore the configuration of a SCSI routing instance that is still active in the Storage Router, you must stop the instance, restore the configuration from the selected file, then restart the instance. For example, use the following procedure to restore the SCSI routing instance, **scsi2**, from the file, *scsi2_backup*.

1. `enable` — Enter Administrator mode.
2. `show scsirouter` *`scsi2`* `stats` — Display current status of the SCSCI routing instance, scsi2. If the status is active, issue the `no scsirouter enable` command shown in Step 3 to stop the instance.
3. `no scsirouter` *`scsi2`* `enable` — Disable an active SCSI routing instance. You cannot restore an active instance.
4. `show savedconfig` — Confirm that the desired backup file exists in the `savedconfig` directory.
5. `show scsirouter` *`all`* `from` *`scsi2_backup`* — Verify that the instance saved in the configuration file is the one you want to restore.
6. `restore scsirouter` *`scsi2`* `from` *`scsi2_backup`* — Restore the SCSI routing instance.
7. `show scsirouter` *`scsi2`* `from` *`bootconfig`* — Confirm that the configuration of the SCSI routing instance is now correct.
8. `scsirouter` *`scsi2`* `enable` — Restart the SCSI routing instance.
9. `show scsirouter` *`scsi2`* — Verify the configuration of the restored and restarted SCSI routing instance. The running configuration should now match the restored permanent configuration. Once the instance has been restored and restarted, modifications to its configuration can also be made.
10. `save scsirouter` *`scsi2`* `bootconfig` — If changes are made to the SCSI routing instance configuration, save the restored SCSI routing instance to the Storage Router's bootable configuration.

## Restoring an Access List

When you restore an access list, existing entries are never deleted. The restore will add missing entries and overwrite entries of the same name, but will never purge or delete existing entries. If necessary, you can delete an entire access list and then restore if from a saved configuration file.

Use the following procedure to restore the access list, **mylist1**, from the file, *accesslist_backup.xml*. In this example, **mylist1** in the running configuration contains the following entries:

- 10.1.1.30/32
- 172.16.255.220/32
- chap-username 12h7b.lab2.webservices
- chap-username 12784.lab1.webservices

The saved access list in the configuration file, *accesslist_backup.xml*, contains these entries:

- 209.165.200.225/32
- 10.1.1.30/32
- chap-username 12h7b.lab2.webservices
- chap-username test2.sys3

**Note:** In a cluster environment, access lists management functions are handled by a single Storage Router. If you issue an `access list` command from a Storage Router that is not performing access list management functions, the CLI displays an informational message with the name of the Storage Router that is currently handling those functions.

1. `enable` — Enter Administrator mode.
2. `show accesslist` *`mylist1`* — Display the current entries associated with access list, **mylist1**.
3. `show accesslist` *`mylist1`* `from` *`accesslist_backup.xml`* — Display the entries associated with access list, mylist1, saved in the configuration file, *accesslist_backup.xml*. The configuration file must exist in the `savedconfig` directory.
4. `restore accesslist` *`mylist1`* `from` *`accesslist backup.xml`* — Restore the access list entries for mylist1 from the saved configuration file, *accesslist_backup.xml*.
5. `show accesslist` *`mylist1`* — Display the entries for the restored access list, **mylist1**. The entries are:
   - 10.1.1.30/32
   - 172.16.255.220/32
   - 209.165.200.225/32
   - chap-username 12h7b.lab2.webservices
   - chap-username 12784.lab1.webservices
   - chap-username test2.sys3
6. `save accesslist` *`mylist1`* `bootconfig` — If any entries prior to the restore were not saved, issue the `copy` command to save the current access list configuration to the storage router bootable configuration. (Optional)

## Restoring AAA Authentication Information

When you restore AAA authentication information, the following configuration settings are updated:

- AAA authentication list
- The user names and passwords in the local username database
- Radius servers and associated server and global authentication port, retransmit, time-out, and key values
- TACACS+ servers, and associated server and global authentication port, time-out, and key values.

Use the following procedure to restore the AAA authentication configuration that exists in the saved configuration file *aaa_backup.xml*:

1. `enable` — Enter Administrator mode.
2. `show savedconfig` *`aaa_backup.xml`* — Display the contents of the backup file, and verify that this is the AAA authentication configuration that you want to restore. The file must exist in the `savedconfig` directory.
3. `restore aaa from` *`aaa_backup.xml`* — Restore the AAA authentication from the saved configuration file, *aaa_backup.xml*.
4. `show aaa` — Display the AAA authentication information and verify that it is now correct.
5. `save aaa bootconfig` — If you make any changes to the restored AAA authentication configuration, save the changed configuration to the storage router bootable configuration. (Optional)

## Restoring VLANs

You can restore specific VLANs or all VLANs. When you restore a VLAN, the VTP mode is also restored.

Use the following procedure to restore a VLAN. In this example, VLAN 10 (named **TestLab**) will be restored from the saved configuration file named *VLAN_backup.xml*:

---

**Note:** In a cluster environment, VLAN configuration must be performed on the first Storage Router to join the cluster. If you issue a `VLAN` command from another Storage Router in the cluster, the CLI displays an informational message with the system name and IP address of the Storage Router that is currently handling all VLAN functions.

---

1. `enable` — Enter Administrator mode.
2. `show savedconfig` *`VLAN_backup.xml`* — Display the contents on the saved configuration file *VLAN_backup.xml*. Verify that the file contains the VLAN and VTP configuration information that you want to restore (Example 13).
3. `restore vlan 10 from` *`VLAN_backup.xml`* — Restore VLAN 10 from the saved configuration file *VLAN_backup.xml*.
4. `show vlan` — Verify that the VLAN is restored and the configuration is correct.
5. `show vtp` — Verify that the VTP configuration is correct.
6. `save vlan` *`10`* `bootconfig` — If you make any configuration changes to the VLAN after restoration, save the changes to the storage router bootable configuration. (Optional)

**Example 13: Show VLAN Information from Saved Configuration File**

```
!
! VTP DOMAIN
!
vtp domain none
!
! VTP MODE
!
vtp mode transparent
!
! VLAN
!
vlan 10 name TestLab mtusize 1500
```

## Restoring System Configuration

You can restore selected system information using the `restore system` command. You can restore the following information:

- Administrator contact settings
- SNMP network management configuration
- NTP server and date, time, and time zone settings
- DNS configuration
- IP address of remote syslog host
- Software default download locations and associated user names and passwords
- CDP configuration
- Restrict service setting for all interfaces
- Storage router routing table
- Storage router event message logging table
- Configuration settings for all Fibre Channel interfaces

Use the following procedure to restore system configuration information. In this example, SNMP network management configuration and administrator contact settings will be restored from the saved configuration file named *system_backup.xml*:

1. `enable` — Enter Administrator mode.
2. `show savedconfig` *`system_backup.xml`* — Display the contents of the saved configuration file, *system_backup.xml*. Verify that the file contains the SNMP network management configuration and administrator contact information that you want to restore.
3. `restore system snmp from` *`system_backup.xml`* — Restore SNMP network management configuration.
4. `show snmp` — Verify that the SNMP network management information is restored and that the configuration is correct (Example 14).
5. `restore system contactinfo from` *`system_backup.xml`* — Restore administrator contact settings.
6. `show admin` — Verify that the administrator contact information is restored and that the configuration is correct (Example 15).

7. `save system bootconfig` — If you make any configuration changes to the SNMP configuration or administrator contact information after restoration, save the changes to the Storage Router's bootable configuration. (Optional)

**Example 14: Verify SNMP Configuration**

```
➔ [SR2122_PR1]# show snmp
  First Trap Host: 10.1.32.200
  Second Trap Host: 10.2.12.242
  Get Community String: public
  Set Community String: private
  Send Authentication Traps: enabled
  Link Up/Down Enable for mgmt: enabled
  Link Up/Down Enable for fc1: enabled
  Link Up/Down Enable for fc2: enabled
  Link Up/Down Enable for fc3: enabled
  Link Up/Down Enable for fc4: enabled
  Link Up/Down Enable for fc5: enabled
  Link Up/Down Enable for fc6: enabled
  Link Up/Down Enable for fc7: enabled
  Link Up/Down Enable for fc8: enabled
  Link Up/Down Enable for ge1: enabled
  Link Up/Down Enable for ge2: enabled
```

**Example 15: Verify Administrator Contact Information**

```
➔ [SR2122_PR1]# show admin
  Administrator Contact Information
     Name: Pat Hurley
     Email: phurley@abc123z.com
     Phone: 123.456.7890
     Pager: 123.456.3444 pin 2234
```

## Powering Down the Storage Router

If you need to make changes to the physical location or cabling of the Storage Router, you may need to schedule a time to power down the unit. Use the following procedure to properly power down a Storage Router. These steps assure that the file system is in the appropriate state prior to shutdown.

1. `enable` — Enter Administrator mode.
2. `halt` — Assure that all configuration information is saved. Respond to any prompts to save information as desired. The Storage Router can be safely powered down when the `[HALTED]#` command prompt appears.

# Resetting the System

There may be times when you need to return some or all of the storage router configurations to factory defaults, for example, when moving a system between environments (such as test and production) or for troubleshooting purposes.

To reset the Storage Router:

1. Save existing configuration information to a file. (Optional)
2. Clear the current configuration and restore some or all factory defaults, using the `clear conf` command.

**Note:** If the Storage Router is operating in a cluster environment, any SCSI routing instances running on this storage router fail over to another Storage Router in the cluster. If you are operating in a cluster environment but do not want SCSI routing instances to fail over, issue the `no scsirouter enable` command for all instances (or selected instances that should not fail over) before you issue the `clear conf` command. (This will permanently delete the SCSI routing instances from the cluster.) See the "Controlling SCSI Routing Instances in a Cluster" section on page 151 for additional information on operating the Storage Router in a cluster environment.

3. Run the initial configuration script to configure the management interface via an EIA/TIA-232 console connection. (Optional)
4. Restore specific configuration information or reconfigure the Storage Router using CLI commands or the web-based GUI.

## Reset All to Factory Defaults

Use the following procedure if an existing Storage Router is to be physically moved to another environment, and it is not necessary to retain any current configuration information (system setup will be completely different).

1. `enable` — Enter Administrator mode.
2. `clear conf or clear conf all` *`HP`* — Clear the current system configuration, including network management information.

   For storage routers deployed for SCSI routing, you can use the Clear Conf Wizard. At the prompt, enter the Administrator password. Enter all to erase system configuration and management port settings, and all saved configurations and SCSI routing instances (Example 16). Entering the CLI `clear conf all` command, followed by the Administrator password (for example, **hp**) will also erase system configuration and management port settings.

After either of the commands completes, the Storage Router reboots.

**Example 16: Reset Storage Router Configuration**

```
Enter admin password: *****

This process can restore factory default settings for the SR2122.
* Select "apps" to remove active applications and retain system
  configuration settings.
* Select "system" to remove active applications and system
  configuration settings.
* Select "saved" to remove all backup configurations from disk.
* Select "all" to remove active applications, system   configuration,
  and saved configurations.

The system configuration includes the management port, dns, admin and
monitor login, ntp, and snmp. You will need to use the console
to reconfigure the management port if you erase the system
configuration.

The system will reboot if you select "apps", "system", or "all".

Erase what? [apps/system/saved/all/cancel (cancel)]
```

**Note:** After the move, use the EIA/TIA-232 console connection to configure the management interface IP address and other required system information. (See the “Initial System Configuration Script” section in Chapter 5, “Configuring the Storage Router,” for details.) Then configure the Storage Router via the Setup Configuration Wizards or other CLI commands, or via the web-based GUI.

## Reset and Retain System Settings

Use the following procedure if an existing Storage Router is going to be used for testing purposes and then is to be restored to its current configuration, and for the test, the Storage Router’s system configuration information is not going to change. The following procedure retains the system configuration and saved configuration files over the system reset:

1. `enable` — Enter Administrator mode.
2. `save all` *`myfile`* — Save all configuration information in a file called *myfile*. This file is stored in the `savedconfig` directory.
3. `clear conf` — Clear the current configuration but retain system information (such as management and HA interfaces, logging table, DNS, Administrator and Monitor passwords, NTP server, and SNMP information) and saved configuration files.

At the prompt, enter the Administrator password. Enter apps to retain system configuration settings.

The Storage Router reboots.

Perform the required user testing. When finished, continue with Step 4 to restore the original configuration.

4. `restore all from` *`myfile`* — Restore original configuration, which was retained over the `clear conf` command.
5. `reboot` — Reboot to restore the original application configuration into running memory.

## Reset to Remove Saved Configuration Files

Use the following procedure if a stand-alone Storage Router has joined a cluster and adopted the new cluster's configuration. The procedure removes previously saved configuration files from the stand-alone period, but the Storage Router's system configuration, management information, and SCSI routing instances remain unchanged.

1. `enable` — Enter Administrator mode.
2. `clear conf` — Remove all saved configuration files from the `savedconfig` directory.

   At the prompt, enter the Administrator password. Enter saved to retain system configuration settings.

   All files are removed from the `savedconfig` directory, but the Storage Router does not reboot.
3. `show savedconfig` — Verify that all files have been removed from the `savedconfig` directory.

**Note:** You can also use the `delete savedconfig` command to delete selected saved configuration files from the `savedconfig` directory.

# Recovering Passwords

The storage router management interface is password protected. You must enter passwords when accessing the Storage Router via Telnet (for the CLI) or the web-based GUI. Password protection can also be enabled for the storage router console interface, requiring that the same Administrator and Monitor mode passwords that are configured for the management interface be applied to the console interface.

If the passwords have been enabled for the console interface and are lost, you can recover management access to the Storage Router using the password recovery procedure. The password recovery procedure requires physical access to the storage router console and can be found at the following URL:

http://www.hp.com

# Controlling SCSI Routing Instances in a Cluster

It is important to know where SCSI routing instances are running. While automatic failover capabilities keep the storage router cluster operational in times of system difficulties, manual HA controls provide the ability to distribute SCSI routing instances between the storage routers in a cluster to meet your specific network requirements.

The following are typical activities involved with controlling SCSI routing instances in a cluster environment. While most of these activities are performed infrequently, some (such as viewing operational statistics) may be performed on a regular basis.

- Making Changes to Instance Configurations, page 152
- Enabling and Disabling Connections, page 153
- Stopping and Starting Instances, page 154
- Viewing Operational Statistics, page 155
- Handling Failover, page 155

## Making Changes to Instance Configurations

**Note:** To assure that changes are correctly propagated to all storage routers within a cluster, always modify the configuration of a SCSI routing instance from the Storage Router where the instance is currently active.

From time to time, you will make changes to the SCSI routing instance configurations. Changes include such actions as adding or deleting a target, adding or deleting a LUN, remapping a target, or modifying access. It is important to understand the ramifications of these changes on the IP hosts accessing the associated storage resources. For example, changing the instance configuration may change the device presentation to the IP host, effectively changing the name or number assigned to the device by the host operating system. Certain instance configuration changes, such as adding or deleting targets, adding or deleting LUNs within a particular target, or adding or deleting entire instances may change the order of the devices presented to the host. Even if the host is only associated with one SCSI routing instance, the device order could make a difference.

Typically, the IP host operating system assigns drive identifications in the order they are received based on certain criteria. For example, a Linux system assigns drive identifications in the order they are received based on host, bus, target, and LUN information. Changing the order of the storage discovery may result in a changed drive identification. Applications running on the host may require modification to appropriately access the current drives.

If an entire SCSI routing instance is removed, or there are no targets available for the host, the host's iSCSI driver configuration file must be updated to remove the appropriate reference before restarting the iSCSI driver. If a host's iSCSI configuration file contains a reference to an instance which does not exist or has no targets available for the host, the iSCSI driver will not complete a login and will not discover targets associated with any SCSI routing instance.

For additional information and recommended procedures for changing iSCSI driver configuration, see the "Configuring the iSCSI Drivers" section of Chapter 5, or the iSCSI driver readme files.You can access the latest iSCSI drivers and readme files from http://www.hp.com.

## Enabling and Disabling Connections

A SCSI routing instance becomes active, by default, once it is associated with a Gigabit Ethernet interface to IP hosts. Each target that is added to an instance is also, by default, enabled. However, no IP hosts can connect or log in to that target because the target has no access list association. Once you associate an access list with a target, it is automatically enabled; the IP hosts specified by access list entries are allowed to connect or log in to the target.

Use the `scsirouter target disabled` command to control access to the target without changing the access list association or stopping the entire SCSI routing instance. Existing connections and logins are not affected, but future connections and logins are prohibited.

Use the `scsirouter target enabled` command when you are ready to allow connections and logins again.

For example, suppose you have a problem with an entry in the access list, webserver2. This access list is associated with the target, **webstorage2**, which is, in turn, associated with the SCSI routing instance **foo**.

Use the following procedure to temporarily disable access to the target associated with a problem access list:

1. `enable` — Enter Administrator mode.
2. `show scsirouter` *`foo`* `stats` — Display status to confirm the SCSI routing instance, foo, is active on this Storage Router.
3. `show scsirouter` *`foo`* — Verify the name and current status of the target and access list. The target, **webstorage2**, should be associated with the **webserver2** access list and the target should be enabled. (Example 17.)
4. `scsirouter` *`foo`* `target` *`webstorage2`* `disabled` — Disable access to the target, webstorage2. (Example 18)

### Example 17: Verify Target, Access List, and Target Status

```
  [SR2122_PR1]# show scsirouter foo
  foo description “test SCSI routing instance”
  foo authenticate “none”
  foo primary "none"
  foo proxy server disabled
  foo failover primary “none”
  foo failover secondary “none”
  foo lun reset no
  foo cdb retry counter 30
  foo serverif ge2 10.1.0.45/24, TCP port:3260
  foo target webstorage2 description “Web Storage”
  foo target webstorage2 Name
  “ign.1987-05.com.hp.00.0b1aaa415.....webstorage2”
➔ foo target webstorage2 enabled "TRUE"
➔ foo target webstorage2 accesslist "webserver2"
  foo target webstorage2 wwpn "21:00:00:05:ae:42:2f:12"
```

### Example 18: Verify New Target Status

```
  [SR2122_PR1]# show scsirouter foo
  foo description “test SCSI routing instance”
  foo authenticate “none”
  foo primary "none"
  foo proxy server disabled
  foo failover primary “none”
  foo failover secondary “none”
  foo lun reset no
  foo cdb retry counter 30
  foo serverif ge2 10.1.0.45/24,TCP port:3260
  foo target webstorage2 description “Web Storage”
  foo target webstorage2 Name
  “ign.1987-05.com.hp.00.0b1aaa415.....webstorage2”
➔ foo target webstorage2 enabled "FALSE"
  foo target webstorage2 accesslist "webserver2"
  foo target webstorage2 wwpn "21:00:00:05:ae:42:2f:12"
```

## Stopping and Starting Instances

If the Storage Router is experiencing a problem with a specific set of IP hosts or storage resources, you may wish to stop the associated SCSI routing instance from running anywhere in the cluster. The `no scsirouter enable` command causes the specified SCSI routing instance to cease running on the Storage Router, but does not cause a failover to another Storage Router in the cluster. This command effectively stops an instance from running anywhere in the cluster.

Once a SCSI routing instance has been stopped, it can be re-activated by issuing the `scsirouter enable` command. The `scsirouter enable` command must be issued from the same Storage Router as the `no scsirouter enable` command.

See the *Command Line Interface User Guide* for command details.

## Viewing Operational Statistics

Use the `show scsirouter stats` command to display the status of the SCSI routing instance and to see the number of active connections and the number of logins that have occurred since the Storage Router was last restarted (or since statistics were last cleared).

For example, the `show scsirouter stats` command in Example 19 shows that SCSI routing instance, **foo**, is currently active.

### Example 19: Results of "show scsirouter stats" Command

```
[SR2122_PR1]# show scsirouter foo stats

router status    started            iSCSI ver (Min/Max) logins active
foo    ACTIVE    Jan 11 23:06:08          2/2           10     7
```

## Handling Failover

In a cluster, storage routers continually exchange information as heartbeats to detect failures in the cluster. HA messages are sent using UDP over IP and, depending on the message type or situation, may be sent as unicast or multicast messages. To make sure that HA information is exchanged reliably between storage routers, the storage routers alternate transmission of heartbeats between the management and the HA interfaces.

Failover of SCSI routing instances is automatic when the Storage Router detects that another Storage Router in the cluster is no longer responding to heartbeats. Failover of a SCSI routing instance also occurs if the associated Gigabit Ethernet interface is unavailable or if all targets are unavailable.

**Note:** If some targets are available but others are not, failover of the SCSI routing instance does not occur.

Each cluster supports up to 12 active SCSI routing instances. Since each Storage Router can also support up to 12 SCSI routing instances, high availability is ensured for each instance in the cluster (regardless of the division of those instances between storage routers).

## Manual Failover

While failover of SCSI routing instances is automatic, there may be times when you wish to manually move a SCSI routing instance from one Storage Router to another. The move may be temporary, after which the instance will be moved back to its original location. At other times, you may want to move a SCSI routing instance permanently to another Storage Router, ensuring that the instance will continue running on the specified Storage Router whenever possible.

As an example cluster scenario, a cluster is composed of two storage routers, **StorageRouterSys1** and **StorageRouterSys2**. **StorageRouterSys1** is currently running instances, **scsi1** and **scsi2**, and is the primary Storage Router for both instances. **StorageRouterSys2** is currently running instances, **scsi3** and **scsi4**. The primary attribute for **scsi3** and **scsi4** is set to the default setting of **none**, indicating no preferred Storage Router for failover for either instance.

## Failover as Temporary Move

Referring to the example cluster scenario just described, the following procedure moves the SCSI routing instance, **scsi1**, from its primary, or preferred, Storage Router, **StorageRouterSys1**, to the other Storage Router on a temporary basis. The commands in this procedure are issued from a CLI session from Storage Router, **StorageRouterSys1**.

1. `enable` — Enter Administrator mode.
2. `show cluster` or `show scsirouter` *`scsi1`* `stats` — Verify that the instance to be moved, **scsi1**, is indeed running on Storage Router, **StorageRouterSys1**.
3. `failover scsirouter` *`scsi1`* — Failover SCSI routing instance, **scsi1**.

**Note:** Because there are only two storage routers in the cluster, you do not need to specify the failover destination.

4. `show  cluster` or `show scsirouter  ` *`scsi1`* `stats` — Verify that the specified SCSI routing instance, **scsi1**, is no longer running on the Storage Router, **StorageRouterSys1**.

Once the failover is complete, establish a Telnet session to **StorageRouterSys2** and verify — using CLI commands described in Step 1 and Step 2 above — that the SCSI routing instance, **scsi1**, is now running on that Storage Router.

This is considered a temporary move because **StorageRouterSys1** is still designated as the primary Storage Router for the SCSI routing instance, **scsi1**. If, for example, **StorageRouterSys1** is rebooted, **scsi1** will stop running on **StorageRouterSys2** and will start up and run on **StorageRouterSys1**.

**Note:** Use caution if you change the configuration of a SCSI routing instance while it is running on the Storage Router that is not the instance's configured primary Storage Router. If the instance's configuration changes while the designated primary Storage Router for that instance is down (or otherwise removed from the cluster), the changes will not be propagated to that Storage Router. When the primary Storage Router reboots (or otherwise returns to the cluster), it will reassert itself as the primary and will start to run the instance using the last configuration it had before leaving the cluster.

## Failover as Permanent Move

Referring to the example cluster scenario previously described, the following procedure moves the SCSI routing instance, **scsi2**, from its primary, or preferred, Storage Router, **StorageRouterSys1**, to the other Storage Router on a permanent basis. The commands in this procedure are issued from a CLI session from Storage Router, **StorageRouterSys1**.

1. `enable` — Enter Administrator mode.
2. `show cluster` or `show scsirouter` *`scsi2`* `stats` — Verify that the instance to be moved, **scsi2**, is indeed running on Storage Router, **StorageRouterSys1**.
3. `scsirouter` *`scsi2`* `primary` *`StorageRouterSys2`* — Set **StorageRouterSys2** as the primary Storage Router for the desired SCSI routing instance, **scsi2**.
4. `save scsirouter` *`scsi2`* `bootconfig` — Save the current SCSI routing instance configuration, including the primary setting, and circulate the changed configuration around the cluster.
5. `failover scsirouter` *`scsi2`* — Failover the desired SCSI routing instance, **scsi2**.

Once the failover is complete, establish a Telnet session to **StorageRouterSys2** and verify — using the `show scsirouter scsi2` command — that the SCSI routing instance, **scsi2**, is now running on **StorageRouterSys2** and that **StorageRouterSys2** is designated as the primary Storage Router for that instance.

## Failover for Distribution Purposes

In the example cluster scenario previously described, there is a significant increase in traffic for SCSI routing instance, **scsi4**, and as a result, you decide to distribute all of the other instances (**scsi1**, **scsi2**, and **scsi3**) to the **StorageRouterSys1** Storage Router. **StorageRouterSys1** is already running **scsi1** and **scsi2**.

The following procedure moves the SCSI routing instance, **scsi3**, to **StorageRouterSys1**. The commands in this procedure are issued from a CLI session from Storage Router, **StorageRouterSys2**:

1. `enable` — Enter Administrator mode.
2. `show cluster or show scsirouter` *`scsi3`* `stats` — Verify that the SCSI routing instance to be moved is indeed running on Storage Router, **StorageRouterSys2**.
3. `failover scsirouter` *`scsi3`* `to` *`StorageRouterSys1`* — Failover the desired SCSI routing instance, **scsi3**, to **StorageRouterSys1**.

Once the failover is complete, establish a Telnet session to **StorageRouterSys1** and verify — using the `show scsirouter` command — that instances, **scsi1**, **scsi2**, and **scsi3**, are now running there.

**Note:** Because **scsi3** has no primary setting, it will remain running on **StorageRouterSys1** until it is explicitly stopped or failed over, or until it automatically fails over because an interface is unavailable or a software or hardware problem occurred.

# Managing CDP on the Storage Router

Cisco Discovery Protocol (CDP) is primarily used to obtain protocol addresses of neighboring devices and to discover the platform of those devices. CDP is media- and protocol-independent and runs on all Cisco-manufactured equipment including routers, bridges, access servers, and switches.

Each device configured for CDP sends periodic messages, known as advertisements, to a multicast address. Each device advertises at least one address at which it can receive SNMP messages. The advertisements also contain time-to-live, or holdtime, information, which indicates the length of time a receiving device should hold CDP information before discarding it. Each device also listens to the periodic CDP messages sent by others in order to learn about neighboring devices and determine when their interfaces to the media go up or down.

The Storage Router is enabled, by default, to exchange CDP information with other CDP-enabled devices in the network. CDP can be enable or disabled for individual interfaces on the Storage Router, and the holdtime for receiving devices and the frequency of CDP transmissions from the Storage Router can be modified.

## Disable CDP for Selected Interfaces

CDP can be enabled or disabled for the management, HA, and Gigabit Ethernet interfaces on the Storage Router. By default, all interfaces are enabled for CDP. Use the following procedure to disable CDP for an interface:

1. `enable` — Enter Administrator mode.
2. `no cdp interface` *`ge2`* `enable` — Disable CDP on the desired interface **ge2**.
3. `show cdp interface` — Confirm that CDP is disabled for the interface.
4. `save system bootconfig` — Save the CDP change to the Storage Router's bootable configuration. (Optional)

## Modify the CDP Holdtime and Timeout Values

Holdtime is the amount of time the receiving device should hold a CDP packet from the Storage Router before discarding it. The CDP holdtime value must be set to a higher number of seconds than the CDP timer value (the time between CDP transmissions from the Storage Router). For example, the default CDP holdtime value is **180 seconds**. The default CDP timer value is **60 seconds**.

Use the following procedure to change the CDP holdtime value and the CDP timer value:

1. `enable` — Enter Administrator mode.
2. `show cdp` — Verify the current CDP configuration.
3. `cdp holdtime` *`300`* — Set the number of seconds **300** that a receiving device should hold the storage router CDP packet.
4. `cdp timer` *`120`* — Set the number of seconds **120** between transmissions of CDP packets from the Storage Router.
5. `show cdp` — Verify the new CDP configuration. (Optional)
6. `save system bootconfig` — Save the CDP changes to the Storage Router’s bootable configuration. (Optional)

## Using Scripts to Automate Tasks

If you frequently issue a series of CLI commands, you can save time by entering those commands into a script for execution purposes. Command scripts are stored in the `script` directory and are simply ASCII text files containing CLI commands.

Follow these rules when creating a command script:

- Commands can start anywhere on a line. The first word on any line that is not preceded by a comment character is considered to be the start of a command string.
- Comments can be added by placing an exclamation point (!) or number sign (#) character at the beginning of the line or as the first character at any position in the line. Comments are useful for documenting the contents of the file and the expected results. Comments can also be used to prevent a command from executing without removing it from the file by inserting a comment character before the command string.
- You can extend commands across line boundaries by ending a line with a backslash ( \ ) as the continuation character (Example 20). Use the continuation character to make long commands more readable. The line sequence is continued until a command line without a continuation character is encountered. If a comment line is used to end a line continuation sequence, you must add a blank line after the comment.

  **Example 20: Extended Commands:**

  ```
  radius-server host 10.5.0.53 \
  auth-port 1644 \
  timeout 60 \
  retransmit 5
  ! Configure 1st RADIUS server

  radius-server host 10.6.0.61
  . . .
  ```

- Scripts can be invoked from other scripts.

When scripts run, the commands and any responses are echoed on the storage router console.

Scripts can be created on any system using any text editor and placed in the `script` directory (`/ata3/script`) of the target Storage Router using FTP. See the "Using FTP with the Storage Router" section on page 166 for details. You can also use the `copy` command to copy the script file to the Storage Router using HTTP or TFTP.

## Running Command Scripts

Use the following procedure to execute the CLI commands stored in a script file. In this example, the script file is named *CreateSc* and must exist in the `script` directory.

1. `enable` — Enter Administrator mode.
2. `show script` *`CreateSc`* — Verify that the script, **CreateSc**, exists in the `script` directory and that it contains the configuration that you want to recreate.
3. `read script` *`CreateSc`* `or read script` *`CreateSc force`* — Read and execute the CLI commands in the script file. When prompted, confirm that you want to continue and execute the script commands.

   Use the **force** keyword to execute the script immediately without asking for confirmation. (Optional)

After the script completes, issue the appropriate `show` commands to verify that the script executed as expected.

## Managing the Log File

The Storage Router can log event information to a series of log files, based on the routing rules specified in the storage router logging table. The default configuration routes all storage router event messages at notification level info or lower to the log file. Use the `show logging` commands to display log file entries and to search for entries that match specific text strings or regular expressions.

Log files are created in the storage router `log` directory (`/ata4/log`). They can occupy up to 4 MB of memory. Once this limit has been reached, the oldest file is removed and a new one is created. The `show logging size` command can be used to display the size of the existing log files. The `show system` command can be used to display the amount of space allocated to log files, and the amount of log file space currently available.

The name of the log file is *messages*, followed by a number (for example, *messages3* or *messages12*). The first log file is named *messages0*, the next log file is named *messages1*, and so on.

Depending on the needs of your enterprise, you can archive log files to a remote server, or you can clear log files on a periodic basis. You can use FTP to transfer files from the Storage Router to a remote server (see the “Using FTP with the Storage Router” section on page 166 for details), or you can use the web-based GUI to display the contents of the log file and use cut-and-paste techniques to save the information to a local file. You can also issue the `show logging all` command and redirect the output of your console using the logging facilities for your specific console interface.

**Note:** See the “Understanding Logging” section on page 168 for more information about adding routing rules to the storage router logging table.

## Clearing the Log Files

Use the following procedure to periodically clear the storage router log files.

1. `enable` — Enter Administrator mode.
2. `show logging size` — Check the current size of the storage router log files (Example 21).
3. `show logging all` or `show logging last` *`50`* — Display all the current log file entries (first command), or display a selected number of entries, such as **50**, from the end of the file (second command).
4. `clear log` — Clear the existing log file. The Storage Router clears the existing log file and starts a new log file.

**Example 21: Results of “show logging size” Command**

```
[SR2122_PRA]# show logging size
5120 messages (342797 bytes) logged
```

# Gathering Troubleshooting Information

If you experience problems with the Storage Router, you may need to obtain troubleshooting information for HP technical support personnel. The Storage Router provides several features that can help you assemble the necessary information.

The following are typical activities involved with troubleshooting the Storage Router:

- Using the Crash Log, page 164
- Using FTP with the Storage Router, page 166
- Understanding Diagnostics, page 168
- Capturing System Messages at Bootup, page 168
- Understanding Logging, page 168
- Capturing the Storage Router Configuration, page 172
- Using Debug Facilities, page 172

## Using the Crash Log

If the storage router experiences an unexpected problem that forces it to automatically reboot, a special log file is generated. The file is named *crash.txt* and is stored in the `log` directory (`/ata4/log`). You can display the contents of this file to the console using the `show crash` command.

To save the `show crash` command output, redirect the output of your console using the logging facilities for your specific console interface. Depending on your console interface and scroll buffer size, you may also be able to copy and paste the contents from your console into an ASCII text file.

The crash log provides the following information:

- Exception information
- Boot information, including the kernel version and creation date
- Software information
- A list of all tasks, including entry point, task ID and priority for each task
- Task registers and stack trace for each task in the task list
- Net job ring
- A list of all modules, including module ID, data start addresses, and so on.

- A list of all devices and associated drivers
- A list of all drivers, including the number of create, delete, open, close, read, write, and I/O control actions performed
- A list of free memory addresses and a summary of memory usage information
- A list of open file descriptors
- Network interface information, including flags, interface type, addresses, and MTU information for all storage router interfaces
- The storage router route table
- The ARP table
- The storage router host table
- Active Internet connection information, including PCB, connection type (TCP or UDP), receive and send queues, local and foreign addresses, and state for each connection
- Routing statistics
- IP statistics
- ICMP statistics
- TCP statistics
- UDP statistics
- Network stack data pool (MBufs) and cluster pool table information
- NFS authorization
- Mounted NFS file system information
- IDE disk or Flash information, including device types and parameters
- Registered crash dump functions
- Sample registered dump functions
- CPC710 registers at time of exception

Information used to create the *crash.txt* file is periodically written to the *tmpcrash.txt* file in the `log` directory. If a crash occurred at the current time, use the `show crash current` command to display the information as it would be written to the crash log.

## Using FTP with the Storage Router

In certain cases, you may want to copy log files from the Storage Router to another server in your network for analysis purposes, or you may want to copy configuration or script files to another server prior to making them available to another Storage Router. The Storage Router includes an FTP daemon; however, the FTP port (**port 21**) is, by default, **restricted**.

Use the following procedure to enable FTP and to copy the current message log file from the Storage Router to another server in the network.

1. `enable` — Enter Administrator mode.
2. `show restrict` — Display interface restrictions. If port 21 on the management interface **fei0** is closed, use the command in Step 3 to open it.
3. `no restrict mgmt ftp` — Allow FTP functions on the management interface. (Optional)

Once the function is enabled, open the FTP session to the Storage Router from the server. You will be prompted for a user name and password. The user name is *`admin`* and the password is the Storage Router Administrator password. The default Administrator password is **hp**.

**Note:** The user name and the password are case-sensitive.

The storage router log files and crash trace files are stored in the `/ata4/log` directory. Saved configuration files are stored in the `/ata3/savedconfig` directory. Script files are stored in the `/ata3/script` directory.

To use FTP to retrieve the storage router log file, change to the `/ata4/log` directory using the `FTP cd` command. List the files to determine what log file you want to retrieve. (In our example, the log file is *messages0*.) If necessary, specify the binary flag using the `FTP binary` command. Issue the `FTP get` command to retrieve the log file and to copy it to the specified file on your server. When the process completes, close the FTP connection using the `FTP bye` command.

Example 22 illustrates the FTP session just described. In this example, the storage router management interface IP address is **10.1.11.210**.

### Example 22: FTP Session

```
Server1> ftp 10.1.11.210
Connected to 10.1.11.210.
220 VxWorks (5.4.1) FTP server ready
Name: admin
331 Password required
Password:********
230 User logged in
ftp> cd /ata4/log
250 Changed directory to "/ata4/log"
ftp> dir
200 Port set okay
150 Opening ASCII mode data connection
size           date       time      name
--------       ------     ------    --------
     512    Apr-09-2002  20:46:18   .        <DIR>
     512    Apr-09-2002  20:46:18   ..       <DIR>
   13803    May-16-2002  15:13:56   messages0
   92167    Apr-10-2002  19:14:06   tmpcrash.txt

226 Transfer complete
ftp: 374 bytes received in 0.02Seconds 23.38Kbytes/sec.
ftp> binary
200 Type set to I, binary mode
ftp> get
(remote-file) messages0
(local-file) SR2122Sys1_Messages
200 Port set okay
150 Opening BINARY mode data connection
226 Transfer complete
40863 bytes received in 0.049 seconds (8.1e+02 Kbytes/s)
ftp> bye
221 Bye...see you later
```

If you had to remove the restriction on the management interface before proceeding with the FTP session, return to the storage router CLI session and re-enable the restriction, using the following procedure.

1. `show restrict` — Verify that port 21 on the management interface is currently open.
2. `restrict mgmt ftp` — Close the management interface to FTP functions. No FTP functions will be allowed.

## Understanding Diagnostics

The Storage Router performs hardware diagnostics when the unit is powered up. Hardware diagnostics cannot be bypassed. If a hardware diagnostic fails, the Storage Router halts. The boot process cannot be re-initiated.

If you experience a hardware diagnostic failure, contact HP technical support personnel as described in the “HP Technical Support” section in the “About this Guide” Chapter on page xv for further instructions.

The Storage Router performs additional “soft” diagnostics after the hardware diagnostics complete on power up and after every system reboot. If necessary, the soft diagnostics can be bypassed.

If you experience problems with soft diagnostics, contact HP technical support personnel for assistance.

## Capturing System Messages at Bootup

The storage router logs a variety of messages to the console during the system boot process. If you are experiencing problems with the Storage Router, it may be helpful to capture these messages. Use the console interface to perform the boot process and capture the console log using typical external methods.

## Understanding Logging

The Storage Router generates a variety of system event messages. All storage router event and debug messages are issued in the following format:

### Example 23: Event Message

```
Mar 18 11:48:05: %SNMP-5-SASAS: SnmpApp starting...
<timestamp>: %<facility>-<level_number>-<mnemonic>: <message text>
```

All messages are assigned a notification level, which reflects the priority of the message in the system. Messages with the highest priority are assigned a notification level of emergency. Messages at this level indicate that the system is unusable. Messages with the lowest priority are assigned a notification level of debug. Messages at this level are for troubleshooting purposes. In Example 23, the message level number is **5**, indicating a notification level of notice.

Table 16 lists the notification levels, their level number, and their descriptions.

**Table 16: Event Message Notification Levels.**

| Notification Level | Level Number | Description |
|---|---|---|
| emergency | 0 | System unusable |
| alert | 1 | Immediate action needed |
| critical | 2 | Critical conditions |
| error | 3 | Error conditions |
| warning | 4 | Non-fatal warning conditions |
| notice | 5 | Normal but significant conditions |
| info | 6 | Informational messages only |
| debug | 7 | Information for troubleshooting purposes |

Event, trace and debug messages can be routed to various destinations, based on the notification level of the message and the application area (facility) that generated the message. Table 17 lists the logging destinations and their descriptions; Table 18 lists the logging facilities and their descriptions.

**Table 17: Event Message Logging Destinations**

| Destination | Description |
|---|---|
| all | Logs the message to all destinations |
| none | The message is not logged; it is discarded. |
| console | The message is logged to a serial console CLI session. |
| logfile | The message is logged to the storage router log file. |
| rslog | The message is logged to a remote syslog server. Use the `logging syslog` command to specify the IP address of the remote syslog server. |
| vty | The message is logged to all Telnet or other virtual terminal CLI sessions. |

**Table 18: Event Massage Facilities**

| Facility | Description |
|---|---|
| AUTH | AAA authentication |
| CDP | Cisco Discovery Protocol |
| CONF | Configuration functions |
| FC | Storage Router Fibre Channel interfaces |
| GE | Storage Router Gigabit Ethernet interfaces |
| HA | Storage Router High Availability clusters |
| IF | Interface manager |
| INVALID | Generic functions |
| IPROUTER | Storage Router IP functions |
| ISCSI | iSCSI functions |
| MON | Hardware monitor |
| SNMP | Simple Network Management Protocol |
| SNMP | Simple Network Management Protocol |
| SYSLOG | Syslog functions |
| UI | Storage Router user interface |

Messages are routed by creating a list of routing rules that is searched for a facility and notification level match whenever an event or debug message is received. This list of routing rules is known as the storage router logging table.

By default, the logging table includes rules to log all messages at notification level `notice` (or numerically lower levels) to all destinations, and to log all messages at notification level `info` to the storage router log file. Any message that does not find a matching rule is not logged to any destination.

Use the `show logging` command to display the current logging table routing rules and other logging information.

## Filtering and Routing Event Messages

The storage router logging table allows messages to be filtered by their facility and notification level and routed to the specified destination(s). When an event message arrives, the logging table rules are searched by facility name and by level until the first match is found. The message is sent to all the destinations specified by the matching rule. If no match is found, the event message is discarded.

When a new routing rule is added, it is appended to the existing table. Use the `logging level` command to add a new routing rule to the logging table; use the `logging #?` command to insert a routing rule into the logging table before the specified entry.

Each facility can have eight notification levels. Each facility and notification level pair can have up to seven destinations.

In Example 24, the facility is SNMP, and the notification level is 5 (notice). If the logging table included the entries in Example14, the event message in Example 24 would match on the first routing rule, and would be sent to all valid destinations. Any message from the SNMP facility at notification level info, and any message from another facility at notification level info (or lower) would match on the second rule and be sent to the storage router console and log file. All messages from any facility at notification level **debug** would be discarded.

### Example 24: Example Log Route Entries List

```
Index  Level    Priority  Facility  Route
1      notice   5         SNMP      all
2      info     6         all       console log file
```

The logging table can be saved and retained across the storage router restart. The order of the rules in the logging table is preserved when entries are deleted.

## Enabling and Disabling Logging

Logging is enabled by default. By default, the Storage Router includes the following routing rules in the logging table:

- All messages at notification level notice or lower are logged to all valid destinations.
- All messages at notification level info are logged to the storage router log file.
- All debug messages are discarded.

Use the `no logging on` command to quickly disable logging for all destinations without modifying the storage router logging table. No logging will take place until logging is re-enabled by the `logging on command`.

If you clear the logging table without returning to the factory defaults, all rules are removed from the logging table. This causes all messages to be discarded because there are no matching rules in the logging table. To resume logging, you can add new routing rules, restore a previously saved logging table, or clear the logging table back to the factory defaults.

### Viewing and Saving the Log File

You can view the entire storage router log file or selected portions of the log file using the `show logging` command. You can also view the log file using the web-based GUI. If you want to analyze or search the log file in more detail, you can use FTP to retrieve a copy of the log file. See the "Using FTP with the Storage Router" section on page 166 for details.

For additional information about managing the storage router log file, see the "Managing the Log File" section on page 162.

## Capturing the Storage Router Configuration

You can use the `show runningconfig` or `show bootconfig` command to display the Storage Router's current running configuration or bootable configuration. You can then redirect this display to create a script file in the Storage Router's `script` directory. The resulting file can be used as a basis to create command scripts to automate common tasks. See the "Using Scripts to Automate Tasks" section on page 160 for more details.

## Using Debug Facilities

The Storage Router includes debug facilities for SCSI routing instances. Running debug traces can impact the operation of the Storage Router. If you experience problems with a SCSI routing instance that cannot be resolved, HP technical support personnel may ask you to capture some debug traces. They will assist you to properly configure the Storage Router to accomplish this task. By default, debug facilities are disabled for all SCSI routing instances.

# Technical Specifications

A

This appendix gives details about the technical specification of the Storage Router.

# Specifications

This appendix lists the technical specifications in Table 19.

**Table 19: Storage Router Specifications**

| Specifications | |
|---|---|
| **Environmental** | |
| Temperature, ambient operating | 50 to 95°F (10 to 35°C) |
| Temperature, nonoperating and storage | -20 to 140°F (-30 to 60°C) |
| Humidity (RH), ambient (non-condensing) operating | 10 to 70 percent non-condensing |
| Humidity (RH), ambient (non-condensing) nonoperating and storage | 5 to 95 percent non-condensing |
| Altitude, operating and nonoperating | -500 to 10000 ft (-152.4 to 3048 m) |
| **Physical Characteristics** | |
| Dimensions (H x W x D) | 1.75 x 17.44 x 16.13 in.<br>(4.45 x 44.3 x 40.97 cm) 1 RU[1] |
| Weight | 11.25 lb (5.1 kg) |
| **AC power** | |
| Power supply output | 70W |
| System power dissipation | 50W |
| AC current | 1.0A maximum @ 100 to 240 VAC |
| AC frequency | 50 to 60 Hz |
| Airflow | Right side in, left side out |
| Fuse (F1) rating | 3.15A, 250 VAC, time delay, not field-serviceable |

[1] RU = Rack Unit

# B

# Cable and Port Pinouts

This appendix provides cable and port pinout information for the Storage Router and includes the following sections:

# Gigabit and Fibre Channel Ports

Table 20 lists the types of SFP modules and connectors used with the Gigabit Ethernet and Fibre Channel ports in the Storage Router. For more information about the SFP modules and connectors, see the standards for the SFP modules and connectors.

**Table 20: SFP Modules and Connectors**

| Port | Compliance | Connector | Medium |
|---|---|---|---|
| Gigabit Ethernet, GE 1 and GE 2 | 1000 Base-SX | MT-RJ | Fiber-optic |
| | | LC | Fiber-optic |
| Fibre Channel, FC 1 and FC 2 | FC-PI 100/200-M5-SN-I<br>and<br>FC-PI 100/200-M6-SN-I | LC | Fiber-optic |

# 10/100 Ethernet Management and HA Ports

Use modular, RJ-45, straight-through UTP cables to connect the 10/100 Ethernet ports to end systems. Use modular, RJ-45 cross-connect cables to connect to external switches and routers. Figure 45 shows straight-through cables and Figure 46 shows cross-connect cables.

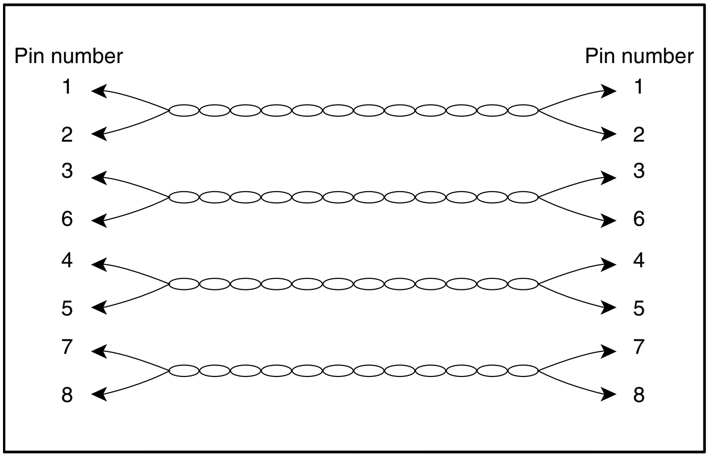


**Figure 45: Straight-through cables**

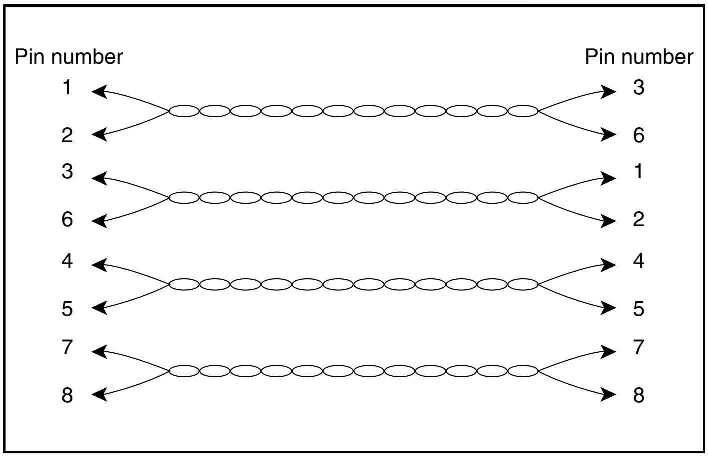


**Figure 46: Cross-connect cables**

The 10/100 Ethernet ports support RJ-45 connectors. Table 21 lists the signals for RJ-45 connector pinouts.

**Table 21: 10/100 Ethernet Management and HA Port Pinouts**

| Pin | Signal | Direction | Description |
|---|---|---|---|
| 1 | TD_P | Output | Transmit Data + |
| 2 | TD_N | Output | Transmit Data - |
| 3 | RD_P | Input | Receive Data + |
| 4 | | | Terminated |
| 5 | | | Terminated |
| 6 | RD_N | Input | Receive Data - |
| 7 | | | Terminated |
| 8 | | | Terminated |

# Console Port

The console port is an EIA/TIA-232 port with a female 8-pin RJ-45 receptacle. Use the rollover cable supplied with the Storage Router to connect to the console port. (see Figure 47.) Table 22 lists the console port pinouts.

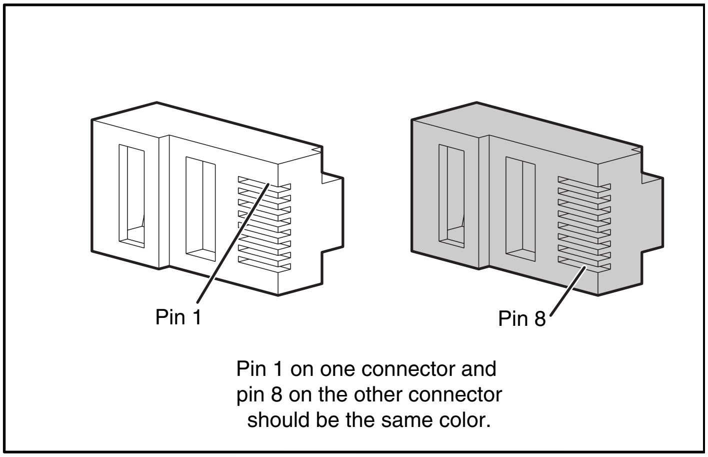

Pin 1
Pin 8
Pin 1 on one connector and pin 8 on the other connector should be the same color.

**Figure 47: Rollover cable for connection to console port**

**Table 22: Console Port Pinouts**

| Pin | Signal | Direction | Description |
|---|---|---|---|
| 1 | RTS | Output | Request to Send |
| 2 | — | — | Not Connected |
| 3 | TxD_N | Output | Transmitted Data |
| 4 | GND | — | Signal Ground |
| 5 | GND | — | Signal Ground |
| 6 | RxD_N | Input | Receive Data - |
| 7 | — | — | Not Connected |
| 8 | CTS | Input | Clear to Send |

The console port uses a subset of the EIA/TIA-232 signals. Only the signals TxD_N, RxD_N, CTS and RTS are connected.

**Note:** The modem control signals are not connected; to access the Storage Router remotely through the console port, you should do so through a terminal server.

# Regulatory Compliance Notices

C

## Regulatory Compliance Identification Numbers

For the purpose of regulatory compliance certifications and identification, your product has been assigned a unique HP Series Number. The series number can be found on the product label, along with the required approval markings and information. When requesting compliance information for this product, always refer to this series number. The series number should not be confused with the marketing name or model number of the product.

## Federal Communications Commission Notice

Part 15 of the Federal Communications Commission (FCC) Rules and Regulations has established Radio Frequency (RF) emission limits to provide an interference-free radio frequency spectrum. Many electronic devices, including computers, generate RF energy incidental to their intended function and are, therefore, covered by these rules. These rules place computers and related peripheral devices into two classes, A and B, depending upon their intended installation. Class A devices are those that may reasonably be expected to be installed in a business or commercial environment. Class B devices are those that may reasonably be expected to be installed in a residential environment (for example, personal computers). The FCC requires devices in both classes to bear a label indicating the interference potential of the device as well as additional operating instructions for the user.

The rating label on the device shows the classification (A or B) of the equipment. Class B devices have an FCC logo or FCC ID on the label. Class A devices do not have an FCC logo or FCC ID on the label. After the Class of the device is determined, refer to the corresponding statement in the following sections.

## Class A Equipment

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at personal expense.

## Class B Equipment

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit that is different from that to which the receiver is connected
- Consult the dealer or an experienced radio or television technician for help

## Declaration of Conformity for Products Marked with the FCC Logo, United States Only

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

For questions regarding your product, contact us by mail or telephone:

- Hewlett-Packard Computer Corporation
  P. O. Box 692000, Mail Stop 530113
  Houston, Texas 77269-2000
- 1-800-652-6672 (1-800-OK COMPAQ) (For continuous quality improvement, calls may be recorded or monitored.)

For questions regarding this FCC declaration, contact us by mail or telephone:

- Hewlett-Packard Computer Corporation
  P. O. Box 692000, Mail Stop 510101
  Houston, Texas 77269-2000
- 1-281-514-3333

To identify this product, refer to the part, series, or model number found on the product.

## Modifications

The FCC requires the user to be notified that any changes or modifications made to this device that are not expressly approved by Hewlett-Packard Computer Corporation may void the user’s authority to operate the equipment.

## Cables

Connections to this device must be made with shielded cables with metallic RFI/EMI connector hoods in order to maintain compliance with FCC Rules and Regulations.

## Power Cords

The power cord set included in your server meets the requirements for use in the country where you purchased your server. If you need to use this server in another country, you should purchase a power cord that is approved for use in that country.

The power cord must be rated for the product and for the voltage and current marked on the product's electrical ratings label. The voltage and current rating of the cord should be greater than the voltage and current rating marked on the product. In addition, the cross sectional area of the wire must be a minimum of 1.00 mm$^2$ or 18AWG, and the length of the cord must be between 6 feet (1.8 m) and 12 feet (3.6 m). If you have questions about the type of power cord to use, contact your HP authorized service provider.

A power cord should be routed so that it is not likely to be walked on or pinched by items placed upon it or against it. Particular attention should be paid to the plug, electrical outlet, and the point where the cord exits from the product.

# Mouse Compliance Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

# Canadian Notice (Avis Canadien)

## Class A Equipment

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

## Class B Equipment

This Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

# European Union Notice

Products with the CE Marking comply with both the EMC Directive (89/336/EEC) and the Low Voltage Directive (73/23/EEC) issued by the Commission of the European Community.

Compliance with these directives implies conformity to the following European Norms (the equivalent international standards are in parenthesis):

- EN55022 (CISPR 22) – Electromagnetic Interference
- EN55024 (IEC61000-4-2, 3, 4, 5, 6, 8, 11) – Electromagnetic Immunity
- EN61000-3-2 (IEC61000-3-2) – Power Line Harmonics
- EN61000-3-3 (IEC61000-3-3) – Power Line Flicker
- EN60950 (IEC950) – Product Safety

# Japanese Notice

ご使用になっている装置にVCCIマークが付いていましたら、次の説明文をお読み下さい。

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。

VCCIマークが付いていない場合には、次の点にご注意下さい。

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です　この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

## Taiwanese Notice

警告使用者：

這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

## Laser Device

All HP systems equipped with a laser device comply with safety standards, including International Electrotechnical Commission (IEC) 825. With specific regard to the laser, the equipment complies with laser product performance standards set by government agencies as a Class 1 laser product. The product does not emit hazardous light; the beam is totally enclosed during all modes of customer operation and maintenance.

### Laser Safety Warnings

**WARNING:** To reduce the risk of exposure to hazardous radiation:

- Do not try to open the laser device enclosure. There are no user-serviceable components inside.
- Do not operate controls, make adjustments, or perform procedures to the laser device other than those specified herein.
- Allow only HP authorized service technicians to repair the laser device.

## Compliance with CDRH Regulations

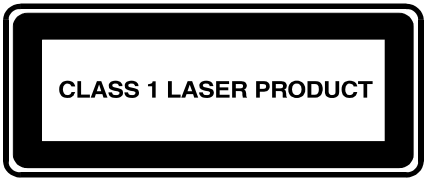
The Center for Devices and Radiological Health (CDRH) of the U.S. Food and Drug Administration implemented regulations for laser products on August 2, 1976. These regulations apply to laser products manufactured from August 1, 1976. Compliance is mandatory for products marketed in the United States.

## Compliance with International Regulations

All HP systems equipped with laser devices comply with appropriate safety standards including IEC 825.

## Laser Product Label

The following label or equivalent is located on the surface of the HP supplied laser device.



CLASS 1 LASER PRODUCT

This label indicates that the product is classified as a CLASS 1 LASER PRODUCT. This label appears on a laser device installed in your product.

## Laser Information

**Table 23: Laser Information**

| Feature | Description |
|---|---|
| Laser type | Semiconductor GaAIAs |
| Wave length | 780 nm +/- 35 nm |
| Divergence angle | 53.5 degrees +/- 0.5 degrees |
| Output power | Less than 0.2 mW or 10,869 W m-2 sr-1 |
| Polarization | Circular 0.25 |
| Numerical aperture | 0.45 inches +/- 0.04 inches |

# Electrostatic Discharge

D

To avoid damaging the system, be aware of the precautions you need to follow when setting up the system or handling parts. A discharge of static electricity from a finger or other conductor may damage system boards or other static-sensitive devices. This type of damage may reduce the life expectancy of the device.

To prevent electrostatic damage, observe the following precautions:

- Avoid hand contact by transporting and storing products in static-safe containers.
- Keep electrostatic-sensitive parts in their containers until they arrive at static-free workstations.
- Place parts on a grounded surface before removing them from their containers.
- Avoid touching pins, leads, or circuitry.
- Always be properly grounded when touching a static-sensitive component or assembly.

## Grounding Methods

There are several methods for grounding. Use one or more of the following methods when handling or installing electrostatic-sensitive parts:

- Use a wrist strap connected by a ground cord to a grounded workstation or computer chassis. Wrist straps are flexible straps with a minimum of 1 megohm ± 10 percent resistance in the ground cords. To provide proper ground, wear the strap snug against the skin.
- Use heel straps, toe straps, or boot straps at standing workstations. Wear the straps on both feet when standing on conductive floors or dissipating floor mats.
- Use conductive field service tools.
- Use a portable field service kit with a folding static-dissipating work mat.

If you do not have any of the suggested equipment for proper grounding, have a HP authorized reseller install the part.

**Note:** For more information on static electricity, or assistance with product installation, contact your HP authorized reseller.

# index