Cisco Systems

Beta Draft—Cisco Confidential Information

Cisco IOS XR Getting Started Guide

Cisco IOS XR Software Release 3.4

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-10957-01

Cisco IOS XR Getting Started Guide

CHAPTER 4

CHAPTER 6

Preface

This guide describes how to create the initial configuration for a router using the Cisco IOS XR software. This guide also describes how to complete additional administration, maintenance, and troubleshooting tasks that may be required after initial configuration.

This preface contains the following sections:

Changes to This Document

Table 1 lists the technical changes made to this document since it was first printed.

Table 1 Changes to This Document

Revision	Date	Change Summary
OL-10957-01	July 2006	Initial release of the document.

About This Document

The following sections provide information about *Cisco IOS XR Getting Started Guide* and related documents:

Intended Audience

This document is intended for the following people:

- Experienced service provider administrators
- Cisco telecommunications management engineers
- Third-party field service technicians who have completed the Cisco IOS XR software training sessions
- Customers who daily use and manage routers running Cisco IOS XR software

Organization of the Document

This document contains the following chapters:

- Chapter 1, "Introduction to Cisco IOS XR Software"
- Chapter 2, "Bringing Up the Cisco IOS XR Software on a Standalone Router"
- Chapter 3, "Bringing Up the Cisco IOS XR Software on a Multishelf System"
- Chapter 4, "Configuring General Router Features"
- Chapter 5, "Configuring Additional Router Features"
- Chapter 6, "CLI Tips, Techniques, and Shortcuts"
- Chapter 7, "Troubleshooting the Cisco IOS XR Software"
- Appendix A, "Understanding Regular Expressions, Special Characters, and Patterns"

Related Documents

For a complete listing of available documentation for the Cisco IOS XR software and the routers on which it operates, see the following Web pages:

- Cisco IOS XR Software Documentation

  http://www.cisco.com/univercd/cc/td/doc/product/ioxsoft/index.htm
- Cisco CRS-1 Carrier Routing System Documentation

  http://www.cisco.com/univercd/cc/td/doc/product/core/crs/
- Cisco 12000 Series Router Documentation

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/index.htm
- Cisco Catalyst 6509 Switch Documentation

  http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

Note Cisco IOS XR software runs only on the Cisco XR 12000 Series Routers listed in the "Supported Standalone System Configurations" section on page 1 in Chapter 1, "Introduction to Cisco IOS XR Software."

Conventions

This document uses the following conventions:

Item	Convention
Commands and keywords	**boldface** font
Variable for which you supply values	*italic* font
Displayed session and system information	`screen` font
Commands and keywords you enter in an interactive environment	**`boldface screen`** font
Variables you enter in an interactive environment	*`italic screen`* font
Menu items and button names	**boldface** font
Menu navigation	**Option > Network Preferences**

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Tip Means *the following information will help you solve a problem.* The information in tips might not be troubleshooting or an action, but contains useful information.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

CHAPTER 1

Introduction to Cisco IOS XR Software

This chapter introduces the routers that support Cisco IOS XR software and the user interfaces you can use to manage routers that run Cisco IOS XR software.

Contents

This chapter contains the following sections:

Supported Standalone System Configurations

The Cisco IOS XR software runs on the following standalone systems:

- Cisco CRS-1 4-Slot Line Card Chassis (LCC)
- Cisco CRS-1 8-Slot LCC
- Cisco CRS-1 16-Slot LCC
- Cisco XR 12006 Router
- Cisco XR 12008 Router
- Cisco XR 12010 Router
- Cisco XR 12012 Router
- Cisco XR 12016 Router
- Cisco XR 12404 Router
- Cisco XR 12406 Router
- Cisco XR 12410 Router
- Cisco XR 12416 Router

Note Many cards operate in both Cisco XR 12000 Series routers and in Cisco 12000 Series routers. For the latest information on which cards are supported by the Cisco IOS XR software in Cisco XR 12000 Series routers and Cisco 12000 Series routers, see *Release Notes for Cisco IOS XR Software Release 3.3*.

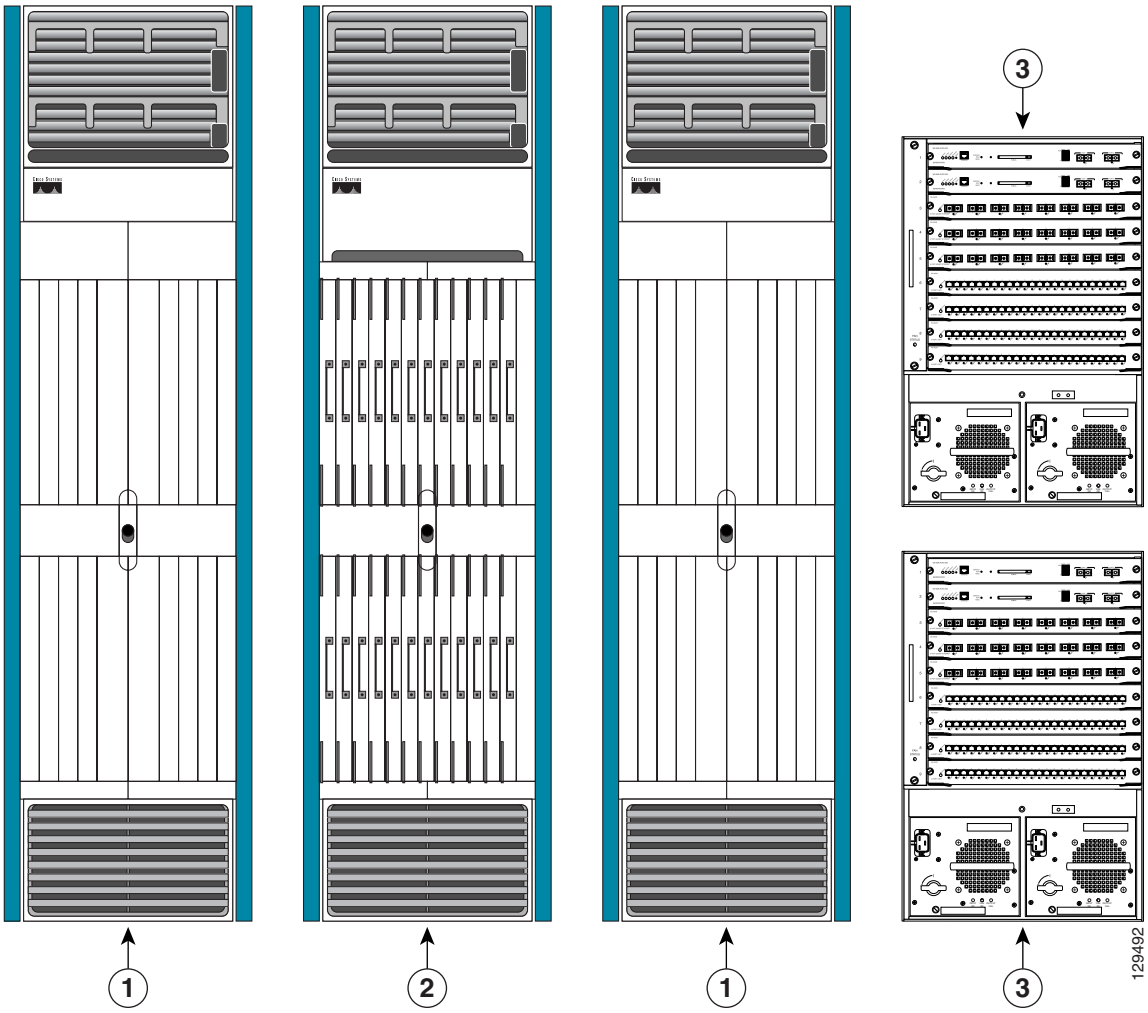
The Cisco IOS XR software also runs on Cisco CRS-1 Multishelf Systems, which are described in the following section.

Cisco CRS-1 Multishelf System Overview

The multishelf system enables multiple Cisco CRS-1 LCCs to act as a single system. This release of the multishelf system supports two 16-slot LCCs and one, two, or four fabric card chassis (FCCs) to provide a total switching capacity of up to 1.28 terabits per second (Tbps). Two external Cisco Catalyst switches provide control-plane connectivity between the chassis.

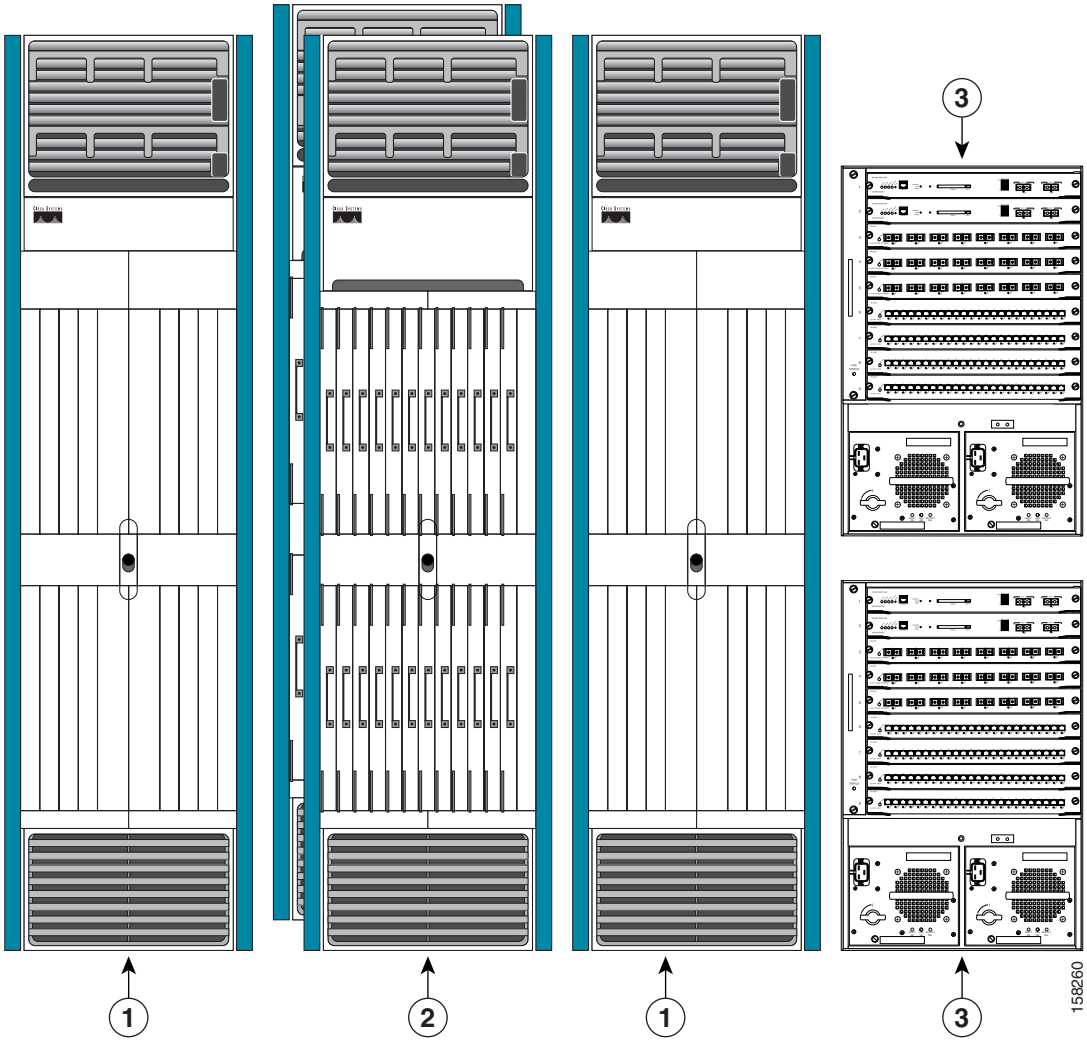
Figure 1-1 shows the single-FCC multishelf system, Figure 1-2 shows the two-FCC multishelf system, and Figure 1-3 shows the four-FCC multishelf system.

Figure 1-1 Single-FCC Multishelf System



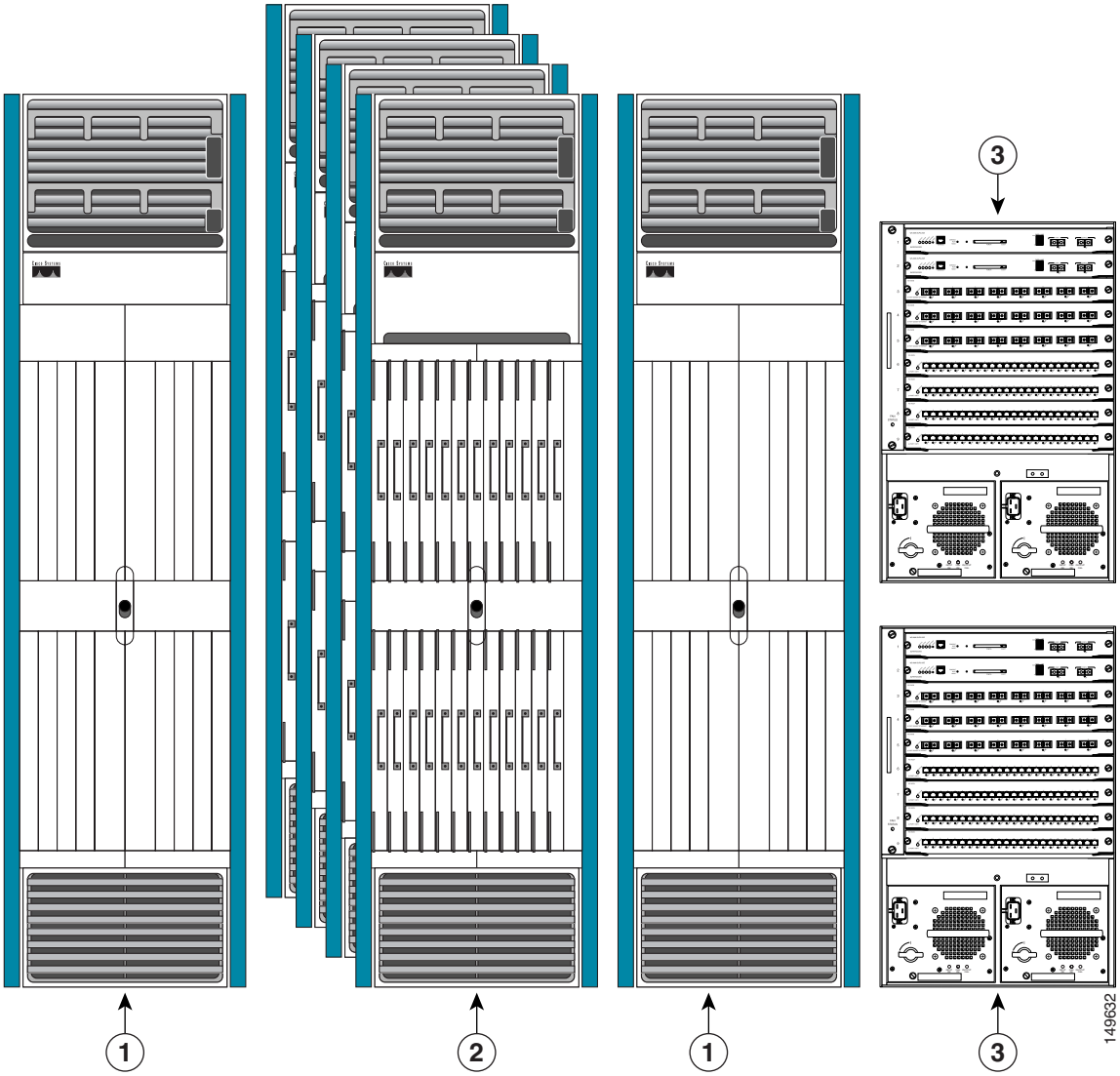
1	Cisco CRS-1 16-Slot Line Card Chassis (two required)	**3**	Cisco Catalyst 6509 Switch (two suggested)
2	Cisco CRS-1 Fabric Card Chassis (one required)		

Figure 1-2 Two-FCC Multishelf System



1	Cisco CRS-1 16-Slot Line Card Chassis (two required)	**3**	Cisco Catalyst 6509 Switch (two suggested)
2	Cisco CRS-1 Fabric Card Chassis (two required)		

Figure 1-3 Four-FCC Multishelf System



1	Cisco CRS-1 16-Slot Line Card Chassis *(*two required*)*	**3**	Cisco Catalyst 6509 Switch (two suggested)
2	Cisco CRS-1 Fabric Card Chassis *(*four required*)*		

For more information on multishelf systems, see Chapter 3, "Bringing Up the Cisco IOS XR Software on a Multishelf System."

Router Management Interfaces

Because new routers are not yet configured for your environment, you must start configuration using the command-line interface (CLI). This guide provides instructions on using the CLI to configure basic router features. The Cisco IOS XR software supports the following router management interfaces, which are described in the following sections:

Command-Line Interface

The CLI is the primary user interface for configuring, monitoring, and maintaining routers that run the Cisco IOS XR software. The CLI allows you to directly and simply execute Cisco IOS XR commands.

All procedures in this guide use the CLI. Before you can use other router management interfaces, you must first use the CLI to install and configure those interfaces. Guidelines for using the CLI are presented in the following chapters:

- Chapter 4, “Configuring General Router Features”
- Chapter 5, “Configuring Additional Router Features”
- Chapter 6, “CLI Tips, Techniques, and Shortcuts”

For information on CLI procedures for other tasks, such as hardware interface and software protocol management, see the Cisco IOS XR software documents listed in the “Related Documents” section on page x.

Craft Works Interface

The Craft Works Interface (CWI) is a client-side application used to configure and manage routers that run the Cisco IOS XR software. CWI includes advanced CLI features and a graphical user interface, and it is included with the Cisco IOS XR Manageability package.

The CWI is a desktop used to launch management and configuration applications. The management and configuration features include fault management, configuration management, performance management, security management, and inventory management, with an emphasis on speed and efficiency. For more information, see the Cisco IOS XR software documents listed in the “Related Documents” section on page x.

Extensible Markup Language API

The Extensible Markup Language (XML) application programming interface (API) is an XML interface used for rapid development of client applications and perl scripts to manage and monitor the router. Client applications can be used to configure the router or request status information from the router by encoding a request in XML API tags and sending it to the router. The router processes the request and

sends the response to the client in the form of encoded XML API tags. The XML API supports readily available transport layers, including Telnet, Secure Shell (SSH), and Common Object Request Broker Architecture (CORBA). The Secure Socket Layer (SSL) transport is also supported by the XML API.

For more information, see the Cisco IOS XR software documents listed in the "Related Documents" section on page x.

Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is an application-layer protocol designed to facilitate the exchange of management information between network devices. By using SNMP-transported data (such as packets per second and network error rates), network administrators can more easily manage network performance, find and solve network problems, and plan for network growth.

The Cisco IOS XR software supports SNMP v1, v2c, and v3. SNMP is part of a larger architecture called the Internet Network Management Framework (NMF), which is defined in Internet documents called RFCs. The SNMPv1 NMF is defined by RFCs 1155, 1157, and 1212, and the SNMPv2 NMF is defined by RFCs 1441 through 1452.

SNMP is a popular protocol for managing diverse commercial internetworks and those used in universities and research organizations. SNMP-related standardization activity continues even as vendors develop and release state-of-the-art, SNMP-based management applications. SNMP is a relatively simple protocol, yet its feature set is sufficiently powerful to handle the difficult problems presented in trying to manage the heterogeneous networks of today.

For more information, see the Cisco IOS XR software documents listed in the "Related Documents" section on page x.

Selecting and Identifying the Designated Shelf Controller

The designated shelf controller (DSC) controls a standalone router or a multishelf System. A DSC is a role that is assigned to one route processor (RP) card or performance route processor (PRP) card in each router or multishelf system. RP cards operate in Cisco CRS-1 routers, and PRP cards operate in Cisco XR 12000 and 12000 Series routers.

Note Throughout this guide, the term RP is used to refer to the RP cards supported on Cisco CRS-1 routers and the PRP cards supported on Cisco XR 12000 Series Routers. If a feature or an issue applies to only one platform, the accompanying text specifies the platform.

Although each router or multishelf system can have multiple RP cards, only one can serve as the DSC and control the router or multishelf system. The DSC provides system-wide administrative functions, including:

- User configuration using a terminal connection or network connection
- Distribution of software to each node in the router or system
- Coordination of software versioning and configurations for all nodes in the router or system
- Hardware inventory and environmental monitoring

The first step in setting up a new router is to select or identify the DSC because the initial router configuration takes place through the DSC. The following sections describe how to select and identify the DSC on different routers and the multishelf system:

Selecting and Identifying the DSC on Cisco CRS-1 Routers

A Cisco CRS-1 router supports up to two RPs. If only one RP is installed, that RP automatically becomes the DSC. If two RPs are installed, the default configuration selects RP0 as the DSC. To select RP1 to become the DSC for a new installation, install RP1 first, apply power to the system, and wait for RP1 to start up. When the Primary LED on the RP1 front panel lights, RP1 is operating as the DSC, and you can install RP0.

Tip After the router starts for the first time, you can use the **redundancy reddrv** command to select which RP becomes the DSC during a restart.

The active RP and DSC lights the Primary LED on the RP front panel. The alphanumeric LED display on the active RP displays ACTV RP. By default, the other RP becomes the standby RP, displays STBY RP on the alphanumeric display, and takes over if the DSC fails.

To visually determine which RP is operating as the DSC in a Cisco CRS-1 router, look for the RP on which the Primary LED is lit. You can also look for the RP that displays the ACTV RP message on the alphanumeric display.

Selecting and Identifying the DSC on Cisco CRS-1 Multishelf Systems

A Cisco CRS-1 Multishelf System supports up to two RPs in each LCC. Each LCC must have at least one RP, so a multishelf system supports between two and four RPs. The RPs in a multishelf system operate much like the RPs in a standalone router. The difference is that only one LCC can host the DSC.

During the initial startup of a multishelf system, the DSC is RP0 in the LCC with the lowest configured rack number, which is usually Rack 0. If you want to select RP1 within Rack 0 to become the DSC, install RP1 first, and wait for RP1 to start up. When the Primary LED on the RP1 front panel lights (or the alphanumeric display shows ACTV RP), RP1 is operating as the DSC, and you can install RP0. If you are setting up a new multishelf system, the instructions in Chapter 3, “Bringing Up the Cisco IOS XR Software on a Multishelf System,” specify the appropriate time to bring up and configure the DSC.

Tip After the router starts for the first time, you can use the **redundancy reddrv** command to select which Rack 0 RP becomes the DSC during a restart.

The active RP and DSC lights the Primary LED on the RP front panel. The alphanumeric LED display on the active RP displays ACTV RP. By default, the other RP becomes the standby RP, displays STBY RP on the alphanumeric display, and takes over if the DSC fails.

After the DSC starts up in Rack 0, the DSC remains in Rack 0 while at least one RP in Rack 0 is operating properly. If both RPs in Rack 0 fail, the active RP in the other rack becomes the DSC. The process of moving the DSC function from one rack to another is called DSC migration. For more information on DSC migration, see the *Cisco IOS XR System Management Configuration Guide, Release 3.4*.

Note Any LCC can host the DSC. The FCC cannot host the DSC function.

Selecting and Identifying the DSC on Cisco XR 12000 and 12000 Series Routers

A Cisco XR 12000 or 12000 Series router supports multiple PRPs. When the router is started for the first time, the PRP in the lowest-numbered slot becomes the active PRP and is identified by the alphanumeric display: ACTV RP. The active PRP serves as the DSC. If another PRP is configured as a standby PRP for the DSC, that PRP can assume the DSC role if the DSC fails.

To have a PRP in a higher-numbered slot become the DSC, you must bring up the router with only that PRP installed. After the chosen PRP becomes the DSC, it remains the DSC after subsequent restarts and you can add the other PRPs.

Note Additional PRPs can be installed to host secure domain routers (SDRs), which are introduced in Chapter 4, "Configuring General Router Features." To configure general router features, you must connect to the DSC. To configure SDR features, you must connect to the PRP for the appropriate SDR.

Connecting to the Router Through the Console Port

The first time you connect to a new router with Cisco IOS XR software, you must connect through the Console port on the DSC. Although typical router configuration and management take place using an Ethernet port on the DSC, this port must be configured for your local area network before it can be used.

Figure 1-4 shows the RP connections on the Cisco CRS-1 16-Slot Line Card Chassis, and Figure 1-5 shows the RP connections on the Cisco CRS-1 4-Slot Line Card Chassis and Cisco CRS-1 8-Slot Line Card Chassis. Figure 1-6 shows the PRP-1 connections on the Cisco XR 12000 Series Router. Figure 1-7 shows the PRP-2 connections on the Cisco XR 12000 Series Router.

Figure 1-4 Communication Ports on the RP for a Cisco CRS-1 16-Slot LCC

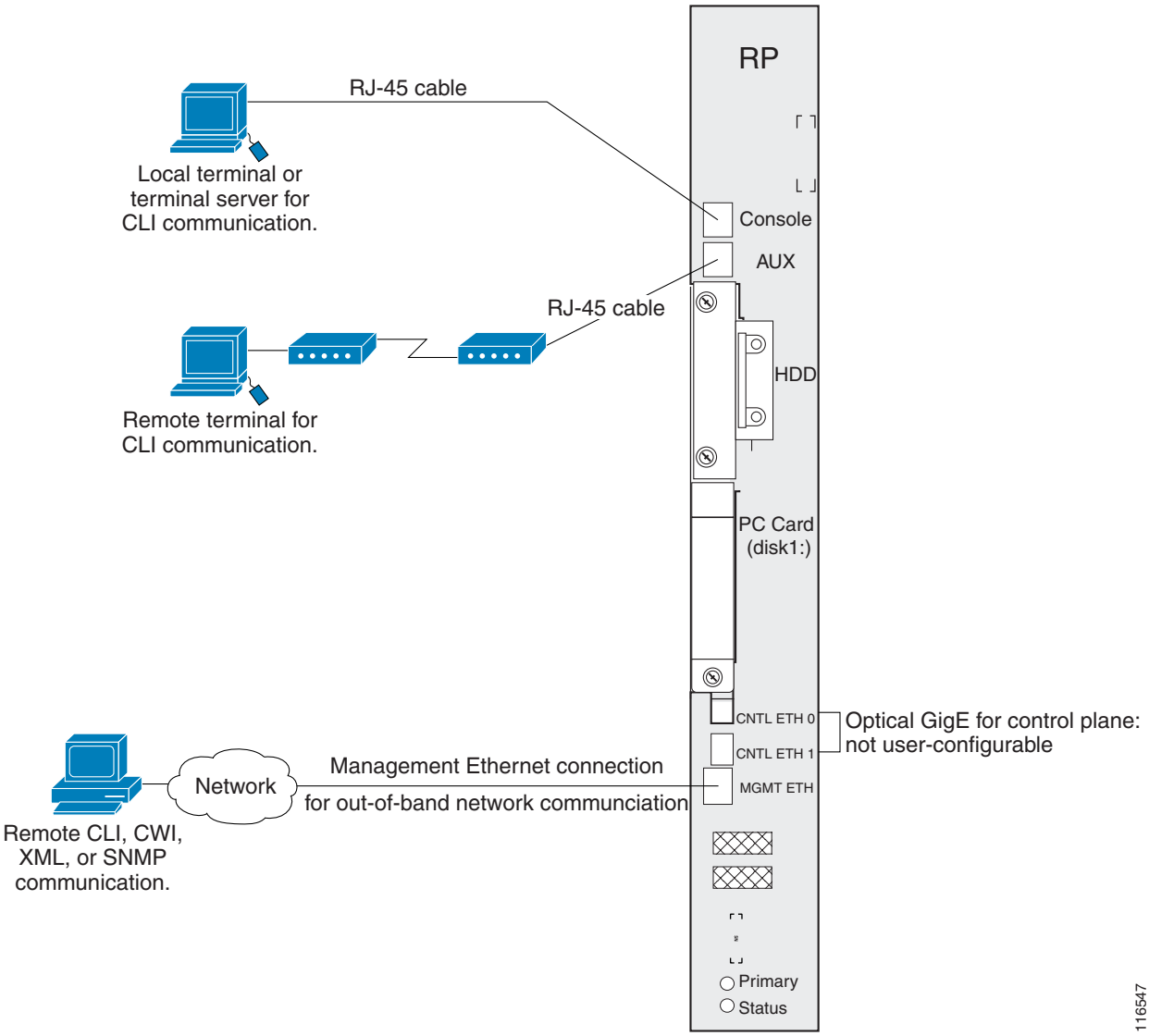


Figure 1-5 Communication Ports on the RP for a Cisco CRS-1 4-slot and 8-Slot LCCs

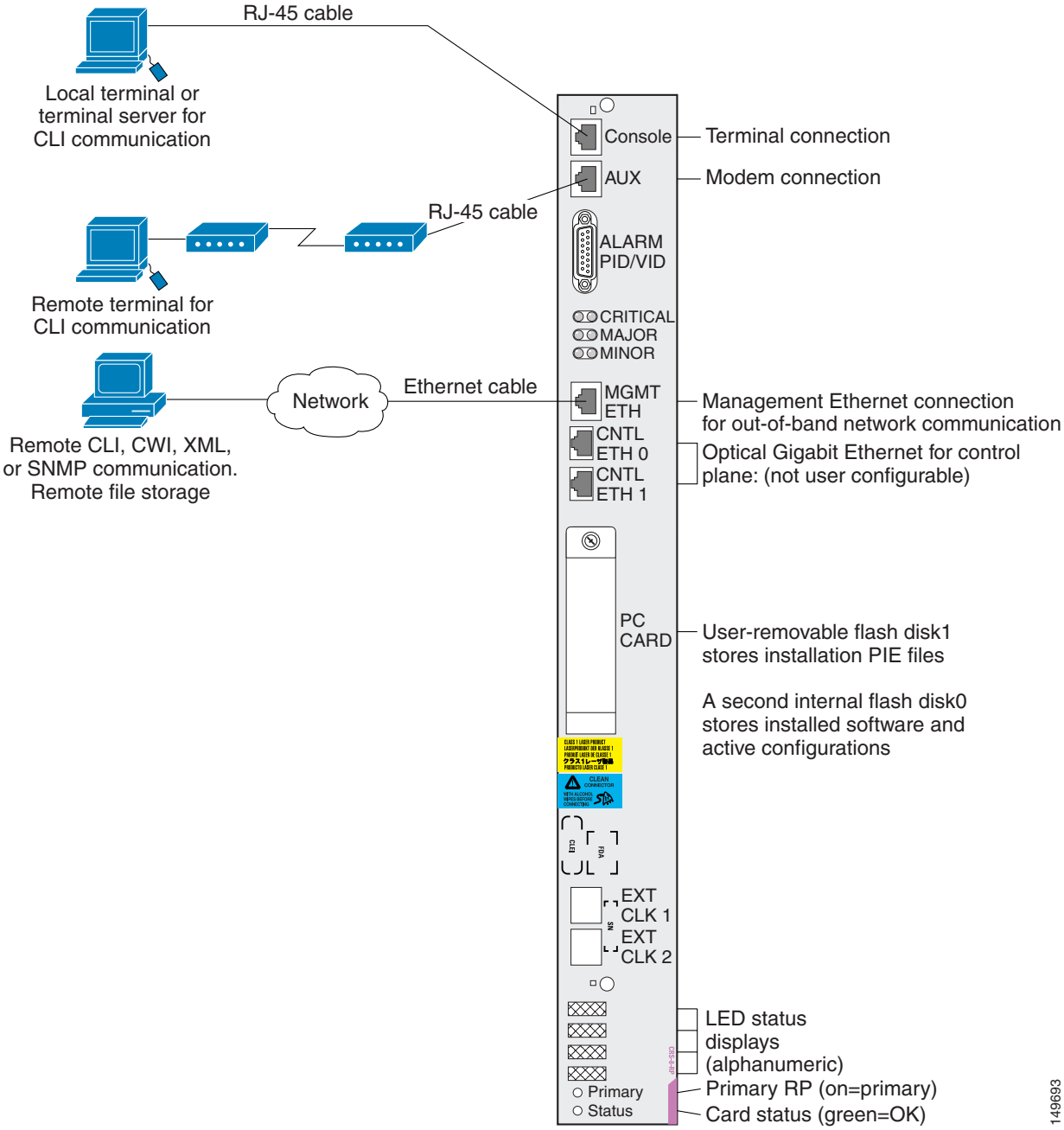


Figure 1-6 Communication Ports on the PRP-1 for a Cisco XR 12000 Series Router

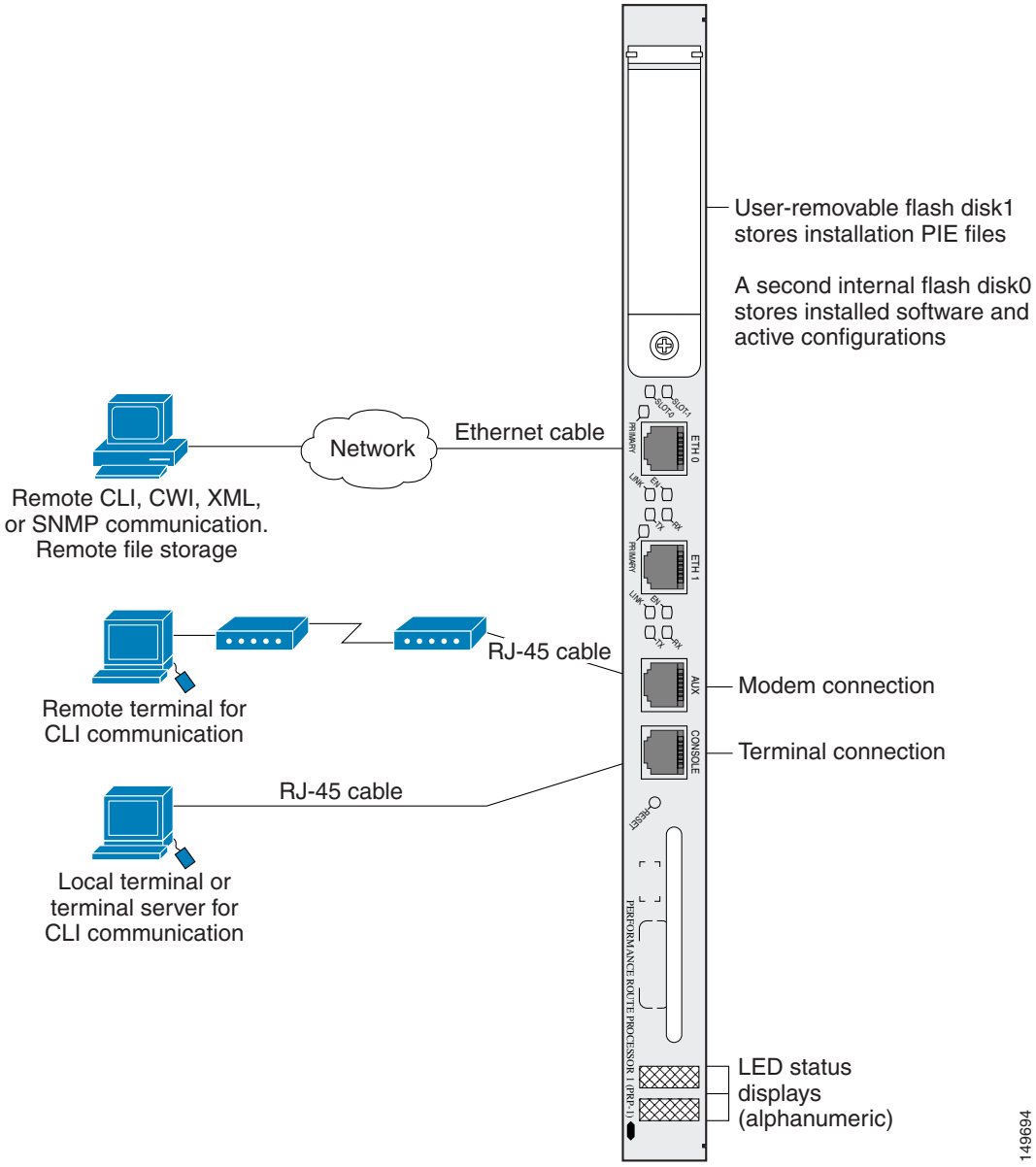
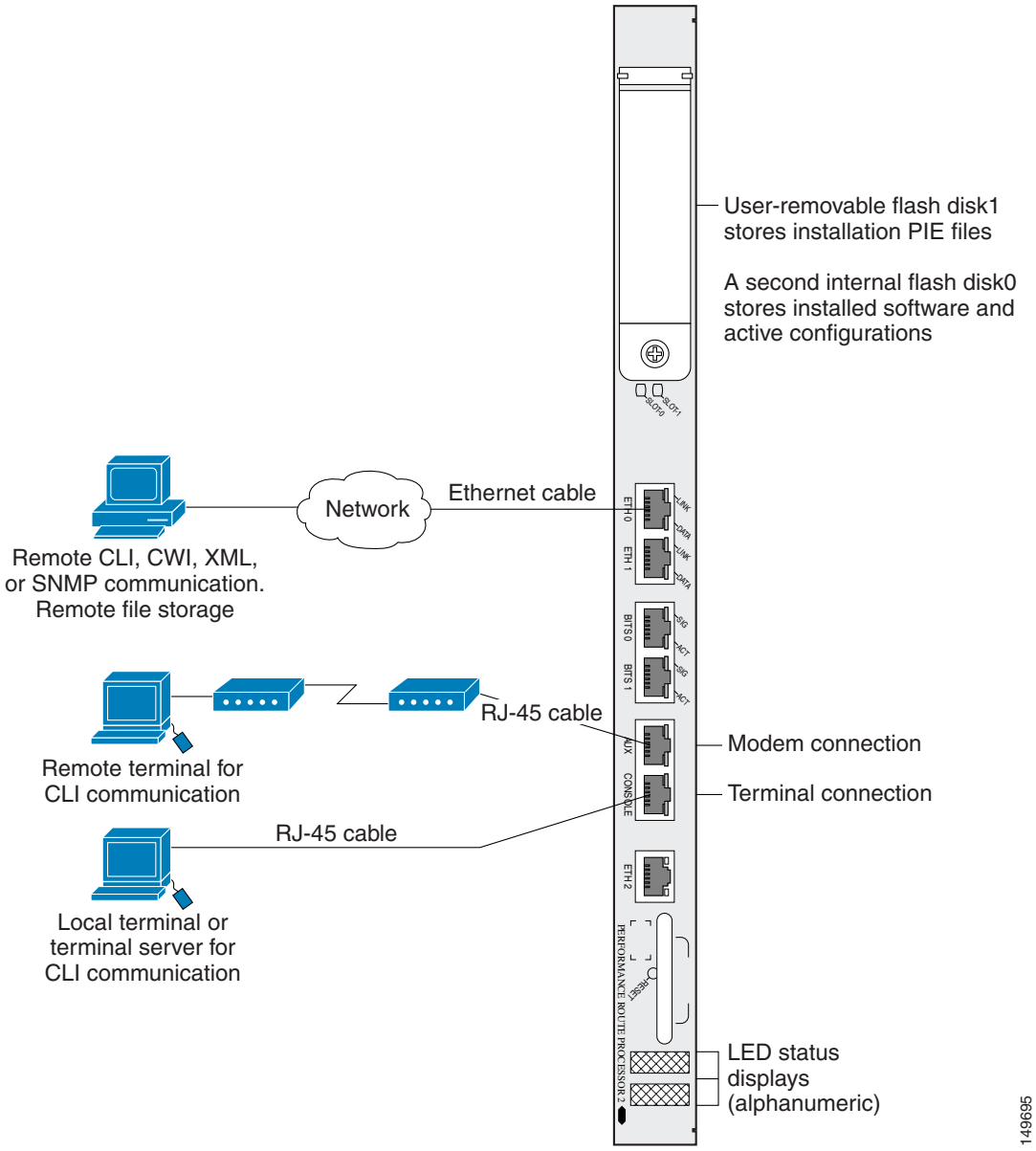


Figure 1-7 Communication Ports on the PRP-2 for a Cisco XR 12000 Series Router



To connect to the router, perform the following procedure.

SUMMARY STEPS

1. Power on the standalone router, or power on Rack 0 in a multishelf system.
2. Identify the DSC.
3. Connect a terminal to the Console port of the DSC.
4. Start the terminal emulation program.
5. Press **Enter**.
6. Log in to the router.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Power on the standalone router, or power on Rack 0 in a multishelf system.	Starts the router or Rack 0. • This step is required only if the power is not on. • For information on power installation and controls, see the hardware documentation listed in the "Related Documents" section on page x.
Step 2	Identify the DSC.	Identifies the RP to which you must connect in the next step. • For more information, see the "Selecting and Identifying the Designated Shelf Controller" section on page 1-7.
Step 3	Connect a terminal to the Console port of the DSC.	Establishes a communications path to the router. • During the initial setup, you can communicate with the router only through the Console port of the DSC. • The router Console port is designed for a serial cable connection to a terminal or a computer that is running a terminal emulation program. • The terminal settings are: – Bits per second: 9600/9600 – Data bits: 8 – Parity: None – Stop bit: 2 – Flow control: None • For information on the cable requirements for the Console port, see the hardware documentation listed in the "Related Documents" section on page x.

	Command or Action	Purpose
Step 4	Start the terminal emulation program.	(Optional.) Prepares a computer for router communications. • The step is not required if you are connecting through a terminal. • Terminals send keystrokes to and receive characters from another device. If you connect a computer to the Console port, you must use a terminal emulation program to communicate with the router. For instructions on using the terminal emulation program, see the documentation for that program.
Step 5	Press **Enter**.	Initiates communication with the router. • If no text or router prompt appears when you connect to the console port, press **Enter** to initiate communications. • If no text appears when you press **Enter**, give the router more time to complete the initial boot procedure, then press **Enter**. • If the prompt gets lost among display messages, press **Enter** again. • If the router has no configuration, the router displays the prompt: `Enter root-system username:` • If the router has been configured, the router displays the prompt: `Username:`
Step 6	Log in to the router.	Establishes your access rights for the router management session. • Enter the root-system username and password or the username and password provided by your system administrator. • After you log in, the router displays the CLI prompt, which is described in the "CLI Prompt" section on page 4-13. • If the router prompts you to enter a root-system username, the router is not configured, and you should follow one of the bring up procedures mentioned in the next section.

Where to Go Next

If you have logged into the router or multishelf system, you are ready to perform general router configuration as described in Chapter 4, "Configuring General Router Features."

If the router is prompting you to enter a root-system username, bring up the router or multishelf system as described in the appropriate chapter:

- Chapter 2, "Bringing Up the Cisco IOS XR Software on a Standalone Router"
- Chapter 3, "Bringing Up the Cisco IOS XR Software on a Multishelf System"

CHAPTER 2

Bringing Up the Cisco IOS XR Software on a Standalone Router

This chapter provides instructions for bringing up the Cisco IOS XR software on a standalone router for the first time. This section applies to standalone routers that are delivered with Cisco IOS XR software installed.

Note If you are upgrading a Cisco 12000 Series Router from Cisco IOS software to Cisco IOS XR software, see the Cisco IOS XR software document titled *Upgrading from Cisco IOS to Cisco IOS XR Software on the Cisco 12000 Series Router.*

Contents

This chapter contains the following sections:

Prerequisites

The following sections describe the software and hardware requirements for bringing up a standalone system.

Software Requirements

The multishelf system requires the following software:

- Cisco IOS XR Software Release 3.4
- ROMMON 1.40 or higher on each RP in the system

Caution The ROM Monitor software must be upgraded to version 1.40 or higher on all RPs before a Cisco CRS-1 system is upgraded to Cisco IOS XR Software Release 3.3.1 or higher release. If the router is brought up with an incompatible version of the ROM Monitor software, then the standby RP may fail to boot. For instructions to overcome a boot block in the standby RP in a single chassis system, see *Cisco IOS XR ROM Monitor Guide*. If a boot block occurs in a multishelf system, contact your Cisco Systems support representative for assistance. See Obtaining Technical Assistance, page -xiii.

Hardware Prerequisites and Documentation

The Cisco IOS XR software runs on the routers listed in the "Supported Standalone System Configurations" section on page 1-1. Before a router can be started, the following hardware management procedures must be completed:

- Site preparation
- Equipment unpacking
- Router installation

For information on how to complete these procedures for your router equipment, see the hardware documents listed in the "Related Documents" section on page x.

Note If you are upgrading a Cisco 12000 Series Router from Cisco IOS software to Cisco IOS XR software, you must first prepare the router. Refer to *Upgrading from Cisco IOS to Cisco IOS XR Software on the Cisco 12000 Series Router* for more information. See the "Related Documents" section on page x for a complete listing of available documents.

Bringing Up and Configuring a Standalone Router

To bring up a standalone router, you need to connect to the router and configure root-system username and password as described in the following procedure:

SUMMARY STEPS

1. Establish a connection to the DSC Console port.
2. Type the username for the root-system login and press **Return**.
3. Type the password for the root-system login and press **Return**.
4. Log in to the router.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Establish a connection to the DSC Console port.	Initiates communication with the router. • For instructions on connecting to the Console port, see the "Connecting to the Router Through the Console Port" section on page 1-9. • If the router has been configured, the router displays the prompt: `Username:` • If the Username prompt appears, skip this procedure and continue general router configuration as described in Chapter 4, "Configuring General Router Features."
Step 2	Type the username for the root-system login and press **Return**.	Sets the root-system username, which is used to log in to the router.
Step 3	Type the password for the root-system login and press **Return**.	Creates an encrypted password for the root-system username. **Note** This password can be changed with the **secret** command.
Step 4	Retype the password for the root-system login and press **Return**.	Allows the router to verify that you have entered the same password both times. • If the passwords do not match, the router prompts you to repeat the process.
Step 5	Log in to the router.	Establishes your access rights for the router management session. • Enter the root-system username and password that were created earlier in this procedure. • After you log in, the router displays the CLI prompt, which is described in the "CLI Prompt" section on page 4-13.

Examples

The following example shows the root-system username and password configuration for a new router, and it shows the initial log in:

```
--- Administrative User Dialog ---


  Enter root-system username: cisco
  Enter secret:
  Enter secret again:
RP/0/0/CPU0:Jan 10 12:50:53.105 : exec[65652]: %MGBL-CONFIG-6-DB_COMMIT :
'Administration configuration committed by system'. Use 'show configuration
commit changes 2000000009' to view the changes.
Use the 'admin' mode 'configure' command to modify this configuration.



User Access Verification
```

```
Username: cisco
Password:
RP/0/0/CPU0:ios#
```

The *secret* line in the configuration command script shows that the password is encrypted. When you enter the password during configuration and login, the password is hidden.

Verifying the System After Initial Bring-Up

To verify the status of the router, perform the following procedure:

SUMMARY STEPS

1. **show version**
2. **admin**
   show platform [*node-id*]
   end
3. **show redundancy**
4. **show environment**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show version** `RP/0/RP0/CPU0:router# show version`	Displays information about the router, including image names, uptime, and other system information.

Step 2	**admin**
	show platform [*node-id*]
	exit
	
	`RP/0/RP0/CPU0:router# admin`
	`RP/0/RP0/CPU0:router(admin)# show platform`
	`RP/0/RP0/CPU0:router(admin)# exit`
		Places the router in administration EXEC mode, displays information about the status of cards and modules installed in the router, and terminates administration EXEC mode.
		• Some cards support a CPU module and service processor (SP) module. Other cards support only a single module.
		• A card module is also called a node. When a node is working properly, the status of the node in the State column is IOS XR RUN.
		• Type the **show platform** *node-id* command to display information for a specific node. Replace *node-id* with a node name from the **show platform** command Node column.
		Note To view the status of all cards and modules, the **show platform** command must be executed in administration EXEC mode.

Step 3	**show redundancy** **Example:** `RP/0/RP0/CPU0:router# show redundancy`	Displays the state of the primary (active) and standby (inactive) RPs, including the ability of the standby to take control of the system. • If both RPs are working correctly, one node displays *active role*, the *Partner node* row displays *standby role*, and the *Standby node* row displays *Ready*.
Step 4	**show environment** **Example:** `RP/0/RP0/CPU0:router# show environment`	Displays information about the hardware attributes and status.

Examples of show Commands

The following sections provide examples of **show** commands:

show version Command

To display basic information about the router configuration, type the **show version** command in EXEC mode, as shown in the following example:

```
RP/0/RP1/CPU0:CRS-8_P1# show version
```

```
Cisco IOS XR Software, Version 3.3.0[2I]
Copyright (c) 2006 by cisco Systems, Inc.

ROM: System Bootstrap, Version 1.38(20050525:193559) [CRS-1 ROMMON],

CRS-8_P1 uptime is 1 week, 1 day, 17 hours, 1 minute
System image file is "disk0:hfr-os-mbi-3.3.0/mbihfr-rp.vm"

cisco CRS-8/S (7457) processor with 4194304K bytes of memory.
7457 processor at 1197Mhz, Revision 1.2

16 Packet over SONET/SDH network interface(s)
16 SONET/SDH Port controller(s)
2 Ethernet/IEEE 802.3 interface(s)
16 GigabitEthernet/IEEE 802.3 interface(s)
2043k bytes of non-volatile configuration memory.
38079M bytes of hard disk.
1000592k bytes of ATA PCMCIA card at disk 0 (Sector size 512 bytes).
1000640k bytes of ATA PCMCIA card at disk 1 (Sector size 512 bytes).

Package active on node 0/1/SP:
hfr-diags, V 3.3.0[2I], Cisco Systems, at disk0:hfr-diags-3.3.0
    Built on Mon Mar 13 12:58:02 UTC 2006
    By iox8.cisco.com in /auto/ioxws48/production/3.3.0.2I/hfr/workspace for c8

hfr-admin, V 3.3.0[2I], Cisco Systems, at disk0:hfr-admin-3.3.0
    Built on Mon Mar 13 11:46:36 UTC 2006
    By iox8.cisco.com in /auto/ioxws48/production/3.3.0.2I/hfr/workspace for c8

hfr-base, V 3.3.0[2I], Cisco Systems, at disk0:hfr-base-3.3.0
    Built on Mon Mar 13 11:43:22 UTC 2006
    By iox8.cisco.com in /auto/ioxws48/production/3.3.0.2I/hfr/workspace for c8

hfr-os-mbi, V 3.3.0[2I], Cisco Systems, at disk0:hfr-os-mbi-3.3.0
    Built on Mon Mar 13 11:27:02 UTC 2006
    By iox8.cisco.com in /auto/ioxws48/production/3.3.0.2I/hfr/workspace for c8

 --More--
```

show environment Command

To display environmental monitor parameters for the system, use the **show environment** command in EXEC or administration EXEC mode. The following command syntax is used:

show environment [options]

Enter the **show environment ?** command to display the command options.

In the following example, temperature information for a Cisco CRS-1 router is shown:

```
RP/0/RP0/CPU0:router# show environment temperatures

R/S/I   Modules         Inlet              Exhaust            Hotspot
                        Temperature        Temperature        Temperature
                        (deg C)            (deg C)            (deg C)

0/1/*
        host              32, 30            26, 27            35
        cpu                                                   34
        fabricq0                                              27
        fabricq1                                              32
        ingressq                                              37
        egressq                             32                27
```

```
        ingresspse                                      35
        egresspse                                       29
        jacket          25              24              25
        spa0            19                              25, 32
        spa5            25                              24
0/6/*
        host            32, 26          27, 25          33
        cpu                                             35
        fabricq0                                        27
        fabricq1                                        32
        ingressq                                        37
        egressq                         30              25
        ingresspse                                      31
        egresspse                                       29
        jacket          24              25              26
        spa0            19                              25, 31
        spa4            22                              33, 35
        spa5            24                              24
0/RP0/*
        host            23              24              24, 33, 26,
                                                            24, 27
0/RP1/*
        host            23              24              24, 32, 26,
                                                            24, 26
```

In the following example, LED status of the nodes in a Cisco CRS-1 router is shown:

```
RP/0/RP0/CPU0:router# show environment leds

0/1/*: Module (host) LED status says: OK
0/1/*: Module (jacket) LED status says: OK
0/1/*: Module (spa0) LED status says: OK
0/1/*: Module (spa5) LED status says: OK
0/6/*: Module (host) LED status says: OK
0/6/*: Module (jacket) LED status says: OK
0/6/*: Module (spa0) LED status says: OK
0/6/*: Module (spa4) LED status says: OK
0/6/*: Module (spa5) LED status says: OK
0/RP0/*: Module (host) LED status says: OK
0/RP0/*: Alarm LED status says: NONE
0/RP1/*: Module (host) LED status says: OK
0/RP1/*: Alarm LED status says: NONE
```

See the *Cisco IOS XR Interface and Hardware Component Command Reference* for more information.

show platform Command

The **show platform** command displays information on router resources. In EXEC mode, the **show platform** command displays the resources assigned to the secure domain router (SDR) you are managing. In administration EXEC mode, the **show platform** command displays all router resources.

Note SDRs are introduced in Chapter 4, "Configuring General Router Features."

The following EXEC mode sample output displays the nodes assigned to the default SDR, which is called the *owner SDR*:

```
RP/0/RP0/CPU0:router# show platform
Node            Type            PLIM            State           Config State
-------------------------------------------------------------------------------
0/1/CPU0        MSC             Jacket Card     IOS XR RUN      PWR,NSHUT,MON
0/1/0           MSC(SPA)        4XOC3-POS       OK              PWR,NSHUT,MON
0/1/5           MSC(SPA)        8X1GE           OK              PWR,NSHUT,MON
```

```
0/6/CPU0        MSC             Jacket Card     IOS XR RUN      PWR,NSHUT,MON
0/6/0           MSC(SPA)        4XOC3-POS       OK              PWR,NSHUT,MON
0/6/4           MSC(SPA)        8XOC3/OC12-POS  OK              PWR,NSHUT,MON
0/6/5           MSC(SPA)        8X1GE           OK              PWR,NSHUT,MON
0/RP0/CPU0      RP(Active)      N/A             IOS XR RUN      PWR,NSHUT,MON
0/RP1/CPU0      RP(Standby)     N/A             IOS XR RUN      PWR,NSHUT,MON
```

The following administration EXEC mode sample output displays all router nodes:

```
RP/0/RP0/CPU0:router# admin

RP/0/RP0/CPU0:router(admin)# show platform

Node            Type            PLIM            State           Config State
--------------------------------------------------------------------------------
0/1/SP          MSC(SP)         N/A             IOS XR RUN      PWR,NSHUT,MON
0/1/CPU0        MSC             Jacket Card     IOS XR RUN      PWR,NSHUT,MON
0/1/0           MSC(SPA)        4XOC3-POS       OK              PWR,NSHUT,MON
0/1/5           MSC(SPA)        8X1GE           OK              PWR,NSHUT,MON
0/6/SP          MSC(SP)         N/A             IOS XR RUN      PWR,NSHUT,MON
0/6/CPU0        MSC             Jacket Card     IOS XR RUN      PWR,NSHUT,MON
0/6/0           MSC(SPA)        4XOC3-POS       OK              PWR,NSHUT,MON
0/6/4           MSC(SPA)        8XOC3/OC12-POS  OK              PWR,NSHUT,MON
0/6/5           MSC(SPA)        8X1GE           OK              PWR,NSHUT,MON
0/RP0/CPU0      RP(Active)      N/A             IOS XR RUN      PWR,NSHUT,MON
0/RP1/CPU0      RP(Standby)     N/A             IOS XR RUN      PWR,NSHUT,MON
0/SM0/SP        FC/S(SP)        N/A             IOS XR RUN      PWR,NSHUT,MON
0/SM1/SP        FC/S(SP)        N/A             IOS XR RUN      PWR,NSHUT,MON
0/SM2/SP        FC/S(SP)        N/A             IOS XR RUN      PWR,NSHUT,MON
0/SM3/SP        FC/S(SP)        N/A             IOS XR RUN      PWR,NSHUT,MON

RP/0/RP0/CPU0:router# end
```

Note Line cards in Cisco CRS-1 routers are called modular services cards (MSCs). The **show platform** command output is different for Cisco CRS-1 routers and Cisco XR 12000 Series Routers.

In the following example, information is shown for a single node in a Cisco CRS-1 router:

```
RP/0/RP0/CPU0:CRS-8_P1# show platform 0/1/CPU0

Node            Type            PLIM            State           Config State
--------------------------------------------------------------------------------
0/1/CPU0        MSC             Jacket Card     IOS XR RUN      PWR,NSHUT,MON
```

For more information on node IDs, see the *Cisco IOS XR System Management Configuration Guide, Release 3.4*.

For more information on the **show platform** command, see the *Cisco IOS XR Interface and Hardware Component Command Reference*.

show redundancy Command

To display information about the active and standby (inactive) RPs, enter the **show redundancy** command as follows:

```
RP/0/RP0/CPU0:CRS-8_P1# show redundancy

Redundancy information for node 0/RP0/CPU0:
==========================================
Node 0/RP0/CPU0 is in ACTIVE role
Partner node (0/RP1/CPU0) is in STANDBY role
Standby node in 0/RP1/CPU0 is ready

Reload and boot info
----------------------
RP reloaded Wed Feb 15 13:58:32 2006: 1 week, 6 days, 22 hours, 49 minutes ago
Active node booted Wed Feb 15 13:58:32 2006: 1 week, 6 days, 22 hours, 49 minuto
Standby node boot Wed Feb 15 13:59:00 2006: 1 week, 6 days, 22 hours, 49 minuteo
Standby node last went not ready Wed Mar  1 07:40:00 2006: 5 hours, 8 minutes ao
Standby node last went ready Wed Mar  1 07:40:00 2006: 5 hours, 8 minutes ago
There have been 0 switch-overs since reload
```

Where to Go Next

For information on configuring basic router features, see Chapter 4, “Configuring General Router Features.”

CHAPTER 3

Bringing Up the Cisco IOS XR Software on a Multishelf System

This chapter describes how to bring up the Cisco IOS XR software on a Cisco CRS-1 Carrier Routing System Multishelf System for the first time.

Contents

This chapter contains the following sections:

Prerequisites

The following sections describe the software and hardware requirements for bringing up a multishelf system.

Software Requirements

The multishelf system requires the following software:

- Cisco IOS XR Software Release 3.4
- ROMMON 1.40 or higher on each RP in the system

Caution The ROM Monitor software must be upgraded to version 1.40 or higher on all RPs before a Cisco CRS-1 system is upgraded to Cisco IOS XR Software Release 3.3.1 or higher release. If the router is brought up with an incompatible version of the ROM Monitor software, then the standby RP may fail to boot. For instructions to overcome a boot block in the standby RP in a single chassis system, see *Cisco IOS XR ROM Monitor Guide*. If a boot block occurs in a multishelf system, contact your Cisco Systems support representative for assistance. See Obtaining Technical Assistance, page -xiii.

In addition, Cisco CRS-1 Multishelf systems should be upgraded to ROMMON release 1.40 before being upgraded to IOS XR Release 3.3.1 to ensure RPs are assigned the correct rack numbers during system boot.

For more information, see *Cisco IOS XR ROM Monitor Guide*.

Hardware Requirements

Before you can bring up a multishelf system, the system components must be physically installed and tested. Three multishelf system configurations are supported; and they require the following components:

- Two 16-slot line card chassis containing eight FC/M (S13) fabric cards
- Two external Gigabit Ethernet Cisco Catalyst 6509 Switches

Single-FCC systems require one FCC containing eight SFC (S2) fabric cards. Two-FCC systems require two FCCs, and four-FCC systems require four FCCs. In two- and four-FCC configurations, the eight SFC (S2) fabric cards are distributed equally in the FCCs.

For instructions to install, cable, and verify a multishelf system, see the documents listed on the Cisco CRS-1 documentation web page listed in the "Related Documents" section on page x.

Restrictions

The following restrictions apply to multishelf systems in Cisco IOS XR Software Release 3.3.

- The multishelf system supports:
  - Two 16-slot line card chassis.
  - One, two, or four FCCs.
  - Two external Catalyst switches to form a control Ethernet plane used for administrative management and monitoring of the system.
- The 4-slot and 8-slot LCCs are not supported.
- Although Cisco IOS XR Software Release 3.3 supports the addition of a second line card chassis, the removal of a line card chassis is restricted. Consult your Cisco Systems support representative for more information (see the "Obtaining Technical Assistance" section on page xiii).

Information About Bringing Up a Multishelf System

The following sections provide information that is good to know before you bring up a multishelf system:

Bringup Overview

The bringup procedure for a multishelf system starts after the hardware installation is complete. The bringup procedure tasks configure the system components to work together and verify the operation and configuration of system components. To bring up the multishelf system, complete the following procedures in the sequence shown:

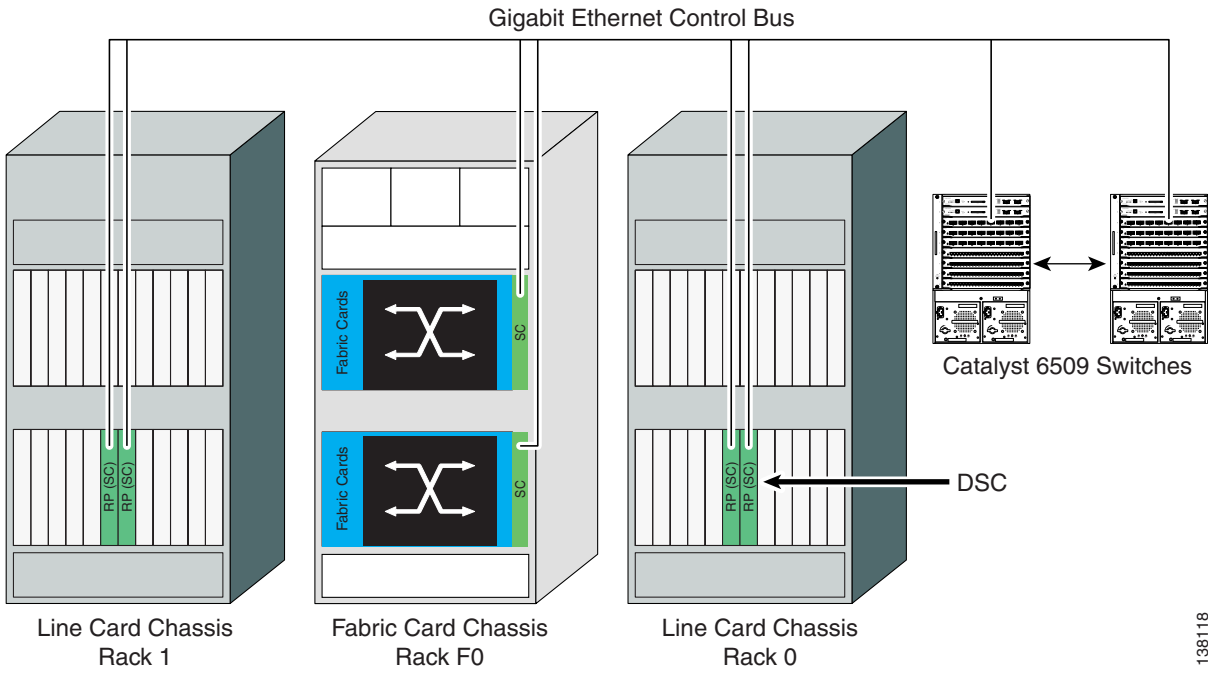
During the bringup procedure, you need the information presented in the following section.

Preparing a Rack Number Plan

In a multishelf system, each chassis must be assigned a unique rack number, as shown in Figure 3-1. This rack number is used to identify a chassis in the system, and maintain the software and configurations for the chassis.

Caution Failure to assign a unique rack number to each chassis in the system can result in serious system error and potential downtime. Unique rack numbers must be assigned and committed on Rack 0 before the additional chassis are powered on and brought on line.

Figure 3-1 DSC in a CRS-1/M-F1 Multishelf System



Note Chassis, shelf, and rack are used interchangeably. Each term refers to the physical tower that contains the installed cards, power, and cooling equipment. In general, *chassis* describes the system components. *Rack* is used in software to assign a rack number to each chassis.

A rack number plan lists each chassis in a system with the correct chassis serial ID and an assigned rack number. The serial ID is the chassis serial number, which can be accessed by the software and uniquely identifies the chassis. The rack number for an LCC is a number in the range of 0 to 255, which is easier to remember and read than serial numbers in display messages.

The rack number plan is used during the startup and configuration of Rack 0. The LCC that hosts the DSC must be configured as Rack 0. The non-DSC LCC must be configured to use a rack number in the range of 1 to 255. FCC rack numbers range from F0 to F3, as shown in Table 1, Table 2 and Table 3.

Table 1 shows a sample rack number plan for a single-FCC system.

Table 1 Sample Rack Number Plan for a Single-FCC Multishelf System

Chassis	Serial ID	Rack Number
LCC containing the active DSC		0
Non-DSC LCC		1
Fabric chassis		F0

Table 2 shows a sample rack number plan for a two-FCC system.

Table 2 Sample Rack Number Plan for a Two-FCC Multishelf System

Chassis	Serial ID	Rack Number
LCC containing the active DSC		0
Non-DSC LCC		1
Fabric chassis 0		F0
Fabric chassis 1		F1

Table 3 shows a sample rack number plan for a four-FCC system.

Table 3 Sample Rack Number Plan for a Four-FCC Multishelf System

Chassis	Serial ID	Rack Number
LCC containing the active DSC		0
Non-DSC LCC		1
Fabric chassis 0		F0
Fabric chassis 1		F1
Fabric chassis 2		F2
Fabric chassis 3		F3

To complete the rack number plan, change the rack number for the non-DSC LCC if you want, and record the serial number for each chassis. The chassis serial number is attached to the back of the chassis, as shown in Figure 2 and Figure 3.

Figure 2 Location of the Serial Number on a Fabric Card Chassis

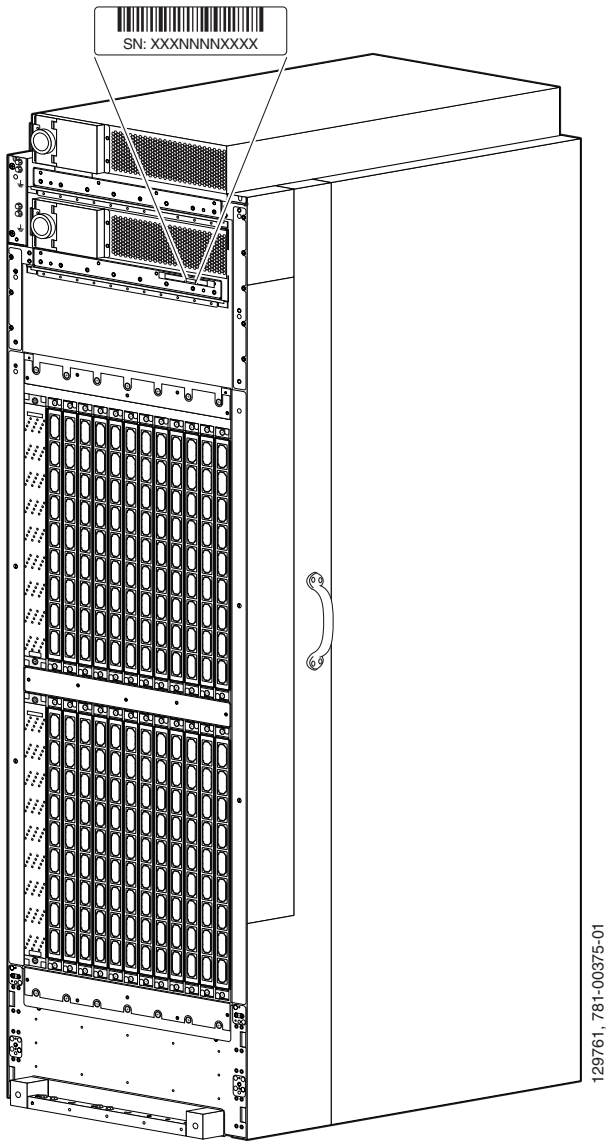
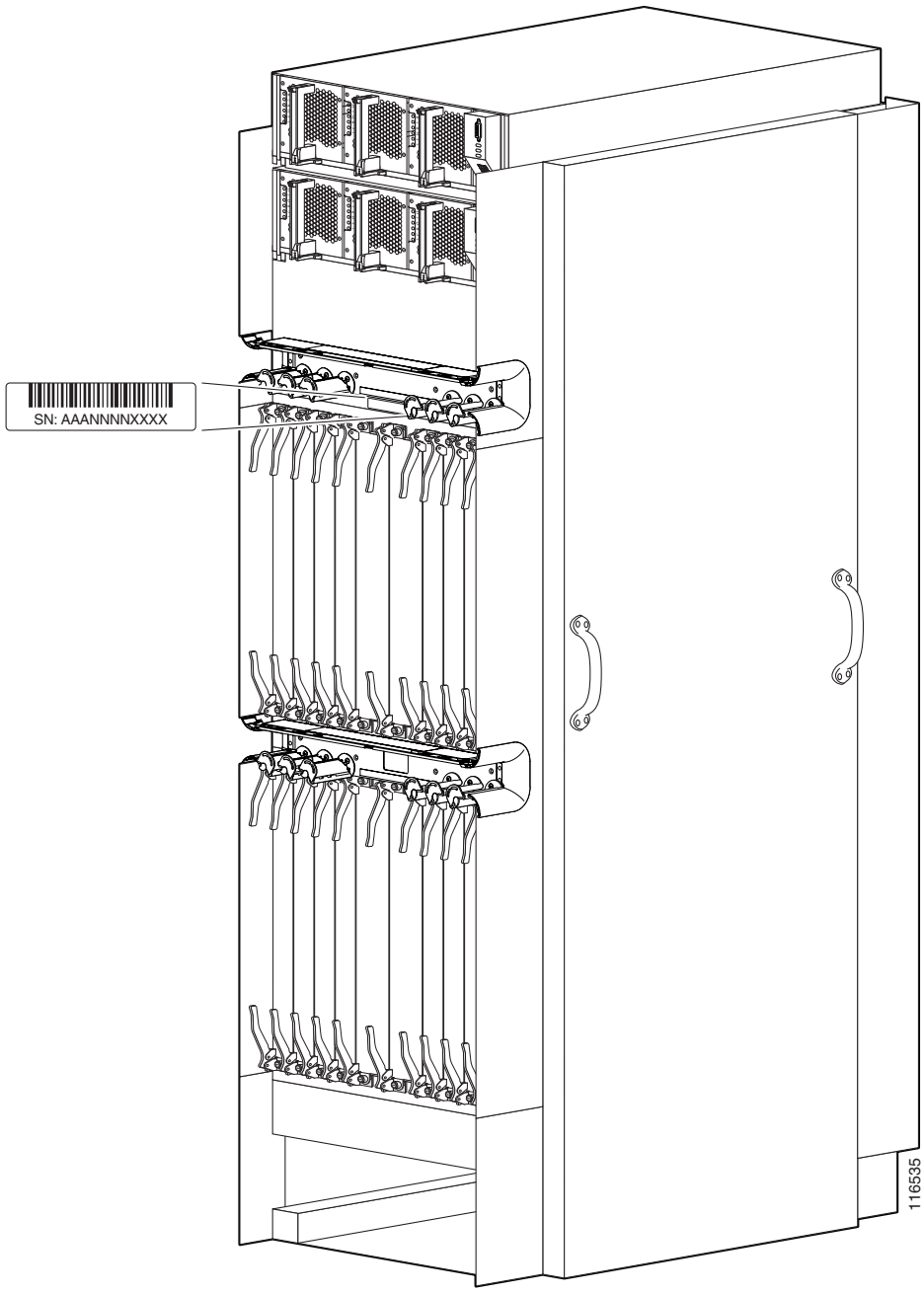


Figure 3 Location of the Serial Number on a Line Card Chassis



Caution Always assign a rack number to each chassis in the system before the chassis is booted. If a chassis is not assigned a rack number, or if the rack number conflicts with an existing chassis, it may not be recognized by the system or cause other operational difficulties.

If you cannot locate or read the chassis serial number on a chassis, you can view the serial number stored in software as described in the following documents:

- To display the chassis serial numbers in administration EXEC mode, see *Cisco IOS XR System Management Configuration Guide, Release 3.4*.
- To display the configured chassis serial numbers in administration EXEC mode, see *Cisco IOS XR System Management Configuration Guide, Release 3.4*.
- To display the chassis serial numbers in ROM Monitor, see *Cisco IOS XR ROM Monitor Guide*.

See the "Bringing Up and Configuring Rack 0" section on page 3-22 for complete instructions to bring up a new router and configure the rack numbers.

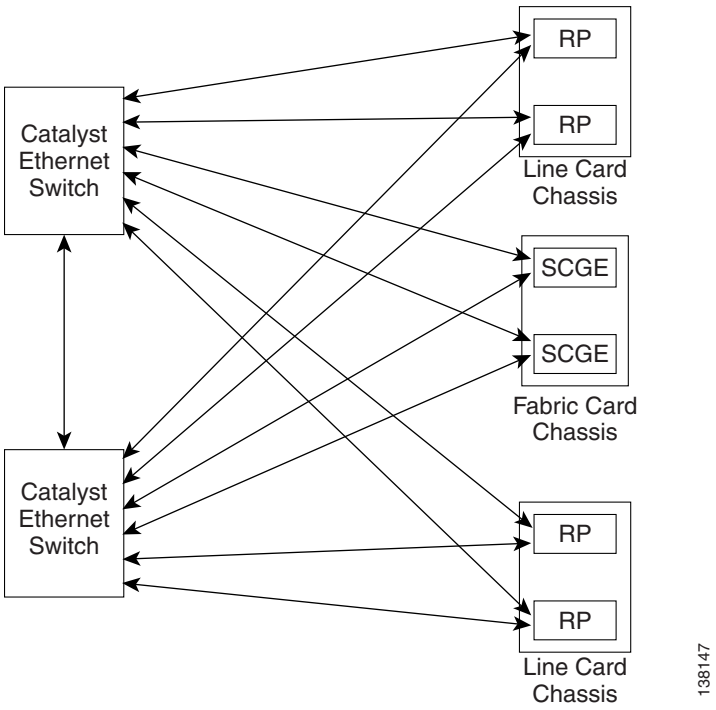
Configuring the External Cisco Catalyst 6509 Switches

The control Ethernet network is formed by interconnecting each RP and shelf controller Gigabit Ethernet (SCGE) card in the system through two external Catalyst switches. (The SCGE card is the control card in an FCC.) The Catalyst switches are also directly connected using one or more Gigabit Ethernet links (see Figure 4).

These Catalyst switches must also be configured for operation with the Cisco CRS-1 multishelf router. This section includes instructions to configure and verify the Catalyst switches using the Cisco IOS software. For instructions to install and cable the Catalyst switches, see *CRS-1 Multishelf System Interconnection and Cabling Guide*.

This section includes the following topics:

Figure 4 Control Ethernet Network Connections in a Single-FCC System



Prerequisites

The following sections describe the software and hardware requirements for bringing up Catalyst 6509 Switches in a multishelf system.

Software Requirements

Each Cisco Catalyst 6509 Switch requires the same software:

- Cisco IOS Release 12.2(14r)S9 with SUP720 Supervisor Engine controller module
- System Bootstrap (ROMMON), Version 1.3 or later
- BOOTLDR: s72033_rp Software (s72033_rp-PSV-M), Version 12.2(17d)SXB7

Both switches should use the same software. The filename of the software is 72033-psv-mz.122-17d.SXB8.bin, and is available on CCO at:

http://www.cisco.com/kobayashi/sw-center/lan/cat6000.shtml

Hardware Requirements

- Two external Cisco Catalyst 6509 Switches correctly cabled to the Cisco CRS-1 multishelf router.
- The recommended hardware configuration for an AC-powered Cisco Catalyst 6509 system is shown in the following table:

Quantity	Description	Part
1	Catalyst 6509 Chassis, 9slot, 15RU, No Pow Supply, No Fan Tray	WS-C6509
1	Cisco CAT6000-SUP720 IOS IP (see Software Requirements for complete details).	S733Z-12217SXB
1	Catalyst 6500/Cisco 7600 Supervisor 720 Fabric MSFC3 PFC3B	WS-SUP720-3B
1	Catalyst 6500 Sup720 Compact Flash Mem 256MB	MEM-C6K-CPTFL256M
1	Catalyst 6000 16-port Gig-Ethernet Mod. (Req. GBICs)	WS-X6416-GBIC
8	1000BASE-LX/LH long haul GBIC (singlemode or multimode)	WS-G5486
1	Catalyst 6509 High Speed Fan Tray	WS-C6K-9SLOT-FAN2
2	Catalyst 6000 2500W AC Power Supply	WS-CAC-2500W
2	Power Cord, 250Vac 16A, straight blade NEMA 6-20 plug, US	CAB-AC-2500W-US1

Restrictions

The following restrictions apply to Cisco Catalyst 6509 Switches that are installed in a multishelf system:

- Both Catalyst switches must operate with the same Cisco IOS software release.
- The spanning tree implementation of Cisco CRS-1 control Ethernet assumes that all Catalyst switch ports connected to the multishelf system are kept in VLAN 1.
- The Gigabit Interface Converter (GBIC) transceiver module used on the Catalyst switches must match the SFP optic used on each RP and SCGE card in the system. The GBIC can be either LX/LH or SX, but the same type must be used on both ends.

Note Both Catalyst switches must be dedicated for use with the multishelf system. The Catalyst switches should not be used for any other purpose.

Before You Begin

Before you begin to bring up the Catalyst 6509 switches, consider the following:

- The Catalyst switches must be installed, including all cables properly connected between the switches and the Cisco CRS-1 router.
- See the "Related Documents" section on page x for a hyperlink to documents on installing and connecting the Catalyst switches.
- For additional information regarding Cisco IOS commands and usage, see the "Cisco IOS Software Configuration" page at the following URL:

  http://www.cisco.com/univercd/cc/td/doc/product/software/index.htm

Information About the Catalyst Switch Configuration

The configuration described in the following sections places all Catalyst ports in VLAN 1. The configuration on the Catalyst switches is the same as the configuration on the Cisco CRS-1 router internal Broadcom switches—they all participate in a Multiple Spanning Tree (MST) region with one MST instance.

The Catalyst switches are made the root of the network by assigning them the highest priority. Because there are two Catalyst switches, one is selected as the root-bridge device. Configure the primary Catalyst switch with priority 0 to make the switch the root of the network. Configure the second Catalyst switch with a number greater than 0 and less than 32768. If the primary Catalyst switch (priority 0) fails, the second switch becomes the root of the network.

Configuring the Catalyst Switches

The Cisco IOS software configuration must be applied to both external Catalyst switches.

Note Configure the primary Catalyst switch with priority 0 to make the switch the root of the network. Configure the second Catalyst switch with a number greater than 0 and less than 32768. If the primary Catalyst switch (priority 0) fails, the second switch becomes the root of the network.

To configure the Catalyst 6509 Switches, use the following procedure:

Summary Steps

1. **configure**
2. **spanning-tree portfast default**
3. **spanning-tree mode mst**
4. **spanning-tree mst configuration**
5. **name** *mst_region*
6. **revision** *number*
7. **instance** *instance_id* **vlan** *range*
8. **end**
9. **spanning-tree mst hello-time** *seconds*
10. **spanning-tree mst forward-time** *seconds*
11. **spanning-tree mst max-age** *seconds*
12. **spanning-tree mst max-hops** *hops*
13. **spanning-tree mst** *instance_id* **priority** *priority*
14. **udld aggressive**
15. **udld message time** *interval*
16. **interface gigabitethernet** *slot/port*
17. **switchport**
18. **switchport mode access**
19. **switchport access vlan 1**
20. **end**
21. Repeat Step 16 through Step 20 for all interfaces.
22. Repeat all steps for the second switch.

Detailed Steps

	Command or Action	Purpose
Step 1	**configure** **Example:** `router# configure`	Places the switch in global configuration mode.
Step 2	**spanning-tree portfast default** **Example:** `router(config)# spanning-tree portfast default`	Enables PortFast by default on all access ports.
Step 3	**spanning-tree mode mst** **Example:** `router(config)# spanning-tree mode mst`	Selects the MST mode for the spanning tree protocol.
Step 4	**spanning-tree mst configuration** **Example:** `router(config)# spanning-tree mst configuration`	Places the router in spanning tree MST configuration mode.
Step 5	**name** *mst_region* **Example:** `router(config-mst)# name STP_1`	Defines a name for an MST region.
Step 6	**revision** *number* **Example:** `router(config-mst)# revision 1`	Sets a revision number for the MST configuration. • This number must be identical on both switches.
Step 7	**instance** *instance_id* **vlan** *range* **Example:** `router(config-mst)# instance 1 vlan 1`	Maps the MST instance to a range of VLANs.
Step 8	**end** **Example:** `router(config-mst)# end`	Exits spanning tree MST configuration mode.
Step 9	**spanning-tree mst hello-time** *seconds* **Example:** `router(config)# spanning-tree mst hello-time 1`	Sets the hello-time delay timer for all instances on the switch. • We recommend 1 second.
Step 10	**spanning-tree mst forward-time** *seconds* **Example:** `router(config)# spanning-tree mst forward-time 6`	Sets the forward-delay timer for all MST instances on the switch. • We recommend 6 seconds.

	Command or Action	Purpose
Step 11	**spanning-tree mst max-age** *seconds* **Example:** `router(config)# spanning-tree mst max-age 8`	Sets the maximum-age timer for all MST instances on the switch. • We recommend 8 seconds.
Step 12	**spanning-tree mst max-hops** *hops* **Example:** `router(config)# spanning-tree mst max-hops 4`	Specifies the number of possible hops in the region before a BPDU is discarded. • We recommend 4 hops.
Step 13	**spanning-tree mst** *instance_id* **priority** *priority* **Example:** `router(config)# spanning-tree mst 0-1 priority 28672`	Sets the spanning tree priority for the switch. • The primary Catalyst switch should be configured with priority 0. Priority 0 makes the switch the root of the network. • The second Catalyst switch should be configured with a number greater than 0 and less than 32768. If the primary Catalyst switch (priority 0) fails, the second switch becomes the root of the network.
Step 14	**udld aggressive** **Example:** `router(config)# udld aggressive`	Enables the Unidirectional Link Detection (UDLD) protocol aggressive mode.
Step 15	**udld message time** *interval* **Example:** `router(config)# udld message time 7`	Configures the time between UDLD probe messages on ports that are in advertisement mode and are currently determined to be bidirectional • Valid values are from 7 to 90 seconds. • We recommend 7 seconds.
Step 16	**interface gigabitethernet** *slot/port* **Example:** `router(config)# interface GigabitEthernet3/1`	Enters interface configuration mode for the specified interface.
Step 17	**switchport** **Example:** `router(config-if)# switchport`	Configures a LAN interface as a Layer 2 interface in preparation for additional **switchport** commands.
Step 18	**switchport mode access** **Example:** `router(config-if)# switchport mode access`	Specifies a nontrunking, nontagged single-VLAN Layer-2 interface.
Step 19	**switchport access vlan 1** **Example:** `router(config-if)# switchport access vlan 1`	(Optional) Assigns ports to VLAN 1, which is the default selection.

	Command or Action	Purpose
Step 20	**end** **Example:** `router(config-if)# end`	Exits interface configuration mode and returns to global configuration mode.
Step 21	Repeat Step 16 through Step 20 for all interfaces.	Configures remaining interfaces. • Repeat this configuration for each port, including ports that are not currently being used (for example, interface gigabitethernet 0/1).
Step 22	Repeat all steps for the second switch.	Configures a second switch for redundancy.

Example: Single-FCC Multishelf System Configuration

Note When configuring the Catalyst 6509 Switches, the difference between configuring single-, two-, and four-FCC multishelf systems is the number of interfaces that require configuration. When additional FCCs are present, additional interfaces must be configured for the connections to those FCCs.

First Catalyst Switch Configuration:

```
CAT6k-1# configure
CAT6k-1(config)# spanning-tree portfast default
CAT6k-1(config)# spanning-tree mode mst
CAT6k-1(config)# no spanning-tree optimize bpdu transmission
CAT6k-1(config)# spanning-tree mst configuration
CAT6k-1(config-mst)# name STP_1
CAT6k-1(config-mst)# revision 1
CAT6k-1(config-mst)# instance 1 vlan 1
CAT6k-1(config-mst)# end
CAT6k-1(config)# spanning-tree mst hello-time 1
CAT6k-1(config)# spanning-tree mst forward-time 6
CAT6k-1(config)# spanning-tree mst max-age 8
CAT6k-1(config)# spanning-tree mst max-hops 4
CAT6k-1(config)# spanning-tree mst 0-1 priority 0
CAT6k-1(config)# udld aggressive
CAT6k-1(config)# udld message time 7
CAT6k-1(config)# interface gigabitethernet 0/1
CAT6k-1(config-if)# switchport
CAT6k-1(config-if)# switchport mode access
CAT6k-1(config-if)# switchport access vlan 1

CAT6k-1(config-if)# end
```

Second Catalyst Switch Configuration:

```
CAT6k-2# configure
CAT6k-2(config)# spanning-tree portfast default
CAT6k-2(config)# spanning-tree mode mst
CAT6k-2(config)# no spanning-tree optimize bpdu transmission
CAT6k-2(config)# spanning-tree mst configuration
CAT6k-2(config-mst)# name STP_1
CAT6k-2(config-mst)# revision 1
CAT6k-2(config-mst)# instance 1 vlan 1
CAT6k-2(config-mst)# end
CAT6k-2(config)# spanning-tree mst hello-time 1
```

```
CAT6k-2(config)# spanning-tree mst forward-time 6
CAT6k-2(config)# spanning-tree mst max-age 8
CAT6k-2(config)# spanning-tree mst max-hops 4
CAT6k-2(config)# spanning-tree mst 0-1 priority 28672
CAT6k-2(config)# udld aggressive
CAT6k-2(config)# udld message time 7
CAT6k-2(config)# interface gigabitethernet 0/1
CAT6k-2(config-if)# switchport
CAT6k-2(config-if)# switchport mode access
CAT6k-2(config-if)# switchport access vlan 1

CAT6k-2(config-if)# end
```

Example: Four-FCC Multishelf System Configuration

Note When configuring the Catalyst 6509 Switches, the difference between configuring single-, two-, and four-FCC multishelf systems is the number of interfaces that require configuration. When additional FCCs are present, additional interfaces must be configured for the connections to those FCCs.

The following configuration display shows an example configuration for one of the Catalyst 6509 Switches in a four-FCC multishelf system:

```
Router# show running-config
Building configuration...

Current configuration : 2873 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service counters max age 10
!
hostname Router
!
logging snmp-authfail
!
ip subnet-zero
!
!
!
mpls ldp logging neighbor-changes
no mls flow ip
no mls flow ipv6
mls cef error action freeze
!
power redundancy-mode combined
!
spanning-tree mode mst
spanning-tree portfast default
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
spanning-tree mst configuration
 name STP_1
 revision 1
 instance 1 vlan 1
!
spanning-tree mst hello-time 1
```

```
spanning-tree mst forward-time 6
spanning-tree mst max-age 8
spanning-tree mst 0-1 priority 28672
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
!
redundancy
 mode sso
 main-cpu
  auto-sync running-config
  auto-sync standard
!
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
!
interface GigabitEthernet1/1
 no ip address
 switchport
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/2
 no ip address
 switchport
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/3
 no ip address
 switchport
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/4
 no ip address
 switchport
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/5
 no ip address
 switchport
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/6
 no ip address
 switchport
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/7
 no ip address
 switchport
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/8
 no ip address
 switchport
 switchport mode access
 spanning-tree portfast
!
```

```
interface GigabitEthernet1/9
 no ip address
 switchport
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/10
 no ip address
 switchport
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/11
 no ip address
 switchport
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/12
 no ip address
 switchport
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/13
 no ip address
 switchport
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/14
 no ip address
 switchport
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/15
 no ip address
 switchport
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/16
 no ip address
 switchport
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet5/1
 no ip address
 shutdown
!
interface GigabitEthernet5/2
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
no ip http server
!
!
```

```
!
!
!
line con 0
line vty 0 4
 login
!
End
```

Verifying the Catalyst Switch

As each rack in the multishelf system is brought up, verify that the Catalyst switch links are operating correctly by completing the tasks in the following sections:

- Verify the Interface Status
- Verify Communication Between the Catalyst Switch and an LCC or FCC
- Verify that the Links are Not Unidirectional

Verify the Interface Status

To verify that the interfaces are connected, enter the command **show interfaces status**. Enter the command on a terminal connected to each Catalyst switch.

```
CAT6k-1# show interfaces status

Port Name Status Vlan Duplex Speed Type
Gi1/1 connected 1 full 1000 1000BaseLH
Gi1/2 connected 1 full 1000 1000BaseLH
Gi1/3 connected 1 full 1000 1000BaseLH
Gi1/4 connected 1 full 1000 1000BaseLH
Gi1/5 connected 1 full 1000 1000BaseLH
Gi1/6 connected 1 full 1000 1000BaseLH
Gi1/7 disabled 1 full 1000 1000BaseSX
Gi1/8 disabled 1 full 1000 1000BaseSX
Gi1/9 disabled 1 full 1000 1000BaseSX
Gi1/10 disabled 1 full 1000 1000BaseSX
Gi1/11 disabled 1 full 1000 1000BaseSX
Gi1/12 disabled 1 full 1000 1000BaseSX
Gi1/13 disabled 1 full 1000 1000BaseSX
Gi1/14 disabled 1 full 1000 1000BaseSX
Gi1/15 disabled 1 full 1000 1000BaseSX
Gi1/16 disabled 1 full 1000 1000BaseSX
Gi5/1 disabled 1 full 1000 1000BaseSX
Gi5/2 connected routed a-full a-100 10/100/1000BaseT
CAT6k-1#
```

Verify Communication Between the Catalyst Switch and an LCC or FCC

To verify that the Catalyst switch is communicating with an LCC or FCC in forwarding mode, enter the command **show spanning tree**.

This command displays the states of the spanning tree ports. Verify that the ports used to connect the DSC, remote LCC RP, and FCC SCGE are in the FWDG state.

The listed interfaces should include the port to which you have connected. If the port is not listed, contact Cisco Technical Support. For contact information, see the "Obtaining Technical Assistance" section on page xiii.

```
CAT6k-1# show spanning-tree

MST00

Spanning tree enabled protocol mstp
Root ID Priority 0
Address 0013.1a4f.75c0
This bridge is the root
Hello Time 1 sec Max Age 8 sec Forward Delay 6 sec
Bridge ID Priority 0 (priority 0 sys-id-ext 0)
Address 0013.1a4f.75c0
Hello Time 1 sec Max Age 8 sec Forward Delay 6 sec
Interface Role Sts Cost Prio.Nbr Type

---------------- ---- --- --------- -------- --------------------------------

Gi1/1 Desg FWD 20000 128.1 P2p
Gi1/2 Desg FWD 20000 128.2 P2p
Gi1/3 Desg FWD 20000 128.3 P2p
Gi1/4 Desg FWD 20000 128.4 P2p
Gi1/5 Desg FWD 20000 128.5 P2p
Gi1/6 Desg FWD 20000 128.6 P2p


MST01
Spanning tree enabled protocol mstp
Root ID Priority 1
Address 0013.1a4f.75c0
This bridge is the root
Hello Time 1 sec Max Age 8 sec Forward Delay 6 sec
Bridge ID Priority 1 (priority 0 sys-id-ext 1)
Address 0013.1a4f.75c0
Hello Time 1 sec Max Age 8 sec Forward Delay 6 sec
Interface Role Sts Cost Prio.Nbr Type

---------------- ---- --- --------- -------- --------------------------------

Gi1/1 Desg FWD 20000 128.1 P2p
Gi1/2 Desg FWD 20000 128.2 P2p
Gi1/3 Desg FWD 20000 128.3 P2p
Gi1/4 Desg FWD 20000 128.4 P2p
Gi1/5 Desg FWD 20000 128.5 P2p
Gi1/6 Desg FWD 20000 128.6 P2p
CAT6k-1#
```

Verify that the Links are Not Unidirectional

After an LCC or FCC is brought up, verify that the Catalyst links are operating correctly. If a link has a partial fiber cut or a bad optic, the control Ethernet network can become unidirectional and cause a loop.

To verify the links in a Catalyst switch using the Cisco IOS software, enter the command **show interface** in EXEC mode.

In the following example, the command is entered for a specific port. The keywords **| inc Gig** narrows the output to Gigabit Ethernet ports.

```
Router# show interface gi 6/1 | inc Gig

GigabitEthernet6/1 is up, line protocol is up (connected)
Router#
```

The output of this command should display “connected.” If it does not, then the connector may have a partial fiber cut or a bad optic. You may need to jiggle the GBIC wire to ensure that it is firmly inserted. Re-enter the command **show interface** until the port displays a status of “connected” or “disabled” for every port that displays a connector type.

Caution If this problem is not resolved and the Cisco CRS-1 router enters the forwarding state, a loop occurs.

Bringing Up and Configuring Rack 0

When the control network has been established by installing, cabling, and configuring the Catalyst switches, it is time to bring up and configure Rack 0 in the multishelf system, as described in the following procedure.

Summary Steps

1. Power down all LCCs and FCCs.
2. Apply power to the LCC that contains the DSC.
3. Connect to the DSC console port and log in.
4. **admin**
5. **configure**
6. **dsc serial** *serial ID* **rack 0**
7. **dsc serial** *serial ID* **rack** *rackNumber*
8. **dsc serial** *serial ID* **rack F***n*
9. **commit**
10. **show running-config | include dsc**
11. **controllers fabric plane** *planeNumber*
    oim count 1
    oim instance 0 location F*rack*/*slot*/**FM**
12. **commit**
13. **end**

Detailed Steps

	Command or Action	Purpose
Step 1	Power down all LCCs and FCCs.	Prepares the LCCs and FCCs for startup in the proper sequence. • Each LCC and FCC should be powered up in the order specified in this chapter.
Step 2	Apply power to the LCC that contains the DSC.	Boots the LCC containing the DSC. • Allow the rack to fully boot. • Verify that "IOS XR RUN" appears on the RP faceplates. • See the Cisco CRS-1 documentation web page listed in the "Related Documents" section on page x for site planning information including DSC placement.

	Command or Action	Purpose
Step 3	Connect to the DSC console port and log in.	Establishes a CLI management session with the router. For more information, see the "Connecting to the Router Through the Console Port" section on page 1-9.
Step 4	**admin** **Example:** `RP/0/RP0/CPU0:router# admin`	Places the router in administration EXEC mode.
Step 5	**configure** **Example:** `RP/0/RP0/CPU0:router(admin)# configure`	Places the router in administration configuration mode.
Step 6	**dsc serial** *serial ID* **rack 0** **Example:** `RP/0/RP0/CPU0:router(admin-config)# dsc serial TBA00000001 rack 0`	Defines which LCC is Rack 0. • The LCC containing the DSC should be configured with the lowest rack number. • Replace *serial ID* with the serial number of the LCC you want to configure as Rack 0. • See the "Preparing a Rack Number Plan" section on page 3-3 for information on locating the serial number.
Step 7	**dsc serial** *serial ID* **rack** *rackNumber* **Example:** `RP/0/RP0/CPU0:router(admin-config)# dsc serial TBA00000002 rack 1`	Defines the rack number for the second LCC. • See the "Preparing a Rack Number Plan" section on page 3-3 for information on locating the serial numbers and selecting rack numbers. • Replace *serial ID* with the serial number of the second LCC. • Replace *rackNumber* with a number in the range of 1 to 255. • When each subsequent LCC comes on line, the DSC examines the chassis serial number and automatically assigns the correct rack number to that chassis.

	Command or Action	Purpose
Step 8	**dsc serial** *serial ID* **rack F***n* **Example:** `RP/0/RP0/CPU0:router(admin-config)# dsc serial TBA00000003 rack F0`	Defines the rack number for an FCC. • See the "Preparing a Rack Number Plan" section on page 3-3 for information on locating the serial numbers and selecting rack numbers. • Enter this command for every FCC in the multishelf system. • Replace *serial ID* with the serial number of the FCC. • Replace *n* with the FCC rack number. These numbers begin with F0 and increment to F1, F2, and F3. • When each subsequent rack comes on line, the DSC examines the chassis serial number and automatically assigns the correct rack number to that chassis.
Step 9	**commit** **Example:** `RP/0/RP0/CPU0:router(admin-config)# commit`	Commits the target configuration to the router running configuration.
Step 10	**show running-config | include dsc** **Example:** `RP/0/RP0/CPU0:router(admin-config)# show running-config | include dsc`	Displays the committed rack number configuration. Verify that the serial numbers entered for each chassis are correct.

Step 11	**controllers fabric plane** *planeNumber*
	oim count 1
	oim instance 0 location F*rack***/SM***slot***/FM**
	
	Example:
	`RP/0/RP0/CPU0:router(admin-config)# controllers fabric plane 0`
	`RP/0/RP0/CPU0:router(admin-config)# oim count 1`
	`RP/0/RP0/CPU0:router(admin-config)# oim instance 0 location F0/SM9/FM`
		Configures a plane to operate in an FCC slot.
		• Enter this command sequence for each of the eight fabric planes.
		• Replace *planeNumber* with the number of the plane (0 to 7) you want to configure.
		• Replace *rack* with the FCC rack number assigned to the FCC that hosts the plane.
		• Replace *slot* with the FCC slot number that supports the fabric plane you are configuring. Valid slot numbers are SM0 to SM23.
		• The plane numbers and slot numbers are determined by the hardware installation and cabling. The software configuration must match the hardware configuration. For more information, see *Cisco CRS-1 Carrier Routing System Multishelf System Interconnection and Cabling Guide*.

	Command or Action	Purpose
Step 12	**commit** **Example:** `RP/0/RP0/CPU0:router(admin-config)# commit`	Commits the target configuration to the router running configuration.

Step 13	**end**
	
	Example:
	`RP/0/RP0/CPU0:router(admin-config)# end`
	`RP/0/RP0/CPU0:router(admin)#`
		Exits administration configuration mode and enters administration EXEC mode.

Examples

This section contains examples for the following subjects:

- Example: Configuring and Verifying the Rack Numbers in a Single-FCC Multishelf System, page 3-25
- Example: Mapping Each Fabric Plane in a Single-FCC Multishelf System, page 3-25
- Example: Mapping Each Fabric Plane in a Two-FCC Multishelf System, page 3-26
- Example: Mapping Each Fabric Plane in a Four-FCC Multishelf System, page 3-27

Example: Configuring and Verifying the Rack Numbers in a Single-FCC Multishelf System

In the following example, rack numbers are assigned to each LCC and FCC in administration configuration mode:

```
RP/0/RP0/CPU0:router# admin
RP/0/RP0/CPU0:router(admin)# configure
RP/0/RP0/CPU0:router(admin-config)# dsc serial TBA00000001 rack 0
RP/0/RP0/CPU0:router(admin-config)# dsc serial TBA00000002 rack 1
RP/0/RP0/CPU0:router(admin-config)# dsc serial TBA00000003 rack F0
RP/0/RP0/CPU0:router(admin-config)# commit
RP/0/RP0/CPU0:router(admin-config)# show running-config | include dsc

Building configuration...
dsc serial TBA00000003 rack F0
dsc serial TBA00000001 rack 0
dsc serial TBA00000002 rack 1
RP/0/RP0/CPU0:router(admin-config)#
```

Example: Mapping Each Fabric Plane in a Single-FCC Multishelf System

In the following example, each fabric plane is assigned to an FCC slot in administration configuration mode:

```
RP/0/RP0/CPU0:router(admin-config)# controllers fabric plane 0
RP/0/RP0/CPU0:router(admin-config)# oim count 1
RP/0/RP0/CPU0:router(admin-config)# oim instance 0 location F0/SM9/FM

RP/0/RP0/CPU0:router(admin-config)# controllers fabric plane 1
RP/0/RP0/CPU0:router(admin-config)# oim count 1
RP/0/RP0/CPU0:router(admin-config)# oim instance 0 location F0/SM6/FM

RP/0/RP0/CPU0:router(admin-config)# controllers fabric plane 2
RP/0/RP0/CPU0:router(admin-config)# oim count 1
```

```
RP/0/RP0/CPU0:router(admin-config)# oim instance 0 location F0/SM3/FM

RP/0/RP0/CPU0:router(admin-config)# controllers fabric plane 3
RP/0/RP0/CPU0:router(admin-config)# oim count 1
RP/0/RP0/CPU0:router(admin-config)# oim instance 0 location F0/SM0/FM

RP/0/RP0/CPU0:router(admin-config)# controllers fabric plane 4
RP/0/RP0/CPU0:router(admin-config)# oim count 1
RP/0/RP0/CPU0:router(admin-config)# oim instance 0 location F0/SM12/FM

RP/0/RP0/CPU0:router(admin-config)# controllers fabric plane 5
RP/0/RP0/CPU0:router(admin-config)# oim count 1
RP/0/RP0/CPU0:router(admin-config)# oim instance 0 location F0/SM15/FM

RP/0/RP0/CPU0:router(admin-config)# controllers fabric plane 6
RP/0/RP0/CPU0:router(admin-config)# oim count 1
RP/0/RP0/CPU0:router(admin-config)# oim instance 0 location F0/SM18/FM

RP/0/RP0/CPU0:router(admin-config)# controllers fabric plane 7
RP/0/RP0/CPU0:router(admin-config)# oim count 1
RP/0/RP0/CPU0:router(admin-config)# oim instance 0 location F0/SM21/FM

RP/0/RP0/CPU0:router(admin-config)# commit
RP/0/RP0/CPU0:router(admin-config)# end
RP/0/RP0/CPU0:router(admin)#
```

Example: Mapping Each Fabric Plane in a Two-FCC Multishelf System

The following display is an example of a configuration for a two-FCC multishelf system:

```
P/0/RP0/CPU0:R2D2-L0(admin)# show running-config

Building configuration...
username admin
 secret 5 $1$iGx3$0BI/8hOKRUMqtfWC4IUn50
 group root-system
 group cisco-support
!
dsc serial TBA09250241 rack 1
dsc serial TBA09270100 rack F0
dsc serial TBA09300128 rack F1
controllers fabric plane 0
 oim count 1
 oim instance 0 location F0/SM0/FM
!
controllers fabric plane 1
 oim count 1
 oim instance 0 location F0/SM9/FM
!
controllers fabric plane 2
 oim count 1
 oim instance 0 location F0/SM12/FM
!
controllers fabric plane 3
 oim count 1
 oim instance 0 location F0/SM21/FM
!
controllers fabric plane 4
 oim count 1
 oim instance 0 location F1/SM0/FM
!
controllers fabric plane 5
 oim count 1
```

```
 oim instance 0 location F1/SM91/FM
!
controllers fabric plane 6
 oim count 1
 oim instance 0 location F1/SM12/FM
!
controllers fabric plane 7
 oim count 1
 oim instance 0 location F1/SM21/FM
!
end
```

Example: Mapping Each Fabric Plane in a Four-FCC Multishelf System

The following configuration display is an example of a configuration for a four-FCC multishelf system:

```
P/0/RP0/CPU0:R2D2-L0(admin)# show running-config

Building configuration...
username admin
 secret 5 $1$iGx3$0BI/8hOKRUMqtfWC4IUn50
 group root-system
 group cisco-support
!
dsc serial TBA09250241 rack 1
dsc serial TBA09270100 rack F0
dsc serial TBA09300128 rack F1
dsc serial TBA09460027 rack F3
dsc serial TBA09460028 rack F2
controllers fabric plane 0
 oim count 1
 oim instance 0 location F0/SM0/FM
!
controllers fabric plane 1
 oim count 1
 oim instance 0 location F0/SM9/FM
!
controllers fabric plane 2
 oim count 1
 oim instance 0 location F1/SM0/FM
!
controllers fabric plane 3
 oim count 1
 oim instance 0 location F1/SM9/FM
!
controllers fabric plane 4
 oim count 1
 oim instance 0 location F2/SM0/FM
!
controllers fabric plane 5
 oim count 1
 oim instance 0 location F2/SM9/FM
!
controllers fabric plane 6
 oim count 1
 oim instance 0 location F3/SM0/FM
!
controllers fabric plane 7
 oim count 1
 oim instance 0 location F3/SM9/FM
!
end
```

Bringing Up and Verifying FCCs

When Rack 0 is up and configured to support the rack number and FCC fabric plane plans, it is time to bring up and configure the FCC in the multishelf system as described in the following procedure.

Summary Steps

1. Apply power to all FCCs.
2. **show controllers fabric rack all detail**
3. **show controllers fabric plane all detail**
4. **show controllers fabric connectivity all detail**
5. On the external Catalyst switches, verify that the links are not unidirectional.

Detailed Steps

	Command or Action	Purpose
Step 1	Apply power to all FCCs.	Starts the FCCs. • Allow each FCC to fully boot. • Verify that "IOS XR RUN" appears on the SC faceplates. • Verify that the indicator LED on the OIM LED panel is green for each fabric cable connected to Rack 0. • Each FCC loads any required software and configurations from the DSC, including the rack number and appropriate Cisco IOS XR software packages. • Do not proceed until both SCGEs in each FCC display "IOS XR RUN." This message indicates that each SCGE has successfully loaded the Cisco IOS XR software.
Step 2	**show controllers fabric rack all detail** **Example:** `RP/0/RP0/CPU0:router(admin)# show controllers fabric rack all detail`	Displays the status of all racks in the system. • In a properly operating system, the rack status for all racks should be *Normal*, and the server status should be *Present*.

	Command or Action	Purpose
Step 3	**show controllers fabric plane all detail** **Example:** `RP/0/RP0/CPU0:router(admin)# show controllers fabric plane all detail`	Displays the status of all racks and additional information for racks in installation mode. • Wait for the status in the *Admin State* and *Oper State* columns to change to UP for all planes.
Step 4	**show controllers fabric connectivity all detail** **Example:** `RP/0/RP0/CPU0:router(admin)# show controllers fabric connectivity all detail`	Displays the LCC cards that can communicate with all eight fabric planes. • The expected output should contain a series of '1's for each of the fabric planes active in the system. If a fabric plane is administratively "shutdown" the output of the command above remains the same. If the fabric card is physically removed or powered down, the "1" changes to "."
Step 5	On the external Catalyst switches, verify that the links are not unidirectional.	Verifies that the links from the chassis to the external Catalyst switches are operating correctly. • If a unidirectional link is present, a loop may occur. • For instructions to verify the Catalyst links, see the "Verifying the Catalyst Switch" section on page 3-19. The verification commands must be entered from a terminal directly connected to the external Catalyst switches, using Cisco IOS CLI commands.

Examples

This section contains an example for the following task:

- Verify That All Fabric Planes Are Ready to Handle Data, page 3-29

Verify That All Fabric Planes Are Ready to Handle Data

In the following examples, the fabric planes are examined in administration EXEC mode to ensure that they are ready to handle traffic.

show controllers fabric rack all detail

In the following example, the rack status is normal and the server status is present.

```
RP/0/RP0/CPU0:router(admin)# show controllers fabric rack all detail

Rack   Rack       Server
Num    Status     Status
----   ------     ------

 0       NORMAL    PRESENT
 1       NORMAL    PRESENT
 F0      NORMAL    PRESENT
RP/0/RP0/CPU0:router(admin)#
```

show controllers fabric plane all detail

In the following example, all eight planes are displayed, and the administrative and operational state of each plane is up.

```
RP/0/RP0/CPU0:CRS-8_P1(admin)# show controllers fabric plane all detail

  Flags: P - plane admin down,       p - plane oper down
         C - card admin down,        c - card  oper down
         L - link port admin down,   l - linkport oper down
         A - asic admin down,        a - asic oper down
         B - bundle port admin Down, b - bundle port oper down
         I - bundle admin down,      i - bundle oper down
         N - node admin down,        n - node down
         o - other end of link down  d - data down
         f - failed component downstream
         m - plane multicast down

 Plane  Admin   Oper       Down       Total     Down
 Id     State   State      Flags      Bundles   Bundles
 ------------------------------------------------------
 0      UP      UP                    0         0
 1      UP      UP                    0         0
 2      UP      UP                    0         0
 3      UP      UP                    0         0
 4      UP      UP                    0         0
 5      UP      UP                    0         0
 6      UP      UP                    0         0
 7      UP      UP                    0         0
```

show controllers fabric connectivity all detail

The expected output should contain a series of 1s for each of the fabric planes active in the system. If a fabric plane is administratively shut down, the output of the command remains the same. If the fabric card is physically removed or powered down, the 1 changes to a dot (.).

```
RP/0/RP0/CPU0:CRS-8_P1(admin)# show controllers fabric connectivity all detail

Flags: P - plane admin down,       p - plane oper down
         C - card admin down,        c - card  oper down
         L - link port admin down,   l - linkport oper down
         A - asic admin down,        a - asic oper down
         B - bundle port admin Down, b - bundle port oper down
         I - bundle admin down,      i - bundle oper down
         N - node admin down,        n - node down
         o - other end of link down  d - data down
         f - failed component downstream
         m - plane multicast down

 Card       In  Tx Planes  Rx Planes  Monitored        Total            Percent
 R/S/M      Use 01234567   01234567   For (s)          Uptime (s)       Uptime
-------------------------------------------------------------------------------
0/1/CPU0    1   11111111   11111111   1245608          1245608          100.0000
0/6/CPU0    1   11111111   11111111   1245608          1245608          100.0000
0/RP0/CPU0  1   11111111   11111111   1245608          1245608          100.0000
0/RP1/CPU0  1   11111111   11111111   1245608          1245608          100.0000
```

Bringing Up and Verifying the Non-DSC LCC

When all FCCs are up and properly supporting Rack 0, it is time to bring up and configure the next LCC in the multishelf system as described in the following procedure:

Summary Steps

1. Apply power to the second LCC.
2. **show controllers fabric rack all detail**
3. **show controllers fabric plane all detail**
4. **show controllers fabric connectivity all detail**
5. On the external Catalyst switches, verify that the links are not unidirectional.
6. **exit**

Detailed Steps

	Command or Action	Purpose
Step 1	Apply power to the second LCC.	Starts up the LCC. • Allow the chassis to fully boot. • Verify that "IOS XR RUN" appears on the RP faceplates. • In each FCC, verify that the indicator LED on the OIM LED panel is green for each fabric cable connected to the non-DSC LCC. • The LCC loads any necessary software and configurations from the DSC, including the rack number and appropriate Cisco IOS XR software packages. • Do not proceed until both RPs in the LCC display "IOS XR RUN." This indicates that the RP has successfully loaded the Cisco IOS XR software.
Step 2	**show controllers fabric rack all detail** **Example:** `RP/0/RP0/CPU0:router(admin)# show controllers fabric rack all detail`	Displays the status of all racks in the system. • In a properly operating system, the rack status for all racks should be *Normal*, and the server status should be *Present*.
Step 3	**show controllers fabric plane all detail** **Example:** `RP/0/RP0/CPU0:router(admin)# show controllers fabric plane all detail`	Displays the status of all racks and additional information for racks in install mode. • Wait for the status in the *Admin State* and *Oper State* columns to change to UP for all planes.

	Command or Action	Purpose
Step 4	**show controllers fabric connectivity all detail** **Example:** `RP/0/RP0/CPU0:router(admin)# show controllers fabric connectivity all detail`	Displays the LCC cards that can communicate with all eight fabric planes. • The expected output should contain a series of '1's for each of the fabric planes active in the system. If a fabric plane is administratively "shutdown" the output of the command above remains the same. If the fabric card is physically removed or powered down, the "1" changes to "."
Step 5	On the external Catalyst switches, verify that the links are not unidirectional.	Verifies that the links from the chassis to the external Catalyst switches are operating correctly. • If a unidirectional link is present, a loop may occur. • For instructions to verify the Catalyst links, see the "Verifying the Catalyst Switch" section on page 3-19. The verification commands must be entered from a terminal directly connected to the external Catalyst switches, using Cisco IOS CLI commands.

Step 6	**exit**
	
	Example:
	`RP/0/RP0/CPU0:router(admin)# exit`
	`RP/0/RP0/CPU0:router#`
		Exits administration EXEC mode and returns to EXEC mode.

Verifying the Spanning Tree

When both LCCs and all FCCs are up and running, it is time to verify the spanning tree on the control network as described in the following procedure.

Summary Steps

1. **admin**
2. **show platform**
3. **show spantree mst 1 detail location** *rack*/*slot*/**cpu0**

Detailed Steps

	Command or Action	Purpose
Step 1	**admin** **Example:** `RP/0/RP0/CPU0:router# admin`	Places the router in administration EXEC mode. • All commands listed in this procedure should be entered on the pre-existing single-chassis system.
Step 2	**show platform** **Example:** `RP/0/RP0/CPU0:router(admin)# show platform`	Displays the status of all hardware components. • The state for all modules should be **IOS XR RUN** or **OK**. • It can take a few minutes for all LCC modules to start up. **Note** To view the status of all cards and modules, the **show platform** command must be executed in administration EXEC mode.

	Command or Action	Purpose

Step 3	**show spantree mst 1 detail location** *rack*/*slot*/**cpu0**
	
	Example:
	`RP/0/RP0/CPU0:router(admin)# show spantree mst 1 detail location 0/rp0/cpu0`
	`RP/0/RP0/CPU0:router(admin)# show spantree mst 1 detail location 0/rp1/cpu0`
	`RP/0/RP0/CPU0:router(admin)# show spantree mst 1 detail location 1/rp0/cpu0`
	`RP/0/RP0/CPU0:router(admin)# show spantree mst 1 detail location 1/rp1/cpu0`
	`RP/0/RP0/CPU0:router(admin)# show spantree mst 1 detail location F0/SC0/cpu0`
	`RP/0/RP0/CPU0:router(admin)# show spantree mst 1 detail location F0/SC1/cpu0`
		Verifies the spanning tree.
		• Enter this command for each RP and SCGE card in the system.
		• The output for each RP and SCGE card should display the following:
		– In the Switched Interface column, one GE port should be in the forwarding (FWD) state.
		– Each RP and SCGE card should display the same designated root MAC address.
		• Verify that the designated root address matches the expected Catalyst switch, as defined by the Catalyst switch configuration. The root address should be the switch with the lowest priority number (0).
		• For more information to configure and verify the external Catalyst switches, see the "Verifying the Catalyst Switch" section on page 3-19.

Examples

This section contains examples for the following subjects:

Verify That the FCCs and Non-DSC LCC Are Communicating with the DSC

In the following EXEC mode example, all modules are displayed and the state for all modules is "IOS XR RUN."

```
RP/0/RP0/CPU0:router# admin

RP/0/RP0/CPU0:router(admin)# show platform

Node            Type            PLIM            State           Config State
------------------------------------------------------------------------------
0/3/SP          MSC(SP)         N/A             IOS XR RUN      PWR,NSHUT,MON
0/3/CPU0        MSC             16OC48-POS/DPT  IOS XR RUN      PWR,NSHUT,MON
0/RP0/CPU0      RP(Active)      N/A             IOS XR RUN      PWR,NSHUT,MON
0/RP1/CPU0      RP(Standby)     N/A             IOS XR RUN      PWR,NSHUT,MON
0/FC0/SP        LCC-FAN-CT(SP)  N/A             IOS XR RUN      PWR,NSHUT,MON
0/FC1/SP        LCC-FAN-CT(SP)  N/A             IOS XR RUN      PWR,NSHUT,MON
0/AM0/SP        ALARM(SP)       N/A             IOS XR RUN      PWR,NSHUT,MON
0/AM1/SP        ALARM(SP)       N/A             IOS XR RUN      PWR,NSHUT,MON
0/SM0/SP        FC/M(SP)        N/A             IOS XR RUN      PWR,NSHUT,MON
0/SM1/SP        FC/M(SP)        N/A             IOS XR RUN      PWR,NSHUT,MON
0/SM2/SP        FC/M(SP)        N/A             IOS XR RUN      PWR,NSHUT,MON
0/SM3/SP        FC/M(SP)        N/A             IOS XR RUN      PWR,NSHUT,MON
0/SM4/SP        FC/M(SP)        N/A             IOS XR RUN      PWR,NSHUT,MON
0/SM5/SP        FC/M(SP)        N/A             IOS XR RUN      PWR,NSHUT,MON
0/SM6/SP        FC/M(SP)        N/A             IOS XR RUN      PWR,NSHUT,MON
0/SM7/SP        FC/M(SP)        N/A             IOS XR RUN      PWR,NSHUT,MON
1/3/SP          MSC(SP)         N/A             IOS XR RUN      PWR,NSHUT,MON
1/3/CPU0        MSC             8-10GbE         IOS XR RUN      PWR,NSHUT,MON
1/RP0/CPU0      RP(Active)      N/A             IOS XR RUN      PWR,NSHUT,MON
1/FC0/SP        LCC-FAN-CT(SP)  N/A             IOS XR RUN      PWR,NSHUT,MON
1/FC1/SP        LCC-FAN-CT(SP)  N/A             IOS XR RUN      PWR,NSHUT,MON
1/AM0/SP        ALARM(SP)       N/A             IOS XR RUN      PWR,NSHUT,MON
1/AM1/SP        ALARM(SP)       N/A             IOS XR RUN      PWR,NSHUT,MON
1/SM0/SP        FC/M(SP)        N/A             IOS XR RUN      PWR,NSHUT,MON
1/SM1/SP        FC/M(SP)        N/A             IOS XR RUN      PWR,NSHUT,MON
1/SM2/SP        FC/M(SP)        N/A             IOS XR RUN      PWR,NSHUT,MON
1/SM3/SP        FC/M(SP)        N/A             IOS XR RUN      PWR,NSHUT,MON
1/SM4/SP        FC/M(SP)        N/A             IOS XR RUN      PWR,NSHUT,MON
1/SM5/SP        FC/M(SP)        N/A             IOS XR RUN      PWR,NSHUT,MON
1/SM6/SP        FC/M(SP)        N/A             IOS XR RUN      PWR,NSHUT,MON
1/SM7/SP        FC/M(SP)        N/A             IOS XR RUN      PWR,NSHUT,MON
F0/SM0/SP       FCC-SFC(SP)     FCC-FM-1S       IOS XR RUN      PWR,NSHUT,MON
F0/SM3/SP       FCC-SFC(SP)     FCC-FM-1S       IOS XR RUN      PWR,NSHUT,MON
F0/SM6/SP       FCC-SFC(SP)     FCC-FM-1S       IOS XR RUN      PWR,NSHUT,MON
F0/SM9/SP       FCC-SFC(SP)     FCC-FM-1S       IOS XR RUN      PWR,NSHUT,MON
F0/SM12/SP      FCC-SFC(SP)     FCC-FM-1S       IOS XR RUN      PWR,NSHUT,MON
F0/SM15/SP      FCC-SFC(SP)     FCC-FM-1S       IOS XR RUN      PWR,NSHUT,MON
F0/SM18/SP      FCC-SFC(SP)     FCC-FM-1S       IOS XR RUN      PWR,NSHUT,MON
F0/SM21/SP      FCC-SFC(SP)     FCC-FM-1S       IOS XR RUN      PWR,NSHUT,MON
F0/SC0/CPU0     FCC-SC(Active)  N/A             IOS XR RUN      PWR,NSHUT,MON
F0/SC1/CPU0     FCC-SC(Standby) N/A             PRESENT         PWR,NSHUT,MON
F0/AM1/SP       ALARM(SP)       N/A             IOS XR RUN      PWR,NSHUT,MON

RP/0/RP0/CPU0:router(admin)# end
```

Verify the Spanning Tree

For each RP and SCGE card in the system, verify that:

- One GE port in the Switched Interface column is in the forwarding (FWD) state.
- Each RP and SCGE card displays the same designated root MAC address.
- The designated root address matches the expected Catalyst switch, as defined by the Catalyst switch configuration. The root address should be the switch with the lowest priority number (0).

The following EXEC commands display RP and SCGE card information that you can use to verify the spanning tree:

```
RP/0/RP0/CPU0:router(admin)# show spantree mst 1 detail location 0/rp0/cpu0

Instance                1
Vlans mapped:           1

Designated Root         00-0e-39-fe-70-00
Designated Root Priority 1 (0 + 1)
Designated Root Port    GE_Port_0

Bridge ID MAC ADDR      00-05-9a-3e-89-4f
Bridge ID Priority      32769 (32768 + 1)
Bridge Max Age  8 sec   Hello Time  1 sec   Forward Delay  6 sec   Max Hops 4

Switched Interface   State Role   Cost    Prio Type
-------------------- ----- ---- --------- ---- --------------------------------
FE_Port_1              BLK altn    200000  128  P2P
GE_Port_0              FWD root     20000  128  P2P
GE_Port_1              BLK altn     20000  128  P2P


RP/0/RP0/CPU0:router(admin)# show spantree mst 1 detail location 0/rp1/cpu0

Instance                1
Vlans mapped:           1

Designated Root         00-0e-39-fe-70-00
Designated Root Priority 1 (0 + 1)
Designated Root Port    GE_Port_0

Bridge ID MAC ADDR      00-05-9a-39-91-14
Bridge ID Priority      32769 (32768 + 1)
Bridge Max Age  8 sec   Hello Time  1 sec   Forward Delay  6 sec   Max Hops 4

Switched Interface   State Role   Cost    Prio Type
-------------------- ----- ---- --------- ---- --------------------------------
FE_Port_0              FWD desg    200000  128  P2P
GE_Port_0              FWD root     20000  128  P2P
GE_Port_1              BLK altn     20000  128  P2P
```

```
RP/0/RP0/CPU0:router(admin)# show spantree mst 1 detail location 1/rp0/cpu0

Instance                 1
Vlans mapped:            1

Designated Root          00-0e-39-fe-70-00
Designated Root Priority 1 (0 + 1)
Designated Root Port     GE_Port_0

Bridge ID MAC ADDR       00-05-9a-3e-89-2a
Bridge ID Priority       32769 (32768 + 1)
Bridge Max Age  8 sec    Hello Time  1 sec   Forward Delay  6 sec   Max Hops 4

Switched Interface   State Role   Cost    Prio Type
-------------------- ----- ---- --------- ---- --------------------------------
FE_Port_1              FWD desg    200000  128  P2P
GE_Port_0              FWD root     20000  128  P2P
GE_Port_1              BLK altn     20000  128  P2P


RP/0/RP0/CPU0:router(admin)# show spantree mst 1 detail location 1/rp1/cpu0

Instance                 1
Vlans mapped:            1

Designated Root          00-0e-39-fe-70-00
Designated Root Priority 1 (0 + 1)
Designated Root Port     GE_Port_0

Bridge ID MAC ADDR       00-05-9a-3e-89-fe
Bridge ID Priority       32769 (32768 + 1)
Bridge Max Age  8 sec    Hello Time  1 sec   Forward Delay  6 sec   Max Hops 4

Switched Interface   State Role   Cost    Prio Type
-------------------- ----- ---- --------- ---- --------------------------------
FE_Port_0              BLK altn    200000  128  P2P
GE_Port_0              FWD root     20000  128  P2P
GE_Port_1              BLK altn     20000  128  P2P


RP/0/RP0/CPU0:router(admin)# show spantree mst 1 detail location F0/SC0/cpu0

Instance                 1
Vlans mapped:            1

Designated Root          00-0e-39-fe-70-00
Designated Root Priority 1 (0 + 1)
Designated Root Port     GE_Port_1

Bridge ID MAC ADDR       00-05-9a-39-91-be
Bridge ID Priority       32769 (32768 + 1)
Bridge Max Age  8 sec    Hello Time  1 sec   Forward Delay  6 sec   Max Hops 4

Switched Interface   State Role   Cost    Prio Type
-------------------- ----- ---- --------- ---- --------------------------------
FE_Port_1              BLK altn    200000  128  P2P
GE_Port_0              BLK altn     20000  128  P2P
GE_Port_1              FWD root     20000  128  P2P
```

```
RP/0/RP0/CPU0:router(admin)# show spantree mst 1 detail location F0/SC1/cpu0

Instance                1
Vlans mapped:           1

Designated Root         00-0e-39-fe-70-00
Designated Root Priority 1 (0 + 1)
Designated Root Port    GE_Port_1

Bridge ID MAC ADDR      00-05-9a-39-91-68
Bridge ID Priority      32769 (32768 + 1)
Bridge Max Age  8 sec   Hello Time  1 sec   Forward Delay  6 sec   Max Hops 4

Switched Interface   State Role   Cost    Prio Type
-------------------- ----- ---- --------- ---- --------------------------------
FE_Port_0              FWD desg    200000  128  P2P
GE_Port_0              BLK altn     20000  128  P2P
GE_Port_1              FWD root     20000  128  P2P
```

Verifying Fabric Cabling Connections

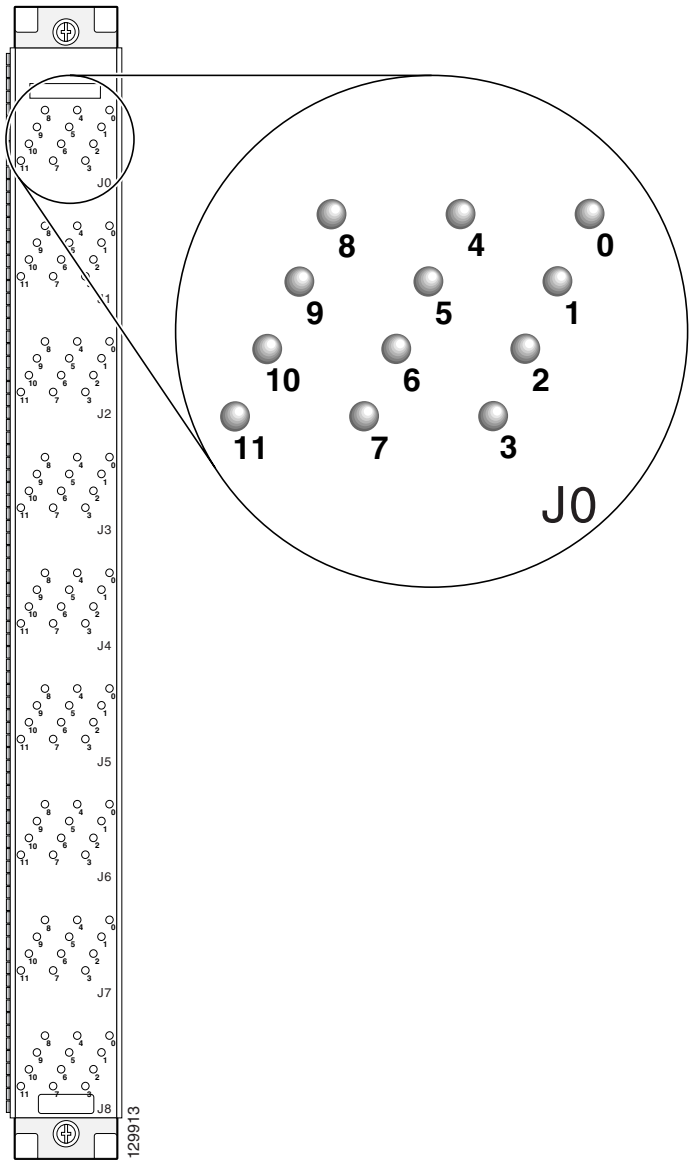
When the fabric cabling is complete and the power is on for all LCCs and FCCs, you can verify the fabric cabling connections, as described in this section.

Figure 3-5 shows the faceplate of the CRS-FCC- LED panel. The CRS-FCC-LED is also called an *optical interface module (OIM) LED panel*. This panel goes into slot LM0 or LM1 in a fabric card chassis.The OIM LED panel provides connectivity information on how the fabric chassis cards are functioning in the multishelf system. LEDs 0 through 11 correspond to OIM 0 through OIM 11 (FM 0 through FM 11 in software). Table 3-4 describes the possible states of the LEDs shown in Figure 3-5.

Table 3-4 LED Status Interpretation

LED State and Color	Meaning
Off	If the LED is off, it can mean: • The board to which the fabric cable is connected is powered off at one end or the other • The board is not present • The fabric cable is not connected at one end or the other.
Green	The fabric cable is properly connected at both ends, and data transmission is okay.
Yellow	The fabric cable is properly connected at both ends, but there are some data errors.
Red	The fabric cable is not connected to the correct place (when more than one fabric cable is incorrect).
Blinking red	The fabric cable is not connected to the correct place (when the fabric cable is the only or “first” such fabric cable)
Blinking green	The blinking LED indicates the place where the first and only incorrect fabric cable should be connected (corresponds to the blinking red above).

Figure 3-5 Optical Interface Module LED Panel (Part CRS-FCC-LED)



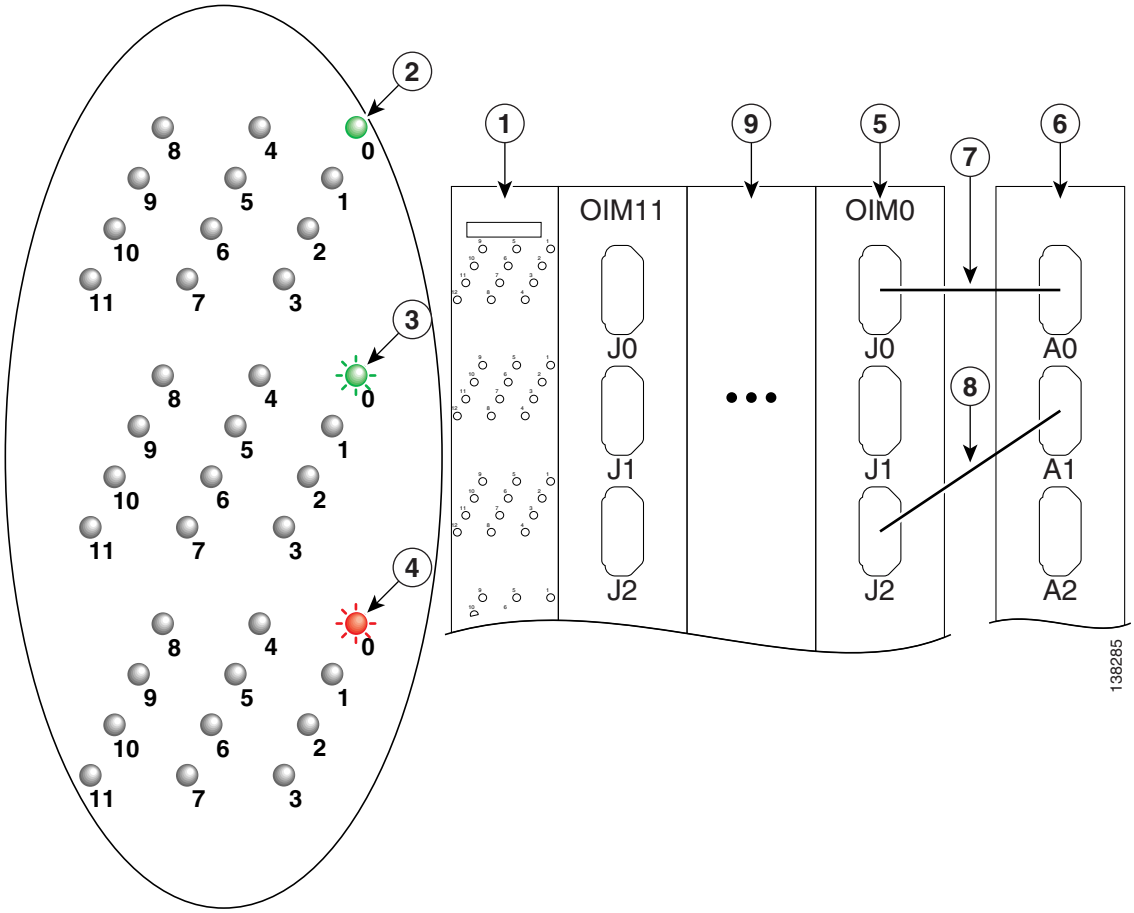
Because the OIM LED panel is present only in the fabric card chassis, the LEDs indicate the status of the bundles in the fabric card chassis only. Therefore, if a connection is wrong, the equipment assumes that the connection at the line card chassis is fixed, and the connection at the fabric card chassis is the one that needs to be relocated to the correct position as indicated by the LEDs.

Bundles are mapped to LEDs as follows:

The OIM LED panel has 9 rows of 12 LEDs— the 9 rows correspond to the 9 connectors for each slot, and 12 LEDs correspond to the 12 slots in the cage. Separate OIM LED panels provide status for the upper and lower card cages. The LED rows map to the connector number, and the LEDs in each LED row map to the slot number.

The following description helps explain the states of LEDs on the OIM LED panel. In Figure 3-6, fabric cables should connect an LCC S13 card to the FCC S2 card as follows: A0 to J0, A1 to J1, and A2 to J2. Instead, A1 is incorrectly connected to J2. This incorrect connection causes the LED corresponding to J2 to blink red, indicating that the cable connection is incorrect. The LED corresponding to J1 blinks green to show where the misplaced cable should be connected.

Figure 3-6 Illustration of How OIM LED Panel LEDs Map to Bundles and Slots (Single-Module Cabling)



1	OIM LED card	**6**	S13 card—This card is installed in an LCC.
2	Solid green LED—Indicates that the fabric cable connected to the corresponding port (J0) is connected correctly.	**7**	Correct fabric cable connection between FCC and LCC.
3	Flashing green LED—Indicates that a single fabric cable is incorrectly connected and should be connected to the corresponding connector (J1).	**8**	Incorrect fabric cable connection between FCC and LCC.
4	Flashing red LED—Indicates that a single fabric cable is incorrectly connected to the corresponding connector (J2).	**9**	Fabric card chassis
5	OIM card		

Where to Go Next

For information on configuring basic router features, see Chapter 4, "Configuring General Router Features."

CHAPTER 4

Configuring General Router Features

This chapter describes how to communicate with the router using the command-line interface (CLI), and it describes basic Cisco IOS XR software configuration management.

Contents

The chapter contains the following sections:

Secure Domain Routers

Cisco CRS-1 routers and Cisco XR 12000 Series Routers can be partitioned into multiple, independent routers known as *secure domain routers* (SDRs). Every router ships with a default SDR, which is called the *owner SDR* because it by default owns all RPs and line cards installed in the routing system. To build additional SDRs, you must create each SDR using configuration commands, name the SDR, assign RP, DRP, and line cards to the SDR, and then configure the interfaces on the line cards on the new SDR. An SDR is a group of cards within a router that is configured to operate as an independent router. SDRs that are created with configuration commands are called *named SDRs* and are configured with custom names to distinguish them from the owner SDR and other named SDRs.

SDRs perform routing functions in the same manner as a physical router, but share some chassis resources with the rest of the system. For example, the applications, configurations, protocols, and routing tables assigned to an SDR belong to that SDR only, but other functions, such as chassis control, switch fabric, and partitioning, are shared with the rest of the system.

To manage the owner SDR, you must connect to the active RP for the owner SDR. In administration configuration mode, you can define new SDRs and assign resources to them (such as DRPs, MSCs, and line cards.) In configuration mode, you can configure the operation of the owner SDR. Although you can reassign cards from one SDR to another, you cannot configure and manage cards assigned to a named SDR. To manage cards assigned to a named SDR, you must connect to the appropriate named SDR.

When you manage a named SDR, you must connect to the active RP for that named SDR. You can connect to the named SDR using any of the connection methods you use for the owner SDR (for example, you can connect through the console port or the Management Ethernet interface), and you have control over only the cards assigned to that named SDR. For example, you cannot configure and manage interfaces on line cards assigned to the owner SDR or other SDRs unless you connect directly to those SDRs.

Note Cisco IOS XR Software releases 2, 3, and 3.2 support only one SDR on the Cisco CRS-1 router. Cisco IOS XR Software Release 3.2 supports multiple SDRs on Cisco XR 12000 Series Routers, and Cisco IOS XR Software Release 3.3 supports multiple SDRs on the Cisco CRS-1 routers and Cisco XR 12000 Series Routers. For more information, see *Cisco IOS XR System Management Configuration Guide.*

Connecting and Communicating with the Router

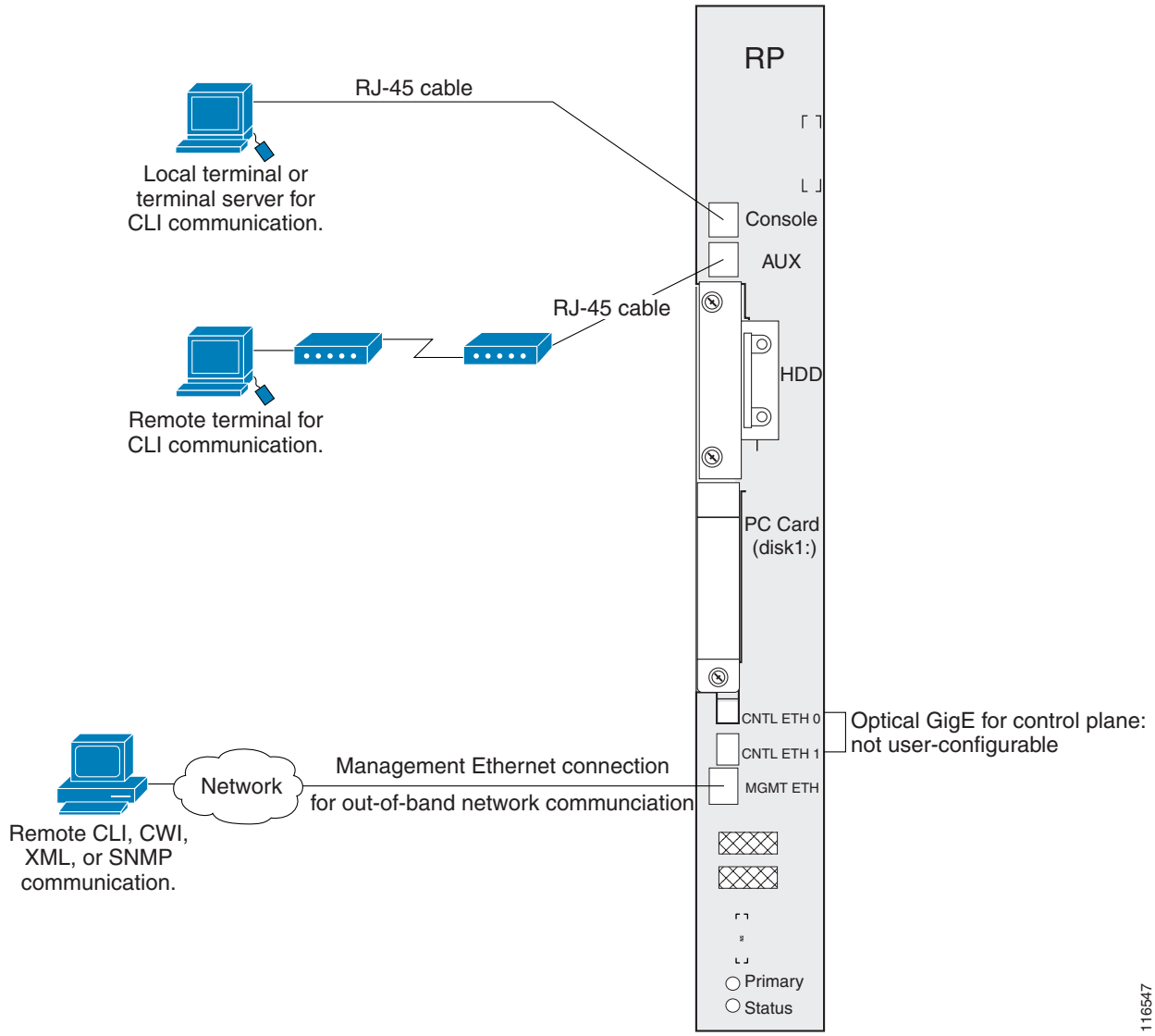
To manage or configure a router running the Cisco IOS XR software, you must first connect to the router using a terminal or a PC. Before you connect to the router, you must determine which router entity you want to manage. You can manage the following router entities:

- Owner SDR. Connect to the designated shelf controller (DSC).
- Router or multishelf system hardware. Connect to the DSC.
- Named SDR. For Cisco CRS-1 routers, connect to the RP or DRP that serves as the designated SDR system controller (DSDRSC) for that named SDR. For Cisco XR 12000 Series Routers, connect to the RP that serves as the DSDRSC for that named SDR.

Connections are made either through a direct physical connection to the Console port of the DSC or DSDRSC or from a remote location using a modem or an Ethernet connection that leads to the DSC or DSDRSC.

- Figure 4-1 shows the RP connections on the Cisco CRS-1 16-Slot Line Card Chassis (LCC), and Figure 4-2 shows the RP connections on the Cisco CRS-1 4-Slot and 8-Slot LCCs.
- Figure 4-3 shows the DRP PLIM connections.
- Figure 4-4 shows the performance route processor 1 (PRP-1) connections for a Cisco XR 12000 Series Router.
- Figure 4-5 shows the performance route processor 2 (PRP-2) connections for a Cisco XR 12000 Series Router.

Figure 4-1 Communication Ports on the RP for a Cisco CRS-1 16-Slot Line Card Chassis



The first time a router is started, you must use a direct connection to the DSC Console port to connect to the router and enter the initial configuration. When you use a direct connection to the Console port, CLI commands are entered at a terminal or at a computer running terminal emulation software. A direct Console port connection is useful for entering initial configurations and performing some debugging tasks.

This chapter describes some of the tasks you might want to perform during your initial configuration. One of those tasks is the configuration of the Management Ethernet interface, which is described in the "Configuring the Management Ethernet Interface" section on page 4-40. After the Management Ethernet interface is configured, most router management and configuration sessions take place over an Ethernet network connected to the Management Ethernet interface. SNMP agents and the CWI also use the network connection.

The modem connection can be used for remote communications with the router and serves as an alternate remote communications path if the Management Ethernet interface fails.

Figure 4-2 Communication Ports on the RP for a Cisco CRS-1 4-Slot and 8-Slot LCCs

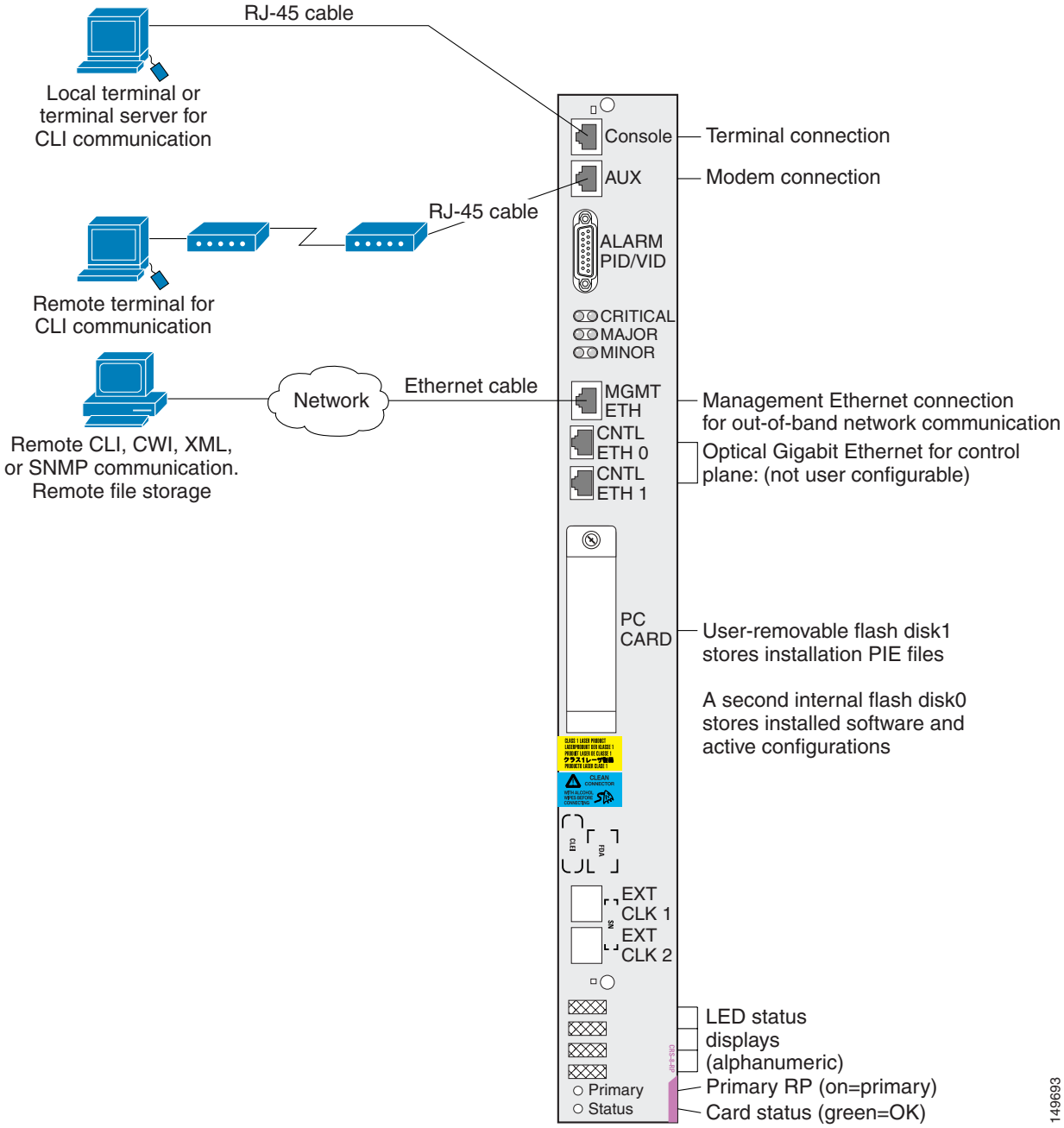


Figure 4-3 Communication Ports on the DRP PLIM

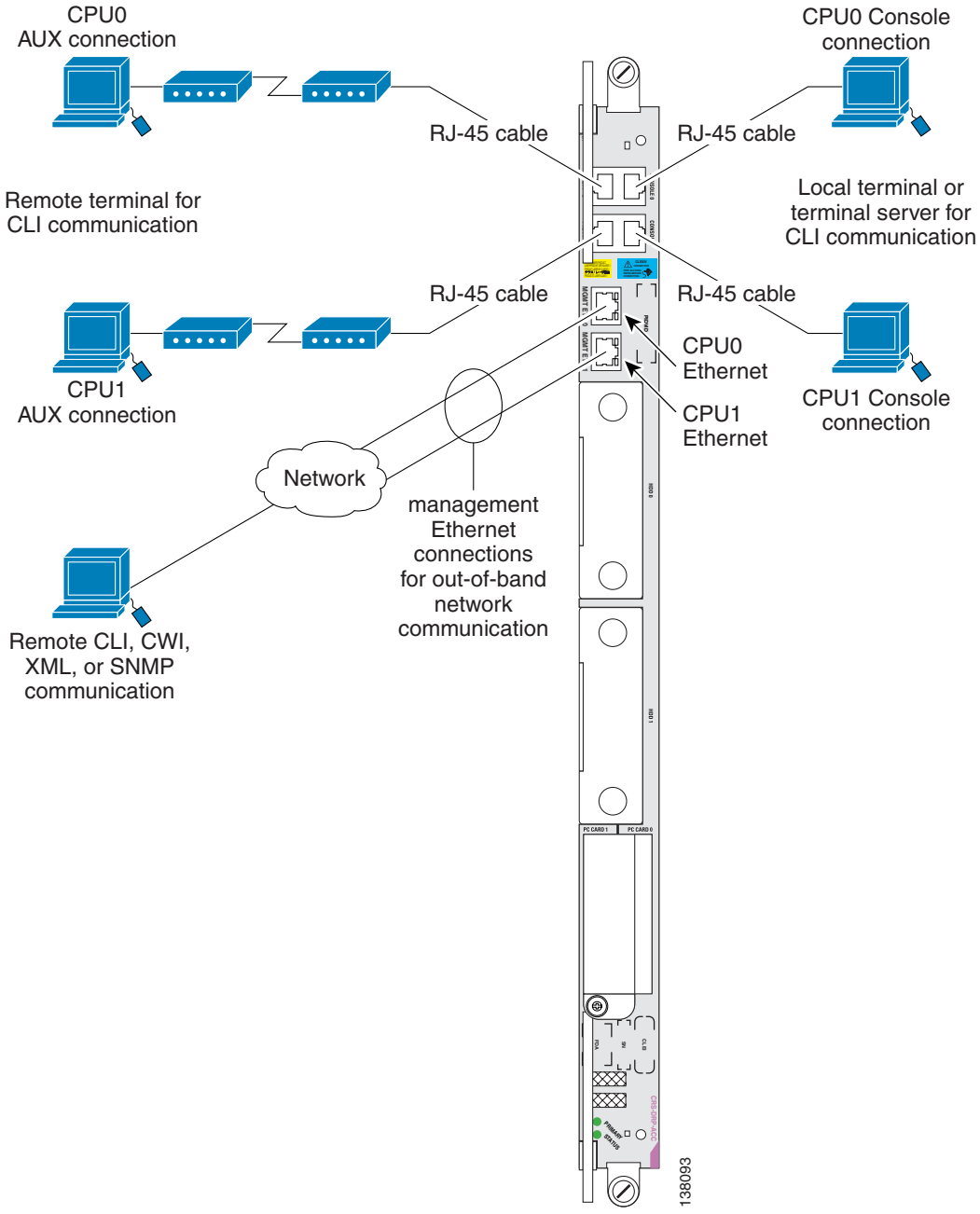


Figure 4-4 Communication Ports on the PRP-1 for a Cisco XR 12000 Series Router

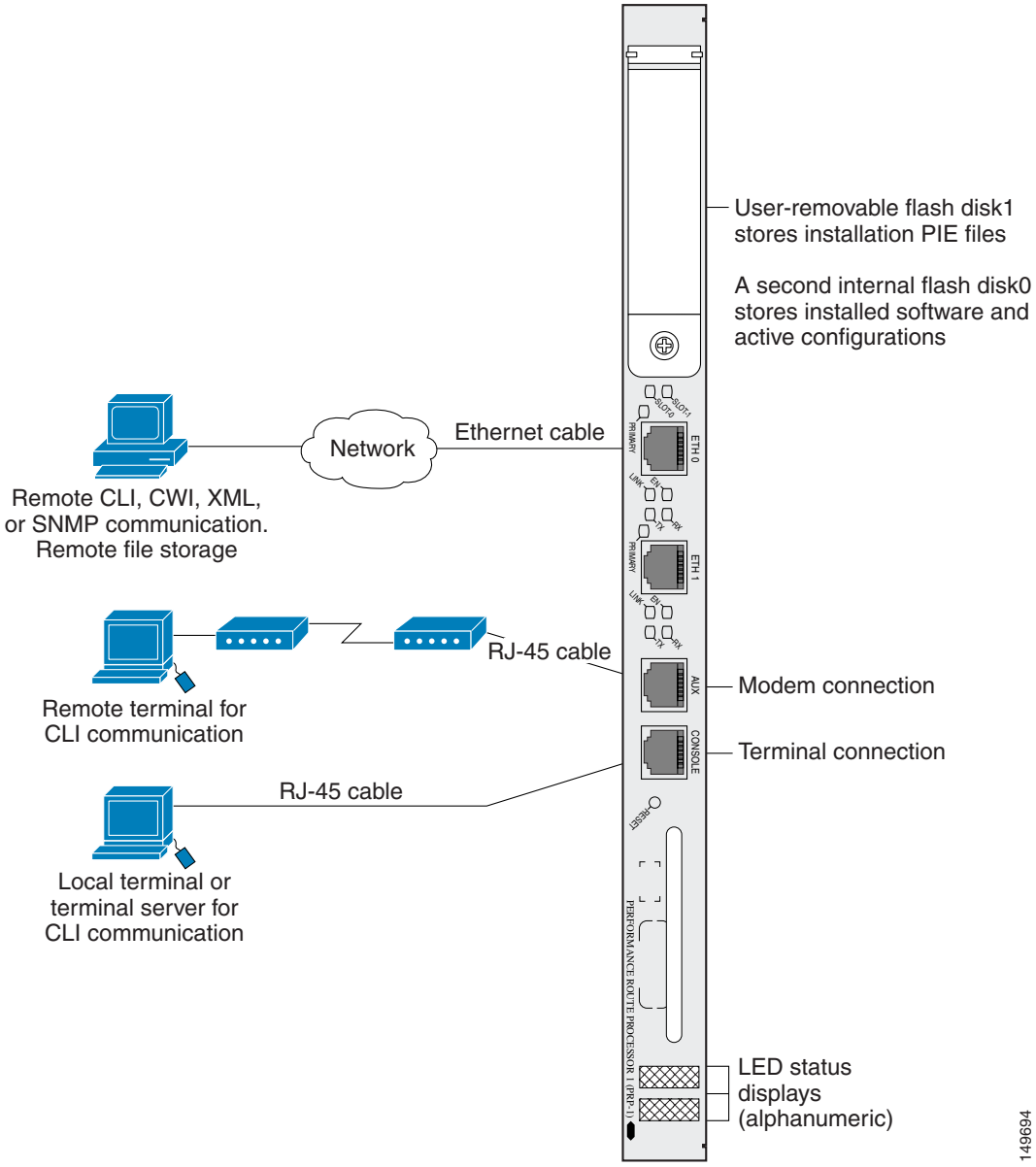
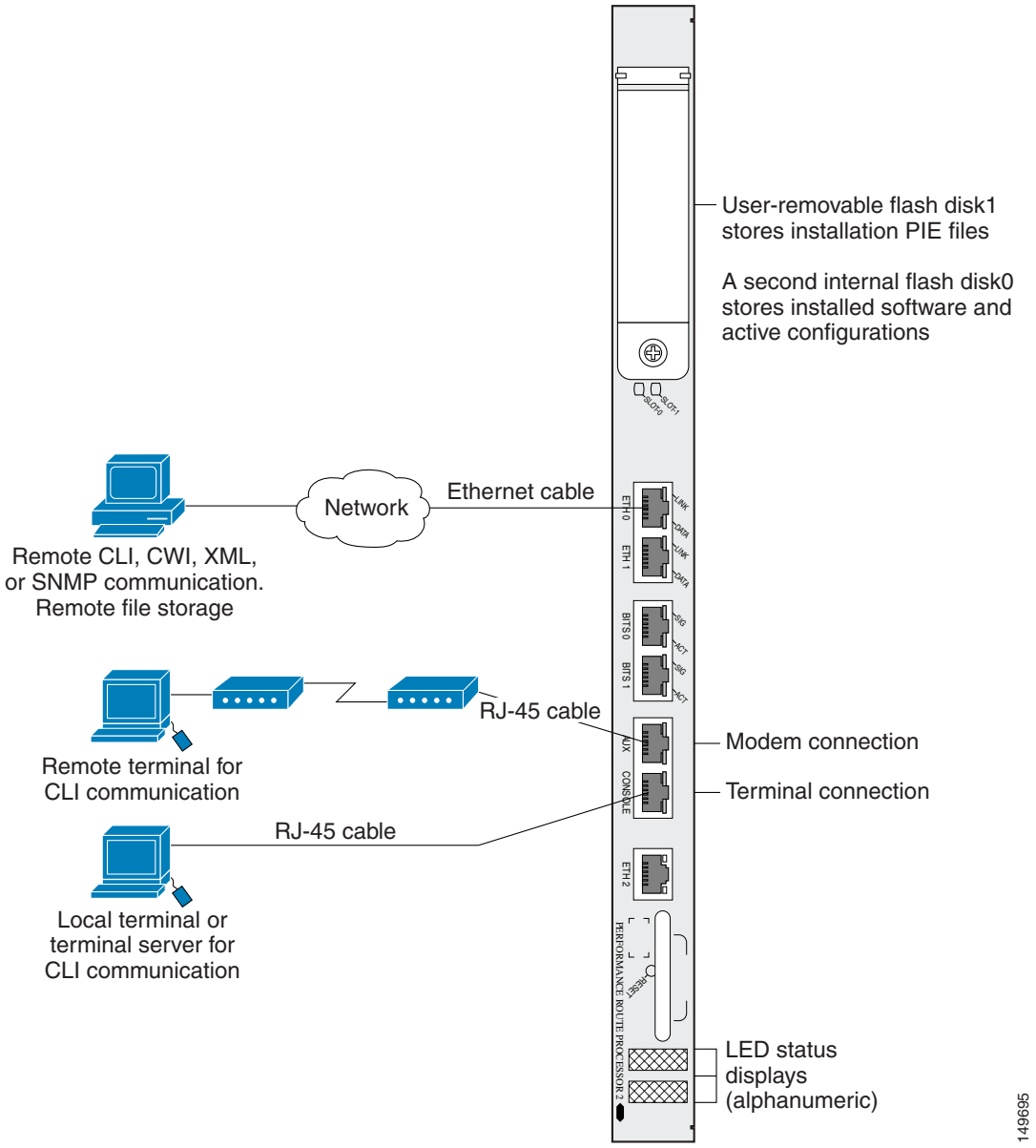


Figure 4-5 Communication Ports on the PRP-2 for a Cisco XR 12000 Series Router



The following sections describe three ways to connect to a DSC or DSDRSC:

- Establishing a Connection Through the Console Port, page 4-8
- Establishing a Connection Through a Terminal Server, page 4-9
- Establishing a Connection Through the Management Ethernet Interface, page 4-11

Establishing a Connection Through the Console Port

To connect to the router through the console port, perform the following procedure.

SUMMARY STEPS

1. Identify the active RP or DRP.
2. Connect a terminal to the Console port of the active RP or DRP.
3. Start the terminal emulation program.
4. Press **Enter**.
5. Log in to the router.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Identify the active RP or DRP.	Identifies the RP or DRP to which you must connect in the next step. • This step is not required when the router hosts only one RP. • On a Cisco CRS-1 router, the active RP or DRP is identified by a lighted Primary LED on the RP front panel. • On a Cisco XR 12000 Series Router, the active RP is identified by the alphanumeric display: ACTV RP.
Step 2	Connect a terminal to the Console port of the active RP or DRP.	Establishes a communications path to the router. • During the initial setup, you can communicate with the router only through the Console port of the active RP. • The router Console port is designed for a serial cable connection to a terminal or a computer that is running a terminal emulation program. • The terminal settings are: – Bits per second: 9600/9600 – Data bits: 8 – Parity: None – Stop bit: 2 – Flow control: None • For information on the cable requirements for the Console port, see the hardware documentation listed in the "Related Documents" section on page x.

	Command or Action	Purpose
Step 3	Start the terminal emulation program.	(Optional) Prepares a computer for router communications. • The step is not required if you are connecting through a terminal. • Terminals send keystrokes to and receive characters from another device. If you connect a computer to the Console port, you must use a terminal emulation program to communicate with the router. For instructions on using the terminal emulation program, see the documentation for that program.
Step 4	Press **Enter**.	Initiates communication with the router. • If no text or router prompt appears when you connect to the Console port, press **Enter** to initiate communications. • If no text appears when you press **Enter** and the router has been started recently, give the router more time to complete the initial boot procedure, then press **Enter**. • If the router has no configuration, the router displays the prompt: `Enter root-system username:`. If a standalone router is starting up for the first time, see Chapter 2, "Bringing Up the Cisco IOS XR Software on a Standalone Router." If a multishelf system is starting up for the first time, see Chapter 3, "Bringing Up the Cisco IOS XR Software on a Multishelf System." • If the router has been configured, the router displays the prompt: `Username:`
Step 5	Log in to the router.	Establishes your access rights for the router management session. • Enter your username and password, as described in the "Logging In to a Router or an SDR" section on page 4-12. • After you log in, the router displays the CLI prompt, which is described in the "CLI Prompt" section on page 4-13.

Establishing a Connection Through a Terminal Server

A terminal server connection provides a way to access the Console port from a remote location. It is less expensive to connect to the router through the Management Ethernet interface (because you do not have the additional cost of a terminal server). However, if you need to perform tasks that require Console port access from a remote location, a terminal server is the best connection method.

The procedure for connecting to the router through a terminal server is similar to the procedure for directly connecting through the Console port. For both connection types, the physical connection takes place through the Console port. The difference is that the terminal server connects directly to the Console port, and you must use a Telnet session to establish communications through the terminal server to the router.

To establish a connection through a terminal server, perform the following procedure:

SUMMARY STEPS

1. Install and configure the terminal server.
2. Connect the terminal server to the Console port of the target RP or DRP.
3. Power on the router.
4. Identify the target RP or DRP.
5. **telnet** *access-server-address port*
6. Press **Enter**.
7. Log in to the router.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Install and configure the terminal server.	Prepares the terminal server for communications with the router and with Telnet clients. • This step is usually preformed once. • For router access, users need the Telnet server IP address and port number for each RP they access. • For additional information on configuring terminal services, including terminal servers and templates, see the *Cisco IOS XR System Management Configuration Guide*.
Step 2	Connect the terminal server to the Console port of the target RP or DRP.	Establishes a communications path between the terminal server and the router. • During the initial router setup, you can communicate with the router only through the Console port of the primary RP. • The router Console port is designed for a serial cable connection to a terminal or terminal server. • The terminal settings are: – Bits per second: 9600/9600 – Data bits: 8 – Parity: None – Stop bit: 2 – Flow control: None • For information on the cable requirements for the Console port, see the hardware documentation listed in the "Related Documents" section on page x. • To enable terminal server connections to the Console ports on multiple RPs and DRPs, install a cable between each Console port and the terminal server.

	Command or Action	Purpose
Step 3	Power on the router.	Starts the router. • This step is required only if the router power is not on. • For information on power installation and controls, see the hardware documentation listed in the "Related Documents" section on page x.
Step 4	Identify the target RP or DRP.	Identifies the RP or DRP to which you connect in the next step. • This step is not required when the router hosts only one RP or DRP. • On a Cisco CRS-1 router, the active RP or DRP is identified by a lighted Primary LED on the RP front panel. • On a Cisco XR 12000 Series Router, the active RP is identified by the alphanumeric display: ACTV RP. • If you cannot look at the RPs, use a Management Ethernet interface connection to determine which RP is active, or establish terminal server connections to both RPs and then try both.
Step 5	**telnet** *access-server-address port*	Establishes a Telnet session with the terminal server. • Replace *access-server-address* with the IP address of the terminal server, and replace *port* with the terminal server port number that connects to the target RP Console port.
Step 6	Press **Enter**.	(Optional) Initiates communications with the RP or DRP. • If no text or router prompt appears when you start the Telnet session, press **Enter** to initiate communications. • If the router has no configuration, the router displays the prompt: `Enter root-system username:` Enter the root-system username and password when prompted. • If the router has been configured, the router displays the prompt: `Username:`
Step 7	Log in to the router.	Establishes your access rights for the router management session. • Enter a username and password when prompted.

Establishing a Connection Through the Management Ethernet Interface

The Management Ethernet interface allows you to manage the router using a network connection. Before you can use the Management Ethernet interface, the interface must be configured, as described in the "Configuring the Management Ethernet Interface" section on page 4-42.

Once configured, the network connection takes place between client software on a workstation computer and a server process within the router. The type of client software you use depends on the server process you want to use. The Cisco IOS XR software supports the following client and server services:

- Telnet clients can connect to a Telnet server in the router. The Telnet server is disabled by default and can be enabled with the **telnet ipv4 server** or **telnet ipv6 server** command in global configuration mode.
- Secure Shell (SSH) clients can connect to an SSH server in the router. The SSH server is disabled by default and can be enabled with the **ssh server** command in global configuration mode. The SSH server handles both Secure Shell Version 1 (SSHv1) and SSHv2 incoming client connections for both IPv4 and IPv6 address families.

To start a Telnet network connection, you start the Telnet client software with a command similar to the following:

telnet *ManagementEthernetInterfaceIPaddress*

For specific instructions on connecting to the router through a Telnet or SSH client, see the instructions for that software.

Ask your system administrator for the IP address of the Management Ethernet interface.

When the Telnet session is established, the router prompts you to log in, as described in the "Logging In to a Router or an SDR" section on page 4-12.

Logging In to a Router or an SDR

The login process can require users to enter a password or a username and password before accessing the router CLI. The user groups to which your username is assigned determine which commands you can use.

If you log in to a router with a single SDR configured (this is the default configuration), you can manage the entire router. If you log in to the owner SDR on a system with multiple SDRs, you can manage general features that apply to the entire system and the interfaces assigned to the owner SDR. If you log in to a named SDR, you can manage only that SDR. For more information on SDRs, see the "Secure Domain Routers" section on page 4-1.

When you log in, the username and password may be validated by any of the following services:

- Usernames configured on the router (**username** command in global configuration mode)
- Root-system usernames configured on the owner SDR
- Passwords configured for the router console and auxiliary ports (**password** or **secret** command in line configuration mode)
- A RADIUS server
- A TACACS+ server

The username and password validation method that your router uses is determined by the router configuration. For information on configuring username and password validation methods, see the *Cisco IOS XR System Security Configuration Guide*. For information on which username and password to use, see your system administrator.

To log in to the router, enter your username and password when prompted. For example:

```
User Access Verification

Username: iosxr
Password: password
RP/0/RP0/CPU0:router#
```

Note Passwords are case sensitive. If you want to log in to an SDR using a root-system username from the owner SDR, enter the username in the following format: *username*@admin. To support admin login, local database authentication must be enabled with the **aaa authentication login remote local** command. For more information, see *Cisco IOS XR System Security Configuration Guide*.

After you log in, the router displays the CLI prompt, which is described in the "CLI Prompt" section on page 4-13. The command set that you can use is determined by the privileges assigned to your username. For information on how privileges are assigned to usernames, see the *Cisco IOS XR System Security Configuration Guide*.

CLI Prompt

After you log in, you see the CLI prompt for the Cisco IOS XR software. This prompt identifies the router or SDR to which you are issuing commands. The CLI prompt represents the path, through the router, to the CPU that executes the commands you enter. The syntax for the CLI prompt is: *type*/*rack*/*slot*/*module*: *router-name*#. The CLI prompt is described in Table 4-1.

Table 4-1 CLI Prompt Description

Prompt Syntax Components	Description
type	Type of interface or card with which you are communicating. For most user communication tasks, the type is "RP."
rack	Rack number. In a standalone router, the rack number is always "0." In a multishelf system, the range for LCC rack numbers is 0 to 255, and the range for FCC rack numbers is F0 to F7.
slot	Slot in which the RP or DRP is installed. In a Cisco CRS-1 router, the RP physical slot number is "RP0" or "RP1." In a Cisco XR 12000 Series Router, the physical slot number can be 0 to 15, and there can be multiple SDRs, each of which is represented by an RP.
module	Entity on a card that executes user commands or communicates with a port (interface). For executing commands from the EXEC prompt, the module is the "CPU0" of the RP. "CPU0" also controls the forwarding and operating system (OS) functions for the system. DRPs have two processors: CPU0 and CPU1.
router-name	Hostname of the router or SDR. The hostname is usually defined during initial configuration of the router, as described in the "Configuring the SDR Hostname" section on page 4-39.

For example, the following prompt indicates that the CLI commands are executed on the RP in rack 0, slot RP0, by the "CPU0" module on a router named "router:"

```
RP/0/RP0/CPU0:router#
```

User Access Privileges

When you log in to the router, your username and password are used to determine if you are authorized to access the router. After you successfully log in, your username is used to determine which commands you are allowed to use. The following sections provide information on how the router determines which commands you can use:

- User Groups, Task Groups, and Task IDs, page 4-14
- Predefined User Groups, page 4-15
- Displaying the User Groups and Task IDs for Your User Account, page 4-16

User Groups, Task Groups, and Task IDs

The commands that each user can use are defined by the user groups to which he or she belongs. Within the Cisco IOS XR software, the commands for a particular feature, such as access control lists, are assigned to tasks, which are uniquely identified by task IDs. If a user wants to use a particular command, his or her username must be associated with the appropriate task ID.

The association between a username and a task ID takes place through two intermediate entities, the user group and task group.

The user group is basically a logical container that can be used to assign the same task IDs to multiple users. Instead of assigning task IDs to each user, you can assign them to the user group, and then assign users to the user group. When a task is assigned to a user group, you can define the access rights for the commands associated with that task. These rights include "read," "write," "execute," and "notify."

The task group is also a logical container, but it is used to group tasks. Instead of assigning task IDs to each user group, you assign them to a task group, which allows you to quickly enable access to a specific set of tasks by assigning a task group to a user group.

To summarize the associations, usernames are assigned to user groups, which are then assigned to task groups. Users can be assigned to multiple user groups, and each user group can be assigned to one or more task groups. The commands that a user can execute are all those commands assigned to the tasks within the task groups that are associated with the user groups to which the user belongs.

Users are not assigned to groups by default and must be explicitly assigned by an administrator.

You can display all task IDs available on the system with the **show task supported** command. For example:

```
RP/0/RP0/CPU0:router# show task supported
bgp
ospf
hsrp
isis
route-map
route-policy
static
vrrp
cef
lpts
iep
```

```
rib
multicast
mpls-te
mpls-ldp
mpls-static
ouni
fabric
bundle
network
transport
ppp
hdlc
 --More--
```

Note Only the root-system users, root-lr users, or users associated with the WRITE:AAA task ID can configure task groups. (The root-lr user has the highest level of privileges in an SDR. In previous releases, SDRs were called logical routers (LRs).)

Predefined User Groups

The Cisco IOS XR software includes a set of predefined user groups that meets the needs of most organizations. The predefined user groups are described in Table 4-2.

Table 4-2 Predefined User Group Descriptions

User Group	Privileges
root-system	Display and execute all commands for all SDRs in the system.
root-lr	Display and execute all commands within a single SDR.
sysadmin	Perform system administration tasks for the router, such as maintaining where the core dumps are stored or setting up the Network Time Protocol (NTP) clock.
netadmin	Configure network protocols, such as Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF) (usually used by network administrators).
operator	Perform day-to-day monitoring activities, and have limited configuration rights.
cisco-support	Debug and troubleshoot features (usually used by Cisco support personnel).

Although the predefined user groups are sufficient for the needs of most organizations, administrators can configure their own groups. For more information, see *Cisco IOS XR System Security Configuration.*

Displaying the User Groups and Task IDs for Your User Account

To display the user groups and task IDs associated with your account, enter the **show user** command in EXEC mode. Table 4-3 summarizes the options available for this command.

Table 4-3 Options to Display Information About Your Account

Command	Description
show user	Displays your user name.
show user group	Displays the user groups assigned to your account.
show user tasks	Displays the task IDs assigned to your account.
show user all	Displays all user groups and task ID information for your account.
show aaa usergroup *group-name*	Displays the task IDs assigned to a user group.

Examples

To display your username, enter the **show user** command:

```
RP/0/RP0/CPU0:CRS-8_P1# show user

cisco
```

To display the tasks assigned to your account and your rights to those tasks, enter the **show user tasks** command:

```
RP/0/RP0/CPU0:CRS-8_P1# show user tasks

Task:                  aaa  : READ    WRITE    EXECUTE    DEBUG
Task:                  acl  : READ    WRITE    EXECUTE    DEBUG
Task:                admin  : READ    WRITE    EXECUTE    DEBUG
Task:                  atm  : READ    WRITE    EXECUTE    DEBUG
Task:       basic-services  : READ    WRITE    EXECUTE    DEBUG
Task:                 bcdl  : READ    WRITE    EXECUTE    DEBUG
Task:                  bfd  : READ    WRITE    EXECUTE    DEBUG
Task:                  bgp  : READ    WRITE    EXECUTE    DEBUG
Task:                 boot  : READ    WRITE    EXECUTE    DEBUG
Task:               bundle  : READ    WRITE    EXECUTE    DEBUG
Task:                  cdp  : READ    WRITE    EXECUTE    DEBUG
Task:                  cef  : READ    WRITE    EXECUTE    DEBUG
Task:          config-mgmt  : READ    WRITE    EXECUTE    DEBUG
Task:      config-services  : READ    WRITE    EXECUTE    DEBUG
Task:               crypto  : READ    WRITE    EXECUTE    DEBUG
Task:                 diag  : READ    WRITE    EXECUTE    DEBUG
Task:              drivers  : READ    WRITE    EXECUTE    DEBUG
Task:                eigrp  : READ    WRITE    EXECUTE    DEBUG
Task:           ext-access  : READ    WRITE    EXECUTE    DEBUG
Task:               fabric  : READ    WRITE    EXECUTE    DEBUG
Task:            fault-mgr  : READ    WRITE    EXECUTE    DEBUG
Task:           filesystem  : READ    WRITE    EXECUTE    DEBUG
Task:             firewall  : READ    WRITE    EXECUTE    DEBUG
Task:                   fr  : READ    WRITE    EXECUTE    DEBUG
Task:                 hdlc  : READ    WRITE    EXECUTE    DEBUG
Task:        host-services  : READ    WRITE    EXECUTE    DEBUG
Task:                 hsrp  : READ    WRITE    EXECUTE    DEBUG
Task:            interface  : READ    WRITE    EXECUTE    DEBUG
Task:            inventory  : READ    WRITE    EXECUTE    DEBUG
```

```
Task:          ip-services  : READ    WRITE    EXECUTE    DEBUG
Task:                 ipv4  : READ    WRITE    EXECUTE    DEBUG
Task:                 ipv6  : READ    WRITE    EXECUTE    DEBUG
Task:                 isis  : READ    WRITE    EXECUTE    DEBUG
Task:              logging  : READ    WRITE    EXECUTE    DEBUG
Task:                 lpts  : READ    WRITE    EXECUTE    DEBUG
Task:              monitor  : READ    WRITE    EXECUTE    DEBUG
Task:             mpls-ldp  : READ    WRITE    EXECUTE    DEBUG
Task:          mpls-static  : READ    WRITE    EXECUTE    DEBUG
Task:              mpls-te  : READ    WRITE    EXECUTE    DEBUG
Task:            multicast  : READ    WRITE    EXECUTE    DEBUG
Task:              netflow  : READ    WRITE    EXECUTE    DEBUG
Task:              network  : READ    WRITE    EXECUTE    DEBUG
Task:                 ospf  : READ    WRITE    EXECUTE    DEBUG
Task:                 ouni  : READ    WRITE    EXECUTE    DEBUG
Task:              pkg-mgmt  : READ    WRITE    EXECUTE    DEBUG
Task:              pos-dpt  : READ    WRITE    EXECUTE    DEBUG
Task:                  ppp  : READ    WRITE    EXECUTE    DEBUG
Task:                  qos  : READ    WRITE    EXECUTE    DEBUG
Task:                  rib  : READ    WRITE    EXECUTE    DEBUG
Task:                  rip  : READ    WRITE    EXECUTE    DEBUG
Task:              root-lr  : READ    WRITE    EXECUTE    DEBUG (reserved)
Task:          root-system  : READ    WRITE    EXECUTE    DEBUG (reserved)
Task:            route-map  : READ    WRITE    EXECUTE    DEBUG
Task:         route-policy  : READ    WRITE    EXECUTE    DEBUG
Task:                  sbc  : READ    WRITE    EXECUTE    DEBUG
Task:                 snmp  : READ    WRITE    EXECUTE    DEBUG
Task:            sonet-sdh  : READ    WRITE    EXECUTE    DEBUG
Task:               static  : READ    WRITE    EXECUTE    DEBUG
Task:               sysmgr  : READ    WRITE    EXECUTE    DEBUG
Task:               system  : READ    WRITE    EXECUTE    DEBUG
Task:            transport  : READ    WRITE    EXECUTE    DEBUG
Task:           tty-access  : READ    WRITE    EXECUTE    DEBUG
Task:               tunnel  : READ    WRITE    EXECUTE    DEBUG
Task:            universal  : READ    WRITE    EXECUTE    DEBUG (reserved)
Task:                 vlan  : READ    WRITE    EXECUTE    DEBUG
Task:                 vrrp  : READ    WRITE    EXECUTE    DEBUG
```

To display the user groups assigned to your user account, enter the **show user group** command:

```
RP/0/RP0/CPU0:CRS-8_P1# show user group

root-system
```

To display the rights assigned to a user group, enter the **show aaa usergroup** *group-name* command*:*

```
RP/0/RP0/CPU0:CRS-8_P1# show aaa usergroup root-system

User group 'root-system'
  Inherits from task group 'root-system'

User group 'root-system' has the following combined set
  of task IDs (including all inherited groups):
Task:                 aaa  : READ    WRITE    EXECUTE    DEBUG
Task:                 acl  : READ    WRITE    EXECUTE    DEBUG
Task:               admin  : READ    WRITE    EXECUTE    DEBUG
Task:                 atm  : READ    WRITE    EXECUTE    DEBUG
Task:       basic-services  : READ    WRITE    EXECUTE    DEBUG
Task:                bcdl  : READ    WRITE    EXECUTE    DEBUG
Task:                 bfd  : READ    WRITE    EXECUTE    DEBUG
Task:                 bgp  : READ    WRITE    EXECUTE    DEBUG
Task:                boot  : READ    WRITE    EXECUTE    DEBUG
Task:              bundle  : READ    WRITE    EXECUTE    DEBUG
Task:                 cdp  : READ    WRITE    EXECUTE    DEBUG
```

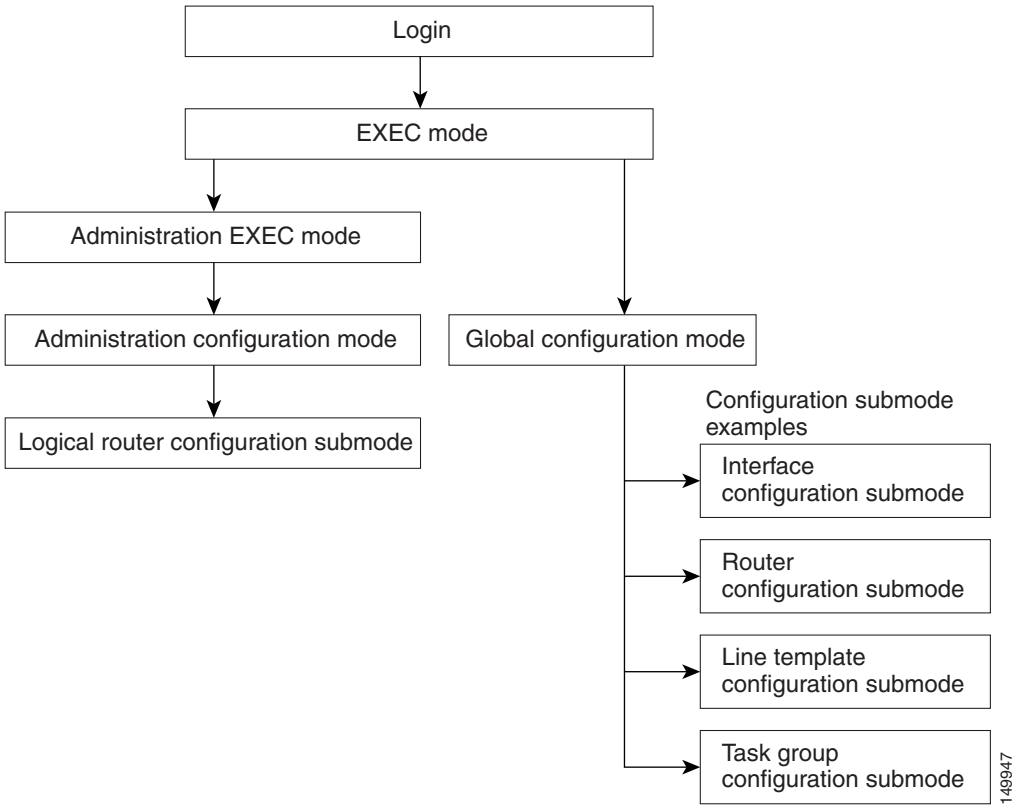
```
Task:                 cef  : READ    WRITE    EXECUTE    DEBUG
Task:          config-mgmt  : READ    WRITE    EXECUTE    DEBUG
Task:      config-services  : READ    WRITE    EXECUTE    DEBUG
Task:              crypto   : READ    WRITE    EXECUTE    DEBUG
Task:                diag   : READ    WRITE    EXECUTE    DEBUG
Task:             drivers   : READ    WRITE    EXECUTE    DEBUG
Task:               eigrp   : READ    WRITE    EXECUTE    DEBUG
Task:          ext-access   : READ    WRITE    EXECUTE    DEBUG
Task:              fabric   : READ    WRITE    EXECUTE    DEBUG
Task:           fault-mgr   : READ    WRITE    EXECUTE    DEBUG
Task:          filesystem   : READ    WRITE    EXECUTE    DEBUG
Task:            firewall   : READ    WRITE    EXECUTE    DEBUG
Task:                  fr   : READ    WRITE    EXECUTE    DEBUG
Task:                hdlc   : READ    WRITE    EXECUTE    DEBUG
Task:        host-services  : READ    WRITE    EXECUTE    DEBUG
Task:                hsrp   : READ    WRITE    EXECUTE    DEBUG
Task:           interface   : READ    WRITE    EXECUTE    DEBUG
Task:           inventory   : READ    WRITE    EXECUTE    DEBUG
Task:          ip-services  : READ    WRITE    EXECUTE    DEBUG
Task:                ipv4   : READ    WRITE    EXECUTE    DEBUG
Task:                ipv6   : READ    WRITE    EXECUTE    DEBUG
Task:                isis   : READ    WRITE    EXECUTE    DEBUG
Task:             logging   : READ    WRITE    EXECUTE    DEBUG
Task:                lpts   : READ    WRITE    EXECUTE    DEBUG
Task:             monitor   : READ    WRITE    EXECUTE    DEBUG
Task:            mpls-ldp   : READ    WRITE    EXECUTE    DEBUG
Task:         mpls-static   : READ    WRITE    EXECUTE    DEBUG
Task:             mpls-te   : READ    WRITE    EXECUTE    DEBUG
Task:           multicast   : READ    WRITE    EXECUTE    DEBUG
Task:             netflow   : READ    WRITE    EXECUTE    DEBUG
Task:             network   : READ    WRITE    EXECUTE    DEBUG
Task:                ospf   : READ    WRITE    EXECUTE    DEBUG
Task:                ouni   : READ    WRITE    EXECUTE    DEBUG
Task:            pkg-mgmt   : READ    WRITE    EXECUTE    DEBUG
Task:             pos-dpt   : READ    WRITE    EXECUTE    DEBUG
Task:                 ppp   : READ    WRITE    EXECUTE    DEBUG
Task:                 qos   : READ    WRITE    EXECUTE    DEBUG
Task:                 rib   : READ    WRITE    EXECUTE    DEBUG
Task:                 rip   : READ    WRITE    EXECUTE    DEBUG
Task:             root-lr   : READ    WRITE    EXECUTE    DEBUG (reserved)
Task:         root-system   : READ    WRITE    EXECUTE    DEBUG (reserved)
Task:           route-map   : READ    WRITE    EXECUTE    DEBUG
Task:        route-policy   : READ    WRITE    EXECUTE    DEBUG
Task:                 sbc   : READ    WRITE    EXECUTE    DEBUG
Task:                snmp   : READ    WRITE    EXECUTE    DEBUG
Task:           sonet-sdh   : READ    WRITE    EXECUTE    DEBUG
Task:              static   : READ    WRITE    EXECUTE    DEBUG
Task:              sysmgr   : READ    WRITE    EXECUTE    DEBUG
Task:              system   : READ    WRITE    EXECUTE    DEBUG
Task:           transport   : READ    WRITE    EXECUTE    DEBUG
Task:          tty-access   : READ    WRITE    EXECUTE    DEBUG
Task:              tunnel   : READ    WRITE    EXECUTE    DEBUG
Task:           universal   : READ    WRITE    EXECUTE    DEBUG (reserved)
Task:                vlan   : READ    WRITE    EXECUTE    DEBUG
Task:                vrrp   : READ    WRITE    EXECUTE    DEBUG
```

Navigating the Cisco IOS XR Command Modes

The CLI for the Cisco IOS XR software is divided into different command modes. Each mode provides access to a subset of commands used to configure, monitor, and manage the router. Access to a mode is determined by your user group assignments. The following sections describe the navigation of the command modes:

Figure 4-6 illustrates the basic command mode navigation for the CLI. Only a small sample of the possible configuration submodes is shown.

Figure 4-6 Example of Command Mode Navigation in Cisco IOS XR software



Identifying the Command Mode in the CLI Prompt

The command mode is identified in the CLI prompt after the router name.

For example, when the router enters global configuration mode from the EXEC mode, the CLI prompt changes to include "(config)" after the router name:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)#
```

When the router enters interface configuration submode, the prompt changes to include "(config-if)" after the router name:

```
RP/0/RP0/CPU0:router(config)# interface POS 0/2/0/0
RP/0/RP0/CPU0:router(config-if)#
```

Summary of Common Command Modes

Table 4-4 summarizes the most common command modes of the Cisco IOS XR software and the associated CLI prompts.

Table 4-4 Common Command Modes and CLI prompts

Command Mode	Description
EXEC	Logging in to an SDR running the Cisco IOS XR software automatically places the router in EXEC mode. Example: `RP/0/RP0/CPU0:router#` EXEC mode enables a basic set of commands to display the operational state of an SDR and the Cisco IOS XR software. Most CLI commands in EXEC mode do not change the SDR operation. The most common EXEC commands are **show** commands (to display SDR configuration or operational data) and **clear** commands (to clear or reset SDR counters). In EXEC mode, you can display the configuration of an SDR but not the configuration of the system. The difference is that SDRs are defined in administration configuration mode, which is a submode of administration EXEC mode. SDRs are configured in global configuration mode. Additional commands are available depending on the access privileges (user groups) assigned to your username. Minimal privileges also include a small set of EXEC commands for connecting to remote devices, changing terminal line settings on a temporary basis, and performing basic tests.

Administration EXEC	Administration EXEC mode is used to manage system resources. In administration EXEC mode, you can display the configuration of the system but not the configuration of an SDR. The difference is that SDRs are defined in administration configuration mode, which is a submode of administration EXEC mode. SDRs are configured in global configuration mode.
	Administration EXEC mode is used primarily to display system-wide parameters, configure the administration plane over the control Ethernet, and configure SDR. These operations are available only to users with the required root level access.
	From EXEC mode, use the **admin** command to enter administration EXEC mode:
	`RP/0/RP0/CPU0:router# admin`
	`RP/0/RP0/CPU0:router(admin)#`

Table 4-4 Common Command Modes and CLI prompts (continued)

Command Mode	Description

administration configuration mode	Administration configuration mode allows you to create SDRs and assign system resources to SDRs. Multishelf systems are also configured in administration configuration mode.
	From administration EXEC mode, use the **configure** command to enter administration configuration submode:
	`RP/0/RP0/CPU0:router(admin)# configure`
	`RP/0/RP0/CPU0:router(admin-config)#`

Global configuration	Global configuration mode is the starting point for SDR configuration. Commands entered in this mode affect the SDR as a whole, rather than just one protocol or interface. Global configuration mode is also used for entering configuration submodes to configure specific elements, such as interfaces or protocols.
	To enter global configuration mode, enter the **configure** command at the EXEC command prompt:
	`RP/0/RP0/CPU0:router# configure`
	`RP/0/RP0/CPU0:router(config)#`
	Note The system prompt changes to "`router(config)`" to indicate that the router is now in global configuration mode.

Configuration submodes	From the global configuration mode, you can also enter other, more specific command modes. These modes are available based on your assigned access privileges and include protocol-specific, platform-specific, and feature-specific configuration modes.
	In the following example, MPLS LDP configuration mode is entered from global configuration mode. The prompt for MPLS LDP configuration submode appears as config-ldp. The following command syntax is used for entering configuration MPLS LDP submode:
	`RP/0/RP0/CPU0:router#`
	`RP/0/RP0/CPU0:router# configure`
	`RP/0/RP0/CPU0:router(config)# mpls ldp`
	`RP/0/RP0/CPU0:router(config-ldp)`
	Note The availability of any particular mode depends on the router features and the access rights of the individual user. For example, a configuration mode for configuring access servers is not available on most routers.

Interface configuration	The interface configuration submode is used to select and configure a hardware interface, such as a Packet-over-SONET/SDH (POS) interface. To enter interface configuration mode from global configuration mode, use an **interface** command. An interface configuration command always follows an interface global configuration command, which defines the interface type. The following command syntax is used for entering interface configuration submode:
	`RP/0/RP0/CPU0:router(config)# interface POS 0/2/0/0`
	`RP/0/RP0/CPU0:router(config-if)#`

Table 4-4 Common Command Modes and CLI prompts (continued)

Command Mode	Description

Router configuration	The router configuration submode is used to select and configure a routing protocol, such as BGP, OSPF, or IS-IS. The following command syntax is used for entering router configuration submode:
	`RP/0/RP0/CPU0:router(config)# router <protocol> <protocol_options>`
	Replace *protocol* with the keyword for the protocol you want to configure. Replace *protocol_options* with any keywords and arguments required for that protocol. In the following example, the router enters the router configuration mode for BGP:
	`RP/0/RP0/CPU0:router# configure`
	`RP/0/RP0/CPU0:router(config)# router bgp 140`
	`RP/0/RP0/CPU0:router(config-bgp)#`

Router submode configuration	Router configuration submodes are accessed from router configuration mode. The following command syntax is used for entering router address family configuration submode:
	`RP/0/RP0/CPU0:router(config)# router bgp 140`
	`RP/0/RP0/CPU0:router(config-bgp)# address-family ipv4 multicast`
	`RP/0/RP0/CPU0:router(config-bgp-af)#`
	For more information, see the following Cisco Systems documents:
	• *Cisco IOS XR Routing Configuration Guide*
	• *Cisco IOS XR Routing Command Reference*

ROM Monitor (ROMMON) mode	The ROM Monitor is a bootstrap program that initializes the hardware and boots the system when a router is powered on or reset. ROM Monitor mode is also known as “ROMMON,” which reflects the CLI prompt for the mode. `rommon B1>` During normal operation, users do not interact with ROMMON. This mode is accessed only by manually interrupting the boot process and placing the system in ROMMON. Once in ROMMON, you can perform ROM Monitor tasks, including reinstallation of the Cisco IOS XR software, password recovery, and other diagnostic tasks. The ROM Monitor CLI mode is accessible only from a terminal connected directly to the Console port of the primary RP, a terminal-modem connection to the AUX port, or through a terminal server. See *Cisco IOS XR ROM Monitor Guide* for information and instructions on using ROM Monitor mode.

Entering EXEC Commands from a Configuration Mode

EXEC commands can be executed from any configuration mode by preceding the command with the **do** keyword. Executing EXEC commands from a configuration mode allows you to display the state of the system without exiting the configuration mode. For example:

```
RP/0/RP0/CPU0:router(config)# do show version

Cisco IOS-XR Software, Version 1.0.0
Copyright (c) 2004 by cisco Systems, Inc.

ROM: System Bootstrap, Version 1.15(20040120:002852) [ROMMON],

router uptime is 1 hour, 40 minutes
1000592k bytes of ATA PCMCIA card at disk 0 (Sector size 512 bytes).
```

```
Configuration register is 0x2

--More--
```

Command Mode Navigation Example

The following steps provide an example of command mode navigation:

Step 1 Start a session by logging in to the router and entering EXEC mode, as shown in the following example:

```
router con0_RP0_CPU0 is now available


Press RETURN to get started.


User Access Verification

Username: iosxr
Password:<secret>
RP/0/RP0/CPU0:router#
```

From EXEC mode you can issue EXEC commands or enter global configuration mode. Examples of EXEC commands are the **show** commands used to display system status and **clear** commands to clear counters or interfaces.

Step 2 Enter a question mark at the end of the prompt, or after a command, to display the available options:

```
RP/0/RP0/CPU0:router# show ?

  aaa                   Show AAA configuration and operational data
  adjacency             Adjacency information
  aliases               Display alias commands
  aps                   SONET APS information
  arm                   IP ARM information
  arp                   ARP table
  as-path-access-list   List AS path access lists
  asic-errors           ASIC error information
  auto-rp               Auto-RP Commands
  bgp                   BGP show commands
  buffer-manager        Show all buffer manager memory related information
  calendar              Display the system calendar
  cdp                   CDP information
  cef                   Cisco Express Forwarding
  cetftp                CRS-1 control plane ethernet TFTP server
  checkpoint            Show checkpoint services
  cinetd                Cisco inetd services
  clns                  Display CLNS related information
  clock                 Display the system clock
  commit                Show commit information
  community-list        List community-list
  configuration         Contents of Non-Volatile memory
--More--
```

Note The commands available to you depend on the router mode and your user group assignments.

Step 3 If you belong to a user group that has configuration privileges, you can place the router in the global configuration mode by entering the **configure** command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)#
```

Step 4 From global configuration mode, you can place the router in a configuration submode, such as interface configuration mode or a protocol-specific configuration mode.

In the following example, the router enters interface configuration mode and the user selects a POS interface for configuration. The command syntax is **interface** *type rack/slot/module/port*.

```
RP/0/RP0/CPU0:router(config)# interface POS 0/2/0/4
RP/0/RP0/CPU0:router(config-if)#
```

The command mode prompt changes from "`(config)`" to "`(config-if)`" and you can now enter configuration commands for the specified interface.

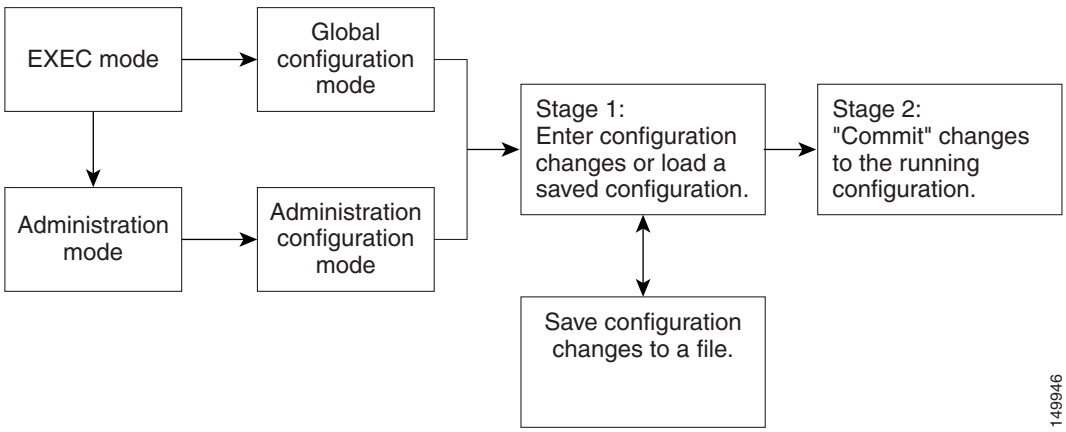
Step 5 To exit interface configuration mode and return to global configuration mode, enter the **exit** command. To return to EXEC mode, enter the **end** command.

Managing Configuration Sessions

In the Cisco IOS XR software, the running (active) configuration can never be altered directly. All configuration changes are entered into an inactive target configuration. When the target configuration is ready for use, you can apply that configuration to the router with the **commit** command. This two-stage process allows configuration changes to be made, edited, and verified before the actual running state of the router is impacted.

Figure 4-7 illustrates the two-stage configuration process.

Figure 4-7 Two-Stage Configuration Process



Global configuration mode is used to configure SDR features, such as routing protocols and interfaces. Administration configuration mode is used to assign hardware components to SDRs and to configure multishelf systems.

The following sections describe the management options for configuration sessions:

- Displaying the Active Configuration Sessions, page 4-25

Displaying the Active Configuration Sessions

Before you start a configuration session, you might want to check to see if there are other configuration sessions in progress. More than one user can open a target configuration session at a time, allowing multiple users to work on separate target configurations.

The procedure for viewing the active configuration sessions depends on the type of configuration session. For administration configuration sessions, which assign hardware components in SDRs and multishelf systems, you must be in administration EXEC mode to view the active administration configuration sessions. For SDR configuration sessions, you must be in EXEC mode to view the active SDR configuration sessions.

To view the active administration configuration sessions, connect to the DSC and enter the **show configuration sessions** command in administration EXEC mode, as shown in the following example:

```
RP/0/RP0/CPU0:CRS-8_P1# admin
RP/0/RP0/CPU0:CRS-8_P1(admin)# show configuration sessions

Session                   Line        User      Date                      Lock
00000201-002180dd-00000000  vty0        cisco     Thu Mar 16 14:47:08 2006
```

To view the active SDR configuration sessions, connect to the appropriate SDR and enter the **show configuration sessions** command in EXEC mode, as shown in the following example:

```
RP/0/RP0/CPU0:router# show configuration sessions

Session                   Line        User      Date                      Lock
00000201-002180dd-00000000  vty0        test      Thu Mar 16 13:16:17 2006
00000201-001b307a-00000000  vty2        cisco     Thu Mar 16 13:16:17 2006  *
```

If an asterisk (*) appears in the Lock column, the user is using an exclusive configuration session and you cannot start a configuration session until the exclusive configuration session is closed. For more information, see the "Starting an Exclusive Configuration Session" section on page 4-27.

Note Configuration sessions for the administration configuration and each SDR are managed independently. For example, if a user locks the administration configuration, you can still configure an SDR if other users have not locked a configuration session for that SDR.

Starting a Configuration Session

When you place the router in global configuration mode or administration configuration mode using the **configure** command, a new target configuration session is created. The target configuration allows you to enter, review, and verify configuration changes without impacting the running configuration.

Note The target configuration is not a copy of the running configuration; the target configuration contains only the configuration commands entered during the target configuration session.

While in configuration mode, you can enter all Cisco IOS XR software commands that are supported in that configuration mode. Each command is added to the target configuration. You can view the target configuration by entering the **show configuration** command in configuration mode. The target configuration is not applied until you enter the **commit** command, as described in the "Committing Changes to the Running Configuration" section on page 4-35.

Target configurations can be saved to disk as nonactive configuration files. These saved files can be loaded, further modified, and committed at a later time. For more information, see the "Saving the Target Configuration to a File" section on page 4-33.

Examples

This example shows a simple owner SDR configuration session in which the target configuration is created and previewed in global configuration mode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/2/0/1
RP/0/RP0/CPU0:router(config-if)# description faq
RP/0/RP0/CPU0:router(config-if)# ipv4 address 10.10.10.10 255.0.0.0
RP/0/RP0/CPU0:router(config-if)# show configuration

Building configuration...
interface POS0/0/0/1
 description faq
 ipv4 address 10.10.10.10 255.0.0.0
end
```

The following example shows a simple administration configuration session in which the target configuration is created and previewed in administration configuration mode:

```
RP/0/RP0/CPU0:CRS-8_P1# admin
RP/0/RP0/CPU0:CRS-8_P1(admin)# configure
RP/0/RP0/CPU0:CRS-8_P1(admin-config)# sdr test
RP/0/RP0/CPU0:CRS-8_P1(admin-config-sdr:test)# location 0/1/SP
RP/0/RP0/CPU0:CRS-8_P1(admin-config-sdr:test)# show configuration

Building configuration...
sdr test
 location 0/1/SP
!
end
```

Starting an Exclusive Configuration Session

An exclusive configuration session allows you to configure the administration configuration or an SDR and lock out all users from committing configuration changes until you are done. Other users can still create and modify a target configuration, but they cannot commit those changes to the running configuration until you exit your exclusive configuration session.

During regular configuration sessions, the running configuration is locked whenever a commit operation is being performed. This automatic locking ensures that each commit operation is completed before the next one begins. Other users receive an error message if they attempt to commit a target configuration while another commit operation is under way.

To start an exclusive configuration session for an SDR, connect to that SDR and enter the **configure exclusive** command:

```
RP/0/RP0/CPU0:router# configure exclusive
RP/0/RP0/CPU0:router(config)#
```

Note If the configuration is already locked by another user, the **configure exclusive** command fails. To display locked and unlocked configuration sessions, see the "Displaying the Active Configuration Sessions" section on page 4-25.

To start an exclusive configuration session for the administration configuration, connect to the DSC and enter the **configure exclusive** command in administration EXEC mode:

```
RP/0/RP0/CPU0:router# admin
RP/0/RP0/CPU0:router(admin)# configure exclusive
RP/0/RP0/CPU0:router(admin-config)#
```

The running configuration is unlocked when the user who started the exclusive configuration session exits the configuration mode, as described in the "Ending a Configuration Session" section on page 4-38.

Displaying Configuration Details with show Commands

The following sections describe the following tasks:

Displaying the Running Configuration

The running configuration is the committed configuration that defines the router operations, and it is divided into the administration configuration and an SDR configuration for each SDR. The portion of the running configuration that you can view depends on the current CLI mode and SDR connection.

In EXEC and global configuration mode, you can view the SDR configuration for the SDR to which you are connected. When you are connected to the DSC and operating in administration EXEC and administration configuration mode, you can view the administration configuration, which includes hardware assignments for SDRs and multishelf systems.

To display the SDR portion of the running configuration, connect to the appropriate SDR and enter the **show running-config** command in EXEC or global configuration mode, as shown in the following example:

```
RP/0/RP1/CPU0:router(config)# show running-config

Building configuration...
!! Last configuration change at 11:05:38 UTC Mon May 02 2005 by cisco
!
hostname router
logging console debugging
telnet ipv4 server max-servers 5
username iosxr
 password 7 011F0706
 group root-system
 group cisco-support
!
ntp
 interface Loopback99
  broadcast
 !
 interface Loopback999
  broadcast
 !
 interface Loopback9999
  broadcast
 !
 authenticate
 max-associations 2000
!
interface Loopback0
 ipv4 address 10.1.2.3 255.255.0.0
 load-interval 0
!
interface Loopback1
 ipv4 address 10.4.5.6 255.255.0.0
!
interface Loopback7
 load-interval 0
!
interface Loopback2000
 load-interval 0
!
interface Loopback2001
 load-interval 0
!
interface Loopback2003
 load-interval 0
!
interface MgmtEth0/RP1/CPU0/0
 ipv4 address 10.11.12.13 255.255.0.0
!
interface POS0/0/0/0
 shutdown
!
interface POS0/0/0/1
 shutdown
!
```

```
interface POS0/0/0/2
 shutdown
!
interface POS0/0/0/3
 shutdown
!
interface POS0/3/0/0
 shutdown
!
interface POS0/3/0/1
 shutdown
!
interface POS0/3/0/2
 shutdown
!
interface POS0/3/0/3
 shutdown
!
interface preconfigure MgmtEth0/RP0/CPU0/0
 shutdown
!
router static
 address-family ipv4 unicast
 0.0.0.0/0 MgmtEth0/RP1/CPU0/0
 !
!
end
```

To display the administration portion of the running configuration, connect to the DSC and enter the **show running-config** command in administration EXEC or administration configuration mode, as shown in the following example:

```
RP/0/RP0/CPU0:CRS-8_P1(admin)# show running-config
Building configuration...
sdr test
 location 0/1/* primary
!
username cisco
 secret 5 $1$SegP$9jcoyk09S5cM.h/tX36yj.
 group root-system
!
end
```

Displaying a Sanitized Version of the Running Configuration

A sanitized running configuration report displays the contents of the running configuration without installation specific parameters. Some configuration details, such as IP addresses, are replaced with different addresses. The sanitized configuration can be used to share a configuration without exposing the configuration details.

In EXEC and global configuration mode, you can view the sanitized SDR configuration for the SDR to which you are connected. When you are connected to the DSC and operating in administration EXEC and administration configuration mode, you can view the sanitized administration configuration, which includes hardware assignments for SDRs and multishelf systems.

To display the sanitized SDR portion of the running configuration, enter the **show running-config sanitized** command in EXEC or global configuration mode, as shown in the following example:

```
RP/0/RP1/CPU0:router(config)# show running-config sanitized

Building configuration...
```

```
!! Last configuration change at 11:05:38 UTC Mon May 02 2005 by <removed>
!
hostname <removed>
logging console debugging
telnet ipv4 server max-servers 5
username <removed>
 password 7 <removed>
 group root-system
 group cisco-support
!
ntp
 interface Loopback99
  broadcast
 !
 interface Loopback999
  broadcast
 !
 interface Loopback9999
  broadcast
 !
 authenticate
 max-associations 2000
!
interface Loopback0
 ipv4 address 10.0.0.0 255.0.0.0
 load-interval 0
!
interface Loopback1
 ipv4 address 10.0.0.0 255.0.0.0
!
interface Loopback7
 load-interval 0
!
interface Loopback2000
 load-interval 0
!
interface Loopback2001
 load-interval 0
!
interface Loopback2003
 load-interval 0
!
interface MgmtEth0/RP1/CPU0/0
 ipv4 address 10.0.0.0 255.0.0.0
!
interface POS0/0/0/0
 shutdown
!
interface POS0/0/0/1
 shutdown
!
interface POS0/0/0/2
 shutdown
!
interface POS0/0/0/3
 shutdown
!
interface POS0/3/0/0
 shutdown
!
interface POS0/3/0/1
 shutdown
!
interface POS0/3/0/2
```

```
 shutdown
!
interface POS0/3/0/3
 shutdown
!
interface preconfigure MgmtEth0/RP0/CPU0/0
 shutdown
!
router static
 address-family ipv4 unicast
 0.0.0.0/0 MgmtEth0/RP1/CPU0/0
 !
!
end
```

To display the sanitized administration portion of the running configuration, connect to the DSC and enter the **show running-config sanitized** command in administration EXEC or administration configuration mode, as shown in the following example:

```
RP/0/RP0/CPU0:CRS-8_P1(admin)# show running-config sanitized
Building configuration...
sdr <removed>
 location 0/1/* primary
!
username <removed>
 secret 5 <removed>
 group root-system
!
end
```

Displaying the Target Configuration

The target configuration includes the configuration changes that have been entered but not yet committed. These changes are not yet part of the running configuration.

You can view the target configuration in global configuration and administration configuration modes. You cannot view the target configuration in EXEC modes because the target configuration must be committed or abandoned before returning to EXEC or administration EXEC mode.

To display the target configuration changes you have entered for an SDR, enter the **show configuration** command in global configuration mode or in any submode, as shown in the following example:

```
RP/0/RP0/CPU0:router(config-if)# show configuration

Building configuration...
interface POS0/3/0/3
 description faq
 ipv4 address 10.1.1.1 255.0.0.0
end
```

To display the target administration configuration changes you have entered, enter the **show configuration** command in administration configuration mode or in any submode, as shown in the following example:

```
RP/0/RP0/CPU0:CRS-8_P1(admin-config-sdr:test)# show configuration
Building configuration...
sdr test
 location 0/1/* primary
!
end
```

Displaying a Combined Target and Running Configuration

Although the target and running configurations remain separate until the target configuration is committed, you can preview the combined target and running configuration without committing the changes. The combined configuration shows what the new running configuration will look like after the changes from the target configuration are committed. It does not represent the actual running configuration.

You can preview the combined configuration in global configuration and administration configuration modes. You cannot preview the combined configuration in EXEC modes because the target configuration must be committed or abandoned before returning to EXEC or administration EXEC mode.

To display the combined target and running configuration, enter the **show configuration merge** command in any configuration mode.

Note The **merge** option does not appear in command help until the target configuration contains at least one configuration change.

The following example shows how to display the active SDR configuration (**show running-config**), configure an interface, and display the "merged" configuration:

```
RP/0/RP0/CPU0:router# show running-config

Building configuration...
!! Last configuration change at 16:52:49 UTC Sun March 10 2004 by cisco
!
hostname router
shutdown
end

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/3/0/3
RP/0/RP0/CPU0:router(config-if)# description faq
RP/0/RP0/CPU0:router(config-if)# ipv4 address 10.1.1.1 255.0.0.0

RP/0/RP0/CPU0:router(config-if)# show configuration merge
Building configuration...
!! Last configuration change at 16:52:49 UTC Sun March 10 2004 by cisco
!
hostname router
interface POS0/3/0/3
 description faq
 ipv4 address 10.1.1.1 255.0.0.0
 shutdown
end
```

Displaying Configuration Error Messages and Descriptions

Configuration changes are automatically verified during the commit operation, and a message is displayed if one or more configuration entries fail. To display an error message and description for a failed configuration, enter the **show configuration failed** command.

Note You can view configuration errors only during the current configuration session. If you exit configuration mode after the commit operation, the configuration error information is lost.

In the following example, an error is introduced in global configuration mode and the error information is displayed after the commit operation fails:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# taskgroup bgp
RP/0/RP0/CPU0:router(config-tg)# description this is a test of an invalid taskgroup
RP/0/RP0/CPU0:router(config-tg)# commit

% Failed to commit one or more configuration items. Please use 'show configurati
on failed' to view the errors

RP/0/RP0/CPU0:router(config-tg)# show configuration failed

!! CONFIGURATION FAILED DUE TO SEMANTIC ERRORS
taskgroup bgp
!!% Usergroup/Taskgroup names cannot be taskid names
!
```

Displaying Configuration Error Messages Without Descriptions

Configuration changes are automatically verified during the commit operation, and a message is displayed if one or more configuration entries fail. To display only the error message (without a description) for a failed configuration, enter the **show configuration failed noerror** command, as shown in the following example:

```
RP/0/RP0/CPU0:router(config-tg)# show configuration failed noerror

!! CONFIGURATION FAILED DUE TO SEMANTIC ERRORS
taskgroup bgp
!
```

Note You can view configuration errors only during the current configuration session. If you exit configuration mode after the commit operation, the configuration error information is lost.

Displaying Configuration Error Messages Produced While Loading a Configuration

To display any syntax errors found in a configuration loaded with the **load** command, enter the **show configuration failed load** command.

Saving the Target Configuration to a File

Target configurations can be saved to a separate file without committing them to the running configuration. Target configuration files can then be loaded at a later time and further modified or committed.

To save the configuration changes in the target configuration to a file, enter the **save configuration** *device***:** command. Replace the *device* argument with the name of the device on which you want to store the file (for example, disk0). After you enter this command, the router prompts you to enter a filename. If you enter only a filename, the file is stored in the root directory of the device. To store the file in a

directory, enter the directory path and filename when prompted. We recommend that you specify the `cfg` file extension for easy identification. This suffix is not required, but it can help locate target configuration files. Example: `myconfig.cfg`

In the following example, a target configuration file is saved to the usr/cisco directory of disk0:

```
RP/0/RP1/CPU0:CRS-8_P1(admin-config)# save configuration disk0:
Destination file name (control-c to abort): [/running-config]?/usr/cisco/test.cfg
Building configuration.
1 lines built in 1 second
[OK]
```

Note You can also save a configuration to a file using the **show configuration | file** *filename* command.

Loading the Target Configuration from a File

To populate the target configuration with the contents of a previously saved configuration file, go to global configuration or administration configuration mode and Enter the **load** *filename* command. Consider the following when entering the *filename* argument:

- The *filename* argument specifies the configuration file to be loaded into the target configuration.
- If the full path of the file is not specified, the router attempts to load the file from the root directory on the device.

In the following example, a target configuration file is loaded into the current configuration session. The current configuration session is therefore populated with the contents of the file:

```
RP/0/RP1/CPU0:CRS-8_P1(config)# load disk0:/usr/cisco/test.cfg
Loading.
77 bytes parsed in 1 sec (76)bytes/sec
```

Loading an Alternative Configuration at System Startup

When a router is reset or powered on, the last running configuration is loaded and used to operate the router.

You can load an alternative configuration during system boot. See *Cisco IOS XR ROM Monitor Guide* for information and instructions on this process.

Clearing All Changes to a Target Configuration

To clear changes made to the target configuration without terminating the configuration session, enter the **clear** command in global configuration mode or administration configuration mode. This command deletes any configuration changes that have not been committed.

In the following example, the user configures an interface but does not commit it. After reviewing the changes to the target configuration with the **show configuration** command, the user decides to remove the changes and start over by entering the **clear** command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/RP0/CPU0:router(config-if)# description this is my interface
RP/0/RP0/CPU0:router(config-if)# ipv4 address 10.1.1.1 255.0.0.0
RP/0/RP0/CPU0:router(config-if)# shutdown
RP/0/RP0/CPU0:router(config-if)# exit

RP/0/RP0/CPU0:router(config)# show configuration

Building configuration...
interface POS0/3/0/1
 description this is my interface
 ipv4 address 10.1.1.1 255.0.0.0
 shutdown
end

RP/0/RP0/CPU0:router(config)# clear
RP/0/RP0/CPU0:router(config)# show configuration
Building configuration...
end
```

Committing Changes to the Running Configuration

The changes in the target configuration do not become part of the running configuration until you enter the **commit** command. When you commit a target configuration, you can use the **commit** command to do either of the following:

- Merge the target configuration with the running configuration to create a new running configuration.
- Replace the running configuration with the target configuration.

Note If you try to end a configuration session without saving your changes to the running configuration with the **commit** command, you are prompted to save the changes. See the "Ending a Configuration Session" section on page 4-38 for more information.

To commit target configuration changes to the running configuration, enter the **commit** command by itself or with one or more of the options described in Table 4-5.

Table 4-5 Commit Command Options

Command	Description
commit	(Default) Merges the target configuration with the running configuration and commits changes only if all changes in the target configuration pass the semantic verification process. If any semantic errors are found, none of the configuration changes takes effect.
commit best-effort	Merges the target configuration with the running configuration and commits only valid changes (best effort). Some configuration changes might fail due to semantic errors.

Table 4-5 Commit Command Options (continued)

Command	Description
commit comment *line*	(Optional) Assigns a comment to a commit. • This text comment is displayed in the commit entry displayed with the **show configuration commit list** [**detail**] command. • The *line* argument is the text for the optional comment or label. • The **comment** option must appear at the end of the command line. If multiple options are entered, all text after the **comment** option is treated as a comment.
commit confirmed *seconds*	(Optional) Commits the configuration in global configuration mode on a trial basis for a minimum of 30 seconds and a maximum of 300 seconds (5 minutes). • During the trial configuration, enter **commit** to confirm the configuration. If you do not enter the **commit** command, the router reverts to the previous configuration when the trial time period expires. • The **confirmed** option is not available in administration configuration mode.
commit label *line*	(Optional) Assigns a meaningful label. This label is displayed in the output for the **show configuration commit list** [**detail**] command instead of the numeric label. • The *line* argument is the text for the optional comment or label.
commit force	(Optional) Merges the target configuration with the running configuration and allows a configuration commit in low-memory conditions. A low-memory warning occurs when a user attempts to commit a target configuration that exceeds the default capacity of the router. The recommended resolution to such a warning is to remove configurations using the **no** commands. **Caution** The **force** option can cause the router to experience severe problems if low-memory conditions occur. The **force** option should be used only to remove configurations.
commit replace	(Optional) Replaces the contents of the running configuration with the target configuration.

Examples

In the following example, the default **commit** command is entered in global configuration mode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/0/0/2
RP/0/RP0/CPU0:router(config-if)# description faq
RP/0/RP0/CPU0:router(config-if)# ipv4 address 10.1.1.1 255.0.0.0
RP/0/RP0/CPU0:router(config-if)# commit

RP/0/0/0:Aug  6 09:26:17.781 : %LIBTARCFG-6-COMMIT Configuration committed by user
'cisco'.   Use 'show configuration commit changes 1000000124' to view the changes.
```

Note The preceding message is stored in the log and appears only if logging is configured to display on screen.

In the next example, the **commit** command is entered with the **label** and **comment** options in administration configuration mode:

```
RP/0/RP0/CPU0:CRS-8_P1# admin
RP/0/RP0/CPU0:CRS-8_P1(admin)# configure
RP/0/RP0/CPU0:CRS-8_P1(admin-config)# sdr test
RP/0/RP0/CPU0:CRS-8_P1(admin-config-sdr:test)# location 0/1/* primary
RP/0/RP0/CPU0:CRS-8_P1(admin-config-sdr:test)# commit label test comment This is a test
RP/0/RP0/CPU0:CRS-8_P1(admin-config)# show configuration commit list detail

   1) CommitId: 2000000018                Label: test
      UserId:   jbowman                   Line:  vty1
      Client:   CLI                       Time:  23:45:40 UTC Tue Mar 07 2006
      Comment:   This is a test
.
.
.
```

Note Configuration files are stored on the same flash disk as the boot image. Access these configurations only through the CLI commands for configuration management, history, and rollback. Direct modification or deletion of these files can result in lost router configurations.

Reloading a Failed Configuration

If the router displays a configuration failure message when you attempt to commit a configuration change, the configuration changes are not lost. While you remain in global configuration mode or administration configuration mode, you can load the configuration changes into the target configuration, correct the errors, and commit the changes. To load a failed configuration, go to global configuration or administration configuration mode and enter the **load configuration failed commit** command, as shown in the following example:

```
RP/0/0/CPU0:router(config)# load configuration failed commit

RP/0/0/CPU0:router(config)# show configuration

Building configuration...
taskgroup bgp
!
end
```

In the preceding example, the **show configuration** command displays the target configuration, which includes the failed configuration.

Note The failed configuration is discarded if you exit global configuration mode or administration configuration mode without recovering the configuration. After recovery, correct and commit the configuration or save it to a file to avoid losing it.

Exiting a Configuration Submode

When you have finished configuration changes in a configuration submode, such as the interface or SDR configuration submodes, you can return to return to the previous configuration mode and continue making configuration changes. To exit a configuration submode, enter the **exit** command, as shown in the following example:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/RP0/CPU0:router(config-if)# description this is my interface
RP/0/RP0/CPU0:router(config-if)# ipv4 address 10.1.1.1 255.0.0.0
RP/0/RP0/CPU0:router(config-if)# exit
RP/0/RP0/CPU0:router(config)#
```

Note If you use the **exit** command to exit global configuration or administration configuration mode, the router prompts you to save changes, discard changes, or cancel the action, as described in the next section.

Ending a Configuration Session

You can use any of the following methods to end a configuration session:

- Enter the **exit** command in global configuration or administration configuration mode.
- Enter the **end** command in any configuration mode or submode
- Press Ctrl-Z.

Note If you enter the **exit** command in a configuration submode, the command returns you to the parent configuration level.

If you end a configuration session without committing the configuration changes, the router prompts you to save changes, discard changes, or cancel the action, as shown in the following example:

```
RP/0/RP0/CPU0:CRS-8_P1(config-if)# end
Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:
```

Respond to the prompt by entering one of the following options:

- **yes**, commit the configuration changes and exit configuration mode
- **no**, exit configuration mode without committing the configuration changes
- **cancel**, remain in configuration mode without committing the configuration changes

Note In EXEC mode, the **exit** command logs the user out of the system.

Aborting a Configuration Session

When you abort a configuration session, any changes are discarded and the configuration session ends. No warning is given before the configuration changes are deleted.

In global configuration mode, the **abort** command discards configuration changes and returns to EXEC mode. In administration configuration mode, the **abort** command discards configuration changes and returns to administration EXEC mode. To abort a configuration session, enter the **abort** command, as shown in the following example:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# hostname host1
RP/0/RP0/CPU0:router(config)# interface POS 0/2/0/2
RP/0/RP0/CPU0:router(config-if)# description this is my interface
RP/0/RP0/CPU0:router(config-if)# ipv4 address 10.1.1.1 255.0.0.0
RP/0/RP0/CPU0:router(config-if)# shutdown
RP/0/RP0/CPU0:router(config-if)# abort
RP/0/RP0/CPU0:router#
```

Configuring the SDR Hostname

The hostname identifies an SDR on the network. Although devices can be uniquely identified by their Layer 2 and Layer 3 addresses (such as an IP address), it is often simpler to remember network devices by an alphanumeric “hostname.” This name is used in the CLI prompt and default configuration filenames and to identify the SDR on the network.

To configure the hostname, enter the **hostname** command with the SDR name as shown in the following example:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# hostname SDR_SJ
RP/0/RP0/CPU0:router(config)# commit
RP/0/RP0/CPU0:Apr  7 00:07:33.246 : config[65669]: %LIBTARCFG-6-COMMIT : Configu
ration committed by user 'user_a'.  Use 'show configuration commit changes 1000000067' to
view the changes.
RP/0/RP0/CPU0:SDR_SJ(config)#
```

The preceding example sets the SDR name to SDR_SJ.

Note No blanks or spaces are permitted as part of a name. Do not expect case to be preserved. Upper- and lowercase characters look the same to many Internet software applications. It may seem appropriate to capitalize a name the same way you might if you were writing, but conventions dictate that computer names appear all lowercase. For more information, see RFC 1178, *Choosing a Name for Your Computer.*

Configuring the Management Ethernet Interface

The Management Ethernet interface on the RPs is used to connect the router to a network for remote management using a Telnet client, the Craft Works Interface (CWI), the Simple Network Management Protocol (SNMP), or other management agents. The following sections provide information on the Management Ethernet interface:

- "Specifying the Management Ethernet Interface Name in CLI Commands"
- "Displaying the Available Management Ethernet Interfaces"
- "Configuring the Management Ethernet Interface"

Specifying the Management Ethernet Interface Name in CLI Commands

Before you can configure the Management Ethernet interface, you must know the Management Ethernet interface name, which is defined using the following syntax: *typerack/slot/module/port*. Table 4-6 describes the Management Ethernet interface name syntax.

Table 4-6 Management Ethernet Interface Name Syntax Description

Syntax Components	Description
type	Interface *type* for a Management Ethernet port is "MgmtEth."
rack	Chassis number of the rack. In a single-shelf system, the *rack* is always "0." In a multishelf system, the LCC rack number range is 0 to 255.
slot	Physical slot of the RP or DRP on which the interface is located. For a Cisco CRS-1 router, the RP *slot* is "RP0" or "RP1," and the DRP slot is a number in the range of 0 to 3 (4-slot chassis), 0 to 7 (8-slot chassis), or 0 to 15 (16-slot chassis). For a Cisco XR 12000 Series Router, the PRPs may be installed in slots 0 through 15, depending on the router model.
module	On an RP, the *module* is "CPU0." DRPs have two processors, so the *module* is either "CPU0" and "CPU1."
port	On Cisco XR 12000 Series Routers, there are two Ethernet ports on PRP-1 cards and three Ethernet ports on PRP-2 cards. The Ethernet ports are labeled ETH 0, ETH 1, and ETH 2. For the ETH 0 port, specify **0**, for the ETH 1 port, specify **1**, and for the ETH 2 port, specify **2**. On a Cisco CRS-1 router, one Ethernet port labeled MGMT ETH exists on each RP, and one port exists for each DRP processor. Specify 0 for the MGMT ETH interface on an RP or DRP.

Table 4-6 provides examples of Management Ethernet interface names for a single-shelf system.

Table 4-7 Management Ethernet Interface Names for Single-Shelf Systems

Management Interface	Interface Name	Example
Cisco CRS-1 RP in slot RP0	MgmtEth0/RP0/CPU0/0	router(config)# **interface MgmtEth0/RP0/CPU0/0**

Table 4-7 Management Ethernet Interface Names for Single-Shelf Systems (continued)

Cisco CRS-1 RP in slot RP1	MgmtEth0/RP1/CPU0/0	router(config)# **interface MgmtEth0/RP1/CPU0/0**
Cisco CRS-1 DRP CPU0 in slot 5	MgmtEth0/5/CPU0/0	router(config)# **interface MgmtEth0/5/CPU0/0**
Cisco CRS-1 DRP CPU1 in slot 5	MgmtEth0/5/CPU1/0	router(config)# **interface MgmtEth0/5/CPU1/0**
Cisco XR 12000 Series Router PRP in slot 0, port ETH0	MgmtEth0/0/CPU0/0	router(config)# **interface MgmtEth0/0/CPU0/0**
Cisco XR 12000 Series Router PRP in slot 0, port ETH1	MgmtEth0/0/CPU0/1	router(config)# **interface MgmtEth0/0/CPU0/1**
Cisco XR 12000 Series Router PRP in slot 1, port ETH0	MgmtEth0/1/CPU0/0	router(config)# **interface MgmtEth0/1/CPU0/0**
Cisco XR 12000 Series Router PRP in slot 1, port ETH1	MgmtEth0/1/CPU0/1	router(config)# **interface MgmtEth0/1/CPU0/1**

Displaying the Available Management Ethernet Interfaces

To display the router interfaces, enter the **show interfaces brief** command in EXEC mode as follows:

```
RP/0/0/CPU0:router# show interfaces brief

                 Intf        Intf         LineP              Encap  MTU       BW
                 Name        State        State               Type (byte)   (Kbps)

--------------------------------------------------------------------------------

                  Nu0          up           up               Null  1500   Unknown

         Mg0/0/CPU0/0          up           up               ARPA  1514    100000

         Mg0/0/CPU0/1   admin-down   admin-down               ARPA  1514     10000

            PO0/3/0/0   admin-down   admin-down               HDLC  4474    155520

            PO0/3/0/1   admin-down   admin-down               HDLC  4474    155520

            PO0/3/0/2   admin-down   admin-down               HDLC  4474    155520

            PO0/3/0/3   admin-down   admin-down               HDLC  4474    155520

            PO0/3/0/4   admin-down   admin-down               HDLC  4474    155520

            PO0/3/0/5   admin-down   admin-down               HDLC  4474    155520

            PO0/3/0/6   admin-down   admin-down               HDLC  4474    155520

            PO0/3/0/7   admin-down   admin-down               HDLC  4474    155520
.
.
.
```

The Management Ethernet interfaces are listed with the prefix Mg in the Intf Name column.

Configuring the Management Ethernet Interface

To use the Management Ethernet interface for system management and remote communication, you must configure an IP address and a subnet mask for the interface. If you want the interface to communicate with devices on other networks (such as remote management stations or TFTP servers), you need to configure a default route for the router.

Tip For information on additional configuration options for the Management Ethernet interface, see the *Cisco IOS XR Interface and Hardware Component Configuration Guide*.

Prerequisites

To configure the Ethernet Management port for network communications, you must enter the interface network addresses and subnet mask. Consult your network administrator or system planner for this information.

SUMMARY STEPS

1. **configure**
2. **interface MgmtEth***rack*/*slot*/**CPU0/***port*
3. **ipv4 address** *ipv4-address subnet-mask*
4. **no shutdown**
5. **exit**
6. **router static address-family ipv4 unicast 0.0.0.0/0** *default-gateway*
7. **commit**
8. **end**
9. **show interfaces MgmtEth***rack*/*slot*/**CPU0/***port*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RP0/CPU0:router# configure`	Enters global configuration mode.
Step 2	**interface MgmtEth***rack*/*slot*/**CPU0/***port* **Example:** `RP/0/RP0/CPU0:router(config)# interface MgmtEth0/RP0/CPU0/0`	Enters interface configuration mode and specifies the Management Ethernet interface of the primary RP. • The syntax is **interface** *typerack/slot/module/port*: The command parameters are described in Table 4-6.

	Command or Action	Purpose
Step 3	**ipv4 address** *ipv4-address subnet-mask* **Example:** `RP/0/RP0/CPU0:router(config-if)# ipv4 address 10.1.1.1 255.0.0.0`	Assigns an IP address and subnet mask to the interface.
Step 4	**no shutdown** **Example:** `RP/0/RP0/CPU0:router(config-if)# no shutdown`	Places the interface in an "up" state.
Step 5	**exit**	Exits the Management Ethernet interface configuration mode.
Step 6	**router static address family ipv4 unicast 0.0.0.0/0** *default-gateway* **Example:** `RP/0/RP0/CPU0:router (config)# router static address-family ipv4 unicast 0.0.0.0/0 12.25.0.1`	Configures a default route to use for communications with devices on other networks. • Replace *default-gateway* with the IP address of the local gateway that can be used to reach other networks. • This default route applies to all interfaces. You might need to configure additional static routes to support your network. For more information on configuring static routes, see the *Cisco IOS XR Routing Configuration Guide*.
Step 7	**commit** **Example:** `RP/0/RP0/CPU0:router(config)# commit`	Commits the target configuration to the running configuration.
Step 8	**end** **Example:** `RP/0/RP0/CPU0:router(config)# end`	Ends the configuration session and returns to EXEC mode.
Step 9	**show interfaces MgmtEth***rack***/***slot***/CPU0/***port* **Example:** `RP/0/RP0/CPU0:router# show interfaces MgmtEth0/RP0/CPU0/0`	Displays the interface details to verify the settings.

Examples

In the following example, the Management Ethernet interface on the RP in slot RP1 is configured with an IP address:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface MgmtEth0/RP1/CPU0/0
RP/0/RP0/CPU0:router(config-if)# ipv4 address 10.1.1.1 255.255.255.0
RP/0/RP0/CPU0:router(config-if)# no shutdown
RP/0/RP0/CPU0:router(config-if)# commit
RP/0/RP0/CPU0:router(config-if)# end
RP/0/RP0/CPU0:router#
```

```
RP/0/RP0/CPU0:router# show interfaces mgmtEth 0/RP0/CPU0/0
MgmtEth0/RP0/CPU0/0 is up, line protocol is up
  Hardware is Management Ethernet, address is 0011.93ef.e8ea (bia 0011.93ef.e8e)
  Description: Connected to Lab LAN
  Internet address is 10.1.1.1/24
  MTU 1514 bytes, BW 100000 Kbit
     reliability 255/255, txload Unknown, rxload Unknown
  Encapsulation ARPA,  loopback not set,
  ARP type ARPA, ARP timeout 04:00:00
  Last clearing of "show interface" counters never
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     375087 packets input, 22715308 bytes, 87 total input drops
     0 drops for unrecognized upper-level protocol
     Received 297320 broadcast packets, 0 multicast packets
              0 runts, 0 giants, 0 throttles, 0 parity
     48 input errors, 43 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     89311 packets output, 6176363 bytes, 0 total output drops
     Output 53 broadcast packets, 0 multicast packets
     0 output errors, 0 underruns, 0 applique, 0 resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
```

Related Documents

Related Topic	Document Title
Additional information on configuring management interfaces	*Cisco IOS XR Interface and Hardware Component Configuration Guide*

Manually Setting the Router Clock

Generally, if the system is synchronized by a valid outside timing mechanism, such as a Network Time Protocol (NTP) or VINES clock source, you need not set the software clock. Use the **clock set** command for initial configuration or if a network time source is not available.

The **clock timezone** command should be entered before the clock is set because it defines the difference between the system time and Coordinated Universal Time (UTC). When you set the time, you set the system time, and the router uses the **clock timezone** command setting to translate that time to UTC. The system internally keeps time in UTC. When you enter the **show clock** command, the router displays the system time.

To manually set the router clock, complete the following steps:

SUMMARY STEPS

1. **configure**
2. **clock timezone** *zone hours-offset*
3. **commit**
4. **end**
5. **clock set** *hh*:*mm*:*ss dd mm yyyy*
6. **clock update-calendar**
7. **show clock**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RP0/CPU0:router# configure`	Enters global configuration mode.
Step 2	**clock timezone** *zone hours-offset* **Example:** `RP/0/RP0/CPU0:router(config)# clock timezone pst -8`	Sets the time zone for the router clock. • The **clock timezone** command should be entered before the clock is set because it defines the difference between the system time and UTC. **Note** The system time is the time that appears when you enter the **show clock** command. • *zone*: Name of the time zone to be displayed when standard time is in effect. • *hours-offset*: Difference in hours from UTC. • For detailed information about setting the system clock, including the configuration of a network time server, see the following Cisco documents: – *Cisco IOS XR System Management Configuration Guide* – *Cisco IOS XR System Security Command Reference*
Step 3	**commit** **Example:** `RP/0/RP0/CPU0:router(config-if)# commit`	Commits the target configuration to the running configuration.
Step 4	**end** **Example:** `RP/0/RP0/CPU0:router(config-if)# end`	Ends the configuration session and returns to EXEC mode.
Step 5	**clock set** *hh:mm:ss dd mm yyyy* **Example:** `RP/0/RP0/CPU0:router# clock set 14:12:00 10 feb 2004`	Sets the system software clock.

Step 6	**clock update-calendar** **Example:** `RP/0/RP0/CPU0:router# clock update-calendar`	Updates the hardware clock (calendar clock) with the new clock settings. • The hardware clock is battery operated and runs continuously, even if the router is powered off or rebooted.
Step 7	**show clock** **Example:** `RP/0/RP0/CPU0:router# show clock`	Displays the clock setting. • Use this command to verify the settings.

Examples

In the following example, the manual system clock is configured:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# clock timezone pst -8
RP/0/RP0/CPU0:router(config)# commit
RP/0/RP0/CPU0:router(config)# end
RP/0/RP0/CPU0:router# clock set 14:12:00 10 feb 2004
14:12:00.090 PST Tue Feb 10 2004
RP/0/RP0/CPU0:router# clock update-calendar
RP/0/RP0/CPU0:router# show clock
14:12:00.090 PST Tue Feb 10 2004
```

Related Documents

Related Topic	Document Title
Descriptions of the clock commands available in the Cisco IOS XR software	*Cisco IOS XR System Management Command Reference*
Commands used to configure the NTP	*Cisco IOS XR System Management Command Reference*
Configuration of the NTP on the Cisco IOS XR software	*Cisco IOS XR System Management Configuration Guide*

Where to Go Next

When you have completed the configuration procedures in this chapter, consider the following resources for additional configuration documentation:

- For information on configuring additional general router features, see Chapter 5, “Configuring Additional Router Features.”
- For information on using the Cisco IOS XR software more efficiently, see Chapter 6, “CLI Tips, Techniques, and Shortcuts.”
- For information on configuring interfaces, see the hardware documents listed in the “Related Documents” section on page x.

CHAPTER 5

Configuring Additional Router Features

This chapter contains instructions and information for entering basic configurations using the command-line interface (CLI).

Contents

This chapter contains the following sections:

Configuring the Domain Name and Domain Name Server

Configure a domain name and domain name server (DNS) for your router to make contacting other devices on your network more efficient. Use the following guidelines:

- To define a default domain name that the Cisco IOS XR software uses to complete unqualified hostnames (names without a dotted-decimal domain name), use the **domain-name** command in global configuration mode.
- To specify the address of one or more name servers to use for name and address resolution, use the **domain name-server** command in global configuration mode. If no name server address is specified, the default name server is 255.255.255.255 so the DNS lookup can be broadcast to the local network segment. If a DNS server is in the local network, it replies. If not, there might be a server that knows how to forward the DNS request to the correct DNS server.
- Use the **show hosts** command in EXEC mode to display the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses.

To configure the DNS and DNS server, complete the following steps:

SUMMARY STEPS

1. **configure**
2. **domain name** *domain-name-of-organization*
3. **domain name-server** *ipv4-address*
4. **commit**
5. **end**
6. **show hosts**

Examples

In the following example, the domain name and DNS are configured:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# domain name cisco.com
RP/0/RP0/CPU0:router(config)# domain name-server 10.1.1.1
RP/0/RP0/CPU0:router(config)# commit
RP/0/RP0/CPU0:router(config)# end
RP/0/RP0/CPU0:router# show hosts

Default domain is cisco.com
Name/address lookup uses domain service
Name servers: 10.1.1.1
```

Related Documents

Related Topic	Document Title
Complete descriptions of the domain services commands	*Implementing Host Services and Applications on Cisco IOS XR Software* in the *Cisco IOS XR IP Addresses and Services Configuration Guide*

Configuring Telnet, HTTP, and XML Host Services

For security, some host services are disabled by default. Host services, such as Telnet, Extensible Markup Language (XML), and HTTP, can be optionally enabled using the commands described in this section. Host services provide the following features:

- Enabling the Telnet server allows users to log in to the router using IPv4 or IPv6 Telnet clients.
- Enabling the HTTP server allows users to log in to the router using the CWI.
- Enabling the XML agent enables XML Common Object Request Broker Architecture (CORBA) agent services so that you can manage and configure the router using an XML interface.

Prerequisites

The following prerequisites must be met before configuring the Telnet, HTTP, and XML host services:

- For the XML and HTTP host services, the Manageability package must be installed and activated on the router.
- To enable the Secure Socket Layer (SSL) of the HTTP and XML services, the Security package must be installed and activated on the router.

See *Cisco IOS XR System Management Configuration Guide, Release 3.4* for information on installing and activating packages.

SUMMARY STEPS

1. **configure**
2. **telnet ipv4 server max-servers 5**
3. **telnet ipv6 server max-servers 5**
4. **http server**
5. **xml agent corba**
6. **commit**

Examples

In the following example, the host services are enabled:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# telnet ipv4 server max-servers 5
RP/0/RP0/CPU0:router(config)# telnet ipv6 server max-servers 5
RP/0/RP0/CPU0:router(config)# http server
RP/0/RP0/CPU0:router(config)# xml agent corba
RP/0/RP0/CPU0:router(config)# commit
```

Related Documents

Related Topic	Document Title
Installation and activation of the Manageability and Security Packages	*Cisco IOS XR System Management Configuration Guide, Release 3.4*
Descriptions of the HTTP and XML server commands	*Cisco IOS XR System Management Command Reference*
Descriptions of the Telnet commands	*Cisco IOS XR IP Addresses and Services Command Reference*

Managing Configuration History and Rollback

After each commit operation, a record of the committed configuration changes is saved. This record contains only the changes made during the configuration session; it does not contain the complete configuration. Each record is assigned a unique ID, known as a *commitID*.

When multiple commitIDs are present, you can use a commitID to identify a previous configuration to which you want to return, or you can use the commitID to load the configuration changes made during that configuration session. You can also load configuration changes from multiple commitIDs, and you can clear commitIDs. If you are thinking about rolling back the configuration to a specific commitID, consider the following guidelines:

- You cannot roll back to a configuration that was removed because of package incompatibility. Configuration rollbacks can succeed only when the configuration passes all compatibility checks with the currently active Cisco IOS XR software.
- If an incompatible configuration is found during the rollback operation, the operation fails and an error is displayed.

The Cisco IOS XR software automatically saves up to 100 of the most recent commitIDs. The following sections describe how to manage configuration changes and roll back to a previously committed configuration:

Displaying the CommitIDs

To display a history of up to 100 of the most recent commitIDs, enter the **show configuration commit list** command in EXEC or administration EXEC mode. Up to 100 of the most recent commitIDs are saved by the system. Each commitID entry shows the user who committed configuration changes, the connection used to execute the commit, and commitID time stamp.

The commitIDs are shown in the “Label/ID” column. The following example shows the **show configuration commit list** command display in EXEC and administration EXEC modes:

```
RP/0/RP1/CPU0:router# show configuration  commit list

SNo. Label/ID    User      Line        Client      Time Stamp
~~~~ ~~~~~~~~    ~~~~      ~~~~        ~~~~~~      ~~~~~~~~~~
1    1000000219  cisco     vty0        CLI         12:27:50 UTC Wed Mar 22 2006
2    1000000218  cisco     vty1        CLI         11:43:31 UTC Mon Mar 20 2006
3    1000000217  cisco     con0_RP0_C  CLI         17:44:29 UTC Wed Mar 15 2006

RP/0/RP1/CPU0:router# admin
RP/0/RP1/CPU0:router(admin)# show configuration commit list

SNo. Label/ID    User      Line        Client      Time Stamp
~~~~ ~~~~~~~~    ~~~~      ~~~~        ~~~~~~      ~~~~~~~~~~
1    2000000022  cisco     vty1        CLI         15:03:59 UTC Fri Mar 17 2006
2    2000000021  cisco     con0_RP0_C  CLI         17:42:55 UTC Wed Mar 15 2006
3    2000000020  SYSTEM    con0_RP0_C  Setup Dial  17:07:39 UTC Wed Mar 15 2006
```

Displaying the Configuration History Log

To display the header records for up to 1000 commit events, enter the **show configuration commit history** command in EXEC or administration EXEC mode, as shown in the following example.

The output from this command does not show the details of the entries, but allows you to display a larger list of the commit events that occurred. To display the commitIDs to which you can roll back, use the **show configuration commit list** command.

```
RP/0/RP0/CPU0:router# show configuration commit history

SNo. Label/ID    User      Line         Client      Time Stamp
~~~~ ~~~~~~~~    ~~~~      ~~~~         ~~~~~~      ~~~~~~~~~~
1    1000000144  user_a    vty0          CLI         00:16:51 UTC Thu May 11 2004
2    1000000143  user_a    vty0          CLI         00:04:32 UTC Thu May 11 2004
3    1000000142  user_a    0.0.0.0       XMLAgent    21:58:36 UTC Wed May 11 2004
4    1000000141  user_a    0.0.0.0       XMLAgent    21:46:07 UTC Wed May 11 2004
5    1000000140  user_b    con0_RP1_C    CLI         21:43:30 UTC Wed May 11 2004
6    1000000139  user_a    0.0.0.0       XMLAgent    21:40:13 UTC Wed May 11 2004
7    1000000138  user_a    0.0.0.0       XMLAgent    21:34:48 UTC Wed May 11 2004
8    1000000137  user_b    con0_RP1_C    CLI         21:32:10 UTC Wed May 11 2004
9    1000000136  user_a    0.0.0.0       XMLAgent    21:30:13 UTC Wed May 11 2004
10   1000000135  user_b     con0_RP1_C   CLI         19:45:04 UTC Wed May 11 2004
11   1000000134  user_b     con0_RP1_C   CLI         19:37:26 UTC Wed May 11 2004
12   1000000133  user_b     con0_RP1_C   CLI         19:36:27 UTC Wed May 11 2004
13   1000000132  user_b     con0_33_1    Rollback    18:34:45 UTC Wed May 11 2004
14   1000000131  user_b     con0_33_1    Rollback    18:32:37 UTC Wed May 11 2004
15   1000000130  user_b     con0_33_1    Rollback    18:31:09 UTC Wed May 11 2004
16   1000000129  user_b     con0_33_1    CLI         18:28:12 UTC Wed May 11 2004
17   1000000128  user_b     con0_33_1    CLI         18:27:22 UTC Wed May 11 2004
18   1000000127  user_b     con0_33_1    CLI         18:27:19 UTC Wed May 11 2004
19   1000000126  user_b     con0_33_1    Rollback    18:25:55 UTC Wed May 11 2004
20   1000000125  user_b     con0_33_1    Rollback    18:24:25 UTC Wed May 11 2004
```

Displaying the Configuration Changes Recorded in a CommitID

To display the configuration changes made during a specific commit session (commitID), go to EXEC or administration EXEC mode and enter the **show configuration commit changes** command followed by a commitID number. The easiest way to determine the commitID is to enter the **show configuration commit changes ?** command first. In the following example, the command help is used to display the available commitIDs, and then the changes for a specific commitID are displayed:

```
RP/0/RP1/CPU0:router(admin)# show configuration commit changes ?

  last        Changes made in the most recent <n> commits
  since       Changes made since (and including) a specific commit
  2000000020  Commit ID
  2000000021  Commit ID
  2000000022  Commit ID

RP/0/RP1/CPU0:router(admin)# show configuration commit changes 2000000020

Building configuration...
username cisco
 secret 5 $1$MgUH$xzUEW6jLfyAYLKJE.3p440
 group root-system
!
end
```

Previewing Rollback Configuration Changes

The **show configuration rollback changes** command allows you to preview the configuration changes that take place if you roll back the configuration to a specific commitID. For example, if you want to roll back the configuration to a specific point, all configuration changes made after that point must be undone. This rollback process is often accomplished by executing the "no" version of commands that must be undone.

To display the prospective rollback configuration changes from the current configuration to a specific commitID, go to EXEC or administration EXEC mode and enter the **show configuration rollback changes to** *commitId* command. In the following example, the command help displays the available commitIDs, and then the rollback changes are displayed.

```
RP/0/RP1/CPU0:router# show configuration rollback changes to ?

  1000000217  Commit ID
  1000000218  Commit ID
  1000000219  Commit ID

RP/0/RP1/CPU0:router# show configuration rollback changes to 1000000218

Building configuration...
no interface Loopback100
interface POS0/1/0/0
 no ipv6 nd dad attempts
!
!
no route-policy xx
end
```

To display the prospective rollback configuration changes from the current configuration to a specified number of previous sessions, go to EXEC or administration EXEC mode and enter the **show configuration rollback changes last** *commit-range* command:

```
RP/0/RP0/CPU0:router# show configuration rollback changes last 2

Building configuration...
interface Loopback3
no description
no ipv4 address 10.0.1.1 255.0.0.0
exit
interface Loopback4
no description
no ipv4 address 10.0.0.1 255.0.0.0
end
```

In the preceding example, the command display shows the proposed rollback configuration changes for the last two commit IDs.

Rolling Back the Configuration to a Specific Rollback Point

When you roll back the configuration to a specific rollback point, you undo all configuration changes made during the session identified by the commit ID for that rollback point, and you undo all configuration changes made after that point. The rollback process rolls back the configuration and commits the rolled-back configuration. The rollback process also creates a new rollback point so that you can roll back the configuration to the previous configuration.

Tip To preview the commands that undo the configuration during a rollback, use the **show configuration rollback changes** command.

To roll back the router configuration to a previously committed configuration, go to EXEC or administration EXEC mode and enter the **rollback configuration to** *commitId* command:

```
RP/0/RP1/CPU0:router# rollback configuration to 1000000220
Loading Rollback Changes.
Loaded Rollback Changes in 1 sec
Committing.
2 items committed in 1 sec (1)items/sec
Updating.
Updated Commit database in 1 sec
Configuration successfully rolled back to '1000000220'.
```

Rolling Back the Configuration over a Specified Number of Commits

When you roll back the configuration over a specific number of commits, you do not have to enter a specific commit ID. Instead, you specify a number *x*, and the software undoes all configuration changes made in the last *x* committed configuration sessions. The rollback process rolls back the configuration, commits the rolled-back configuration, and creates a new commitID for the previous configuration.

Tip To preview the commands that undo the configuration during a rollback, use the **show configuration rollback changes** command.

To roll back to the last *x* commits made, go to EXEC or administration EXEC mode and enter the **rollback configuration last** *x* command; *x* is a number ranging from 1 to the number of saved commits in the commit database.

In the following example, a request is made to roll back the configuration changes made during the previous two commits:

```
RP/0/RP0/CPU0:router# rollback configuration last 2

Loading Rollback Changes.
Loaded Rollback Changes in 1 sec
Committing.
1 items committed in 1 sec (0)items/sec
Updating.
Updated Commit database in 1 sec
Configuration successfully rolled back 2 commits.
```

Loading CommitID Configuration Changes to the Target Configuration

If the changes saved for a specific commitID are close to what you want, but a rollback is not appropriate, you can load the configuration changes for a commitID into the target configuration, modify the target configuration, and then commit the new configuration. Unlike the rollback process, the loaded changes are not applied until you commit them.

Note Unlike the rollback process, loading the commitID configuration changes loads only the changes made during that commit operation. The load process does not load all changes made between the commitID and the current committed configuration.

To load commitID changes in the target configuration, go to global configuration or administration configuration mode and enter the **load commit changes** command with the commitID number. In the following example, show commands are used to display the changes for a commitID, the commitID configuration is loaded into the target configuration, and the target configuration is displayed:

```
RP/0/RP1/CPU0:router# show configuration commit changes ?

  last        Changes made in the most recent <n> commits
  since       Changes made since (and including) a specific commit
  1000000217  Commit ID
  1000000218  Commit ID
  1000000219  Commit ID
  1000000220  Commit ID
  1000000221  Commit ID

RP/0/RP1/CPU0:router# show configuration commit changes 1000000219
Building configuration...
interface Loopback100
!
interface POS0/1/0/0
 ipv6 nd dad attempts 50
!
end

RP/0/RP1/CPU0:router# config

RP/0/RP1/CPU0:router(config)# load commit changes 1000000219
Building configuration...
Loading.
77 bytes parsed in 1 sec (76)bytes/sec

RP/0/RP1/CPU0:router(config)# show configuration

Building configuration...
interface Loopback100
!
interface POS0/1/0/0
 ipv6 nd dad attempts 50
!
end
```

Loading Rollback Configuration Changes to the Target Configuration

If the changes for a specific rollback point are close to what you want, but a rollback is not appropriate, you can load the rollback configuration changes into the target configuration, modify the target configuration, and then commit the new configuration. Unlike the rollback process, the loaded changes are not applied until you commit them.

Tip To display the rollback changes, enter the **show configuration rollback changes** command.

To load rollback configuration changes from the current configuration to a specific session, go to global configuration or administration configuration mode and enter the **load rollback changes to** *commitId* command:

```
RP/0/0/CPU0:router(config)# load rollback changes to 1000000068
Building configuration...
Loading.
233 bytes parsed in 1 sec (231)bytes/sec
```

To load rollback configuration changes from the current configuration to a specified number of previous sessions, go to global configuration or administration configuration mode and enter the **load rollback changes last** *commit-range* command:

```
RP/0/0/CPU0:router(config)# load rollback changes last 6
Building configuration...
Loading.
221 bytes parsed in 1 sec (220)bytes/sec
```

In the preceding example, the command loads the rollback configuration changes for the last six commitIDs.

To load the rollback configuration for a specific commitID, go to global configuration or administration configuration mode and enter the **load rollback changes** *commitId* command:

```
RP/0/0/CPU0:router(config)# load rollback changes 1000000060
Building configuration...
Loading.
199 bytes parsed in 1 sec (198)bytes/sec
```

Deleting CommitIDs

You can delete the oldest configuration commitIDs by entering the **clear configuration commit** command in EXEC or administration EXEC mode. The **clear configuration commit** command must be followed by either the amount of disk space you want to reclaim or number of commitIDs you want to delete. To reclaim disk space from the oldest commitIDs, enter the **clear configuration commit** command followed by the keyword **diskspace** and number of kilobytes to reclaim:

```
RP/0/0/CPU0:router# clear configuration commit diskspace 50
Deleting 4 rollback points '1000000001' to '1000000004'
64 KB of disk space will be freed. Continue with deletion?[confirm]
```

To delete a specific number of the oldest commitIDs, enter the **clear configuration commit** command followed by the keyword **oldest** and number of commitIDs to delete:

```
RP/0/0/CPU0:router# clear configuration commit oldest 5
Deleting 5 rollback points '1000000005' to '1000000009'
80 KB of disk space will be freed. Continue with deletion?[confirm]
```

Configuring Logging and Logging Correlation

System messages generated by the Cisco IOS XR software can be logged to a variety of locations based on the severity level of the messages. For example, you could direct information messages to the system console and also log debugging messages to a network server.

In addition, you can define correlation rules that group and summarize related events, generate complex queries for the list of logged events, and retrieve logging events through an XML interface.

The following sections describe logging and the basic commands used to log messages in Cisco IOS XR software:

Logging Locations and Severity Levels

Error messages can be logged to a variety of locations, as shown in Table 5-1.

Table 5-1 Logging Locations for System Error Messages

Logging Destination	Command (Global Configuration Mode)
console	**logging console**
vty terminal	**logging monitor**
external syslog server	**logging trap**
internal buffer	**logging buffered**

You can log messages based on the severity level of the messages, as shown in Table 5-2.

Table 5-2 Logging Severity Levels for System Error Messages

Level	Description
Level 0—Emergencies	System has become unusable.
Level 1—Alerts	Immediate action needed to restore system stability.
Level 2—Critical	Critical conditions that may require attention.
Level 3—Errors	Error conditions that may help track problems.
Level 4—Warnings	Warning conditions that are not severe.
Level 5—Notifications	Normal but significant conditions that bear notification.
Level 6—Informational	Informational messages that do not require action.
Level 7—Debugging	Debugging messages are for system troubleshooting only.

Alarm Logging Correlation

Alarm logging correlation is used to group and filter similar messages to reduce the amount of redundant logs and isolate the root causes of the messages.

For example, the original message describing a card online insertion and removal (OIR) and system state being up or down can be reported, and all subsequent messages reiterating the same event can be correlated. When you create correlation rules, a common root event that is generating larger volumes of follow-on error messages can be isolated and sent to the correlation buffer. An operator can extract all correlated messages for display later, should the need arise. See the *Cisco IOS XR System Management Configuration Guide* for more information.

Configuring Basic Message Logging

Numerous options for logging system messages in Cisco IOS XR software are available. This section provides a basic example.

To configure basic message logging, complete the following steps:

SUMMARY STEPS

1. **configure**
2. **logging** {*ip-address* | *hostname*}
3. **logging trap** *severity*
4. **logging console** [*severity*]
5. **logging buffered** [*severity* | *buffer-size*]
6. **commit**
7. **end**
8. **show logging**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RP0/CPU0:router# configure`	Enters global configuration mode.
Step 2	**logging** {*ip-address* | *hostname*} **Example:** `RP/0/RP0/CPU0:router(config)# logging 10.1.1.1`	Specifies a syslog server host to use for system logging.
Step 3	**logging trap** *severity* **Example:** `RP/0/RP0/CPU0:router(config)# logging trap debugging`	Limits the logging of messages sent to syslog servers to only those messages at the specified level. • See Table 5-2 for a summary of the logging severity levels.
Step 4	**logging console** [*severity*] **Example:** `RP/0/RP0/CPU0:router(config)# logging console emergencies`	Logs messages on the console. • When a severity level is specified, only messages at that severity level are logged on the console. • See Table 5-2 for a summary of the logging severity levels.

	Command or Action	Purpose
Step 5	**logging buffered** [*severity* | *buffer-size*] **Example:** `RP/0/RP0/CPU0:router(config)# logging buffered 1000000`	Copies logging messages to an internal buffer. • Newer messages overwrite older messages after the buffer is filled. • Specifying a severity level causes messages at that level and numerically lower levels to be logged in an internal buffer. See Table 5-2 for a summary of the logging severity levels. • The buffer size is from 4096 to 4,294,967,295 bytes. Messages above the set limit are logged to the console.
Step 6	**commit** **Example:** `RP/0/RP0/CPU0:router(config)# commit`	Commits the target configuration to the router running configuration.
Step 7	**end** **Example:** `RP/0/RP0/CPU0:router(config)# end`	Ends the configuration session and returns to EXEC mode.
Step 8	**show logging** **Example:** `RP/0/RP0/CPU0:router# show logging`	Displays the messages that are logged in the buffer.

Examples

In the following example, basic message logging is configured:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# logging 10.1.1.1
RP/0/RP0/CPU0:router(config)# logging trap debugging
RP/0/RP0/CPU0:router(config)# logging console emergencies
RP/0/RP0/CPU0:router(config)# logging buffered 1000000
RP/0/RP0/CPU0:router(config)# commit
RP/0/RP0/CPU0:router(config)# end
RP/0/RP0/CPU0:router# show logging
Syslog logging: enabled (162 messages dropped, 0 flushes, 0 overruns)
    Console logging: level emergencies, 593 messages logged
    Monitor logging: level debugging, 0 messages logged
    Trap logging: level debugging, 2 messages logged
    Logging to 10.1.1.1, 2 message lines logged
    Buffer logging: level debugging, 722 messages logged

Log Buffer (1000000 bytes):

RP/0/RP0/CPU0:Apr  8 19:18:58.679 : instdir[203]: %INSTALL-INSTMGR-6-INSTALL_OP
RP/0/RP0/CPU0:Apr  8 19:19:01.287 : instdir[203]: %INSTALL-INSTMGR-6-INSTALL_OP
RP/0/RP0/CPU0:Apr  8 19:22:15.658 : instdir[203]: %INSTALL-INSTMGR-6-INSTALL_OP
LC/0/1/CPU0:Apr  8 19:22:30.122 : sysmgr[74]: %OS-SYSMGR-7-INSTALL_NOTIFICATION
LC/0/6/CPU0:Apr  8 19:22:30.160 : sysmgr[74]: %OS-SYSMGR-7-INSTALL_NOTIFICATION
RP/0/RP0/CPU0:Apr  8 19:22:30.745 : sysmgr[79]: %OS-SYSMGR-7-INSTALL_NOTIFICATI
RP/0/RP1/CPU0:Apr  8 19:22:32.596 : sysmgr[79]: %OS-SYSMGR-7-INSTALL_NOTIFICATI
LC/0/1/CPU0:Apr  8 19:22:35.181 : sysmgr[74]: %OS-SYSMGR-7-INSTALL_FINISHED : s
```

```
LC/0/6/CPU0:Apr  8 19:22:35.223 : sysmgr[74]: %OS-SYSMGR-7-INSTALL_FINISHED : s
RP/0/RP0/CPU0:Apr  8 19:22:36.122 : sysmgr[79]: %OS-SYSMGR-7-INSTALL_FINISHED :
RP/0/RP1/CPU0:Apr  8 19:22:37.790 : sysmgr[79]: %OS-SYSMGR-7-INSTALL_FINISHED :
RP/0/RP0/CPU0:Apr  8 19:22:41.015 : schema_server[332]: %MGBL-SCHEMA-6-VERSIONC
RP/0/RP0/CPU0:Apr  8 19:22:59.844 : instdir[203]: %INSTALL-INSTMGR-4-ACTIVE_SOF
RP/0/RP0/CPU0:Apr  8 19:22:59.851 : instdir[203]: %INSTALL-INSTMGR-6-INSTALL_OP
 --More--
```

Related Documents

For more information on message logging and configuration of alarm correlation, see the following Cisco documents:

Related Topic	Document Title
Configuration of system logging	*Cisco IOS XR System Management Configuration Guide*
Commands used to configure logging	*Cisco IOS XR System Management Command Reference*
Configuration of alarm correlation and generating complex queries	*Cisco IOS XR System Management Configuration Guide*
Commands used to configure alarm correlation	*Cisco IOS XR System Management Command Reference*
Retrieve logging events through an XML interface	*Cisco IOS XR XML API Guide*

Disabling Console Logging

To disable console logging, enter the **logging console disable** command in global configuration mode.

Creating and Modifying User Accounts and User Groups

In the Cisco IOS XR software, users are assigned individual usernames and passwords. Each username is assigned to one or more user groups, each of which defines display and configuration commands the user is authorized to execute. This authorization is enabled by default in the Cisco IOS XR software, and each user must log in to the system using a unique username and password.

The following sections describe the basic commands used to configure users and user groups. For a summary of user accounts, user groups, and task IDs, see the "User Access Privileges" section on page 4-14.

Note The management of user accounts, user groups, and task IDs is part of the "AAA" feature in the Cisco IOS XR software. AAA stands for "authentication, authorization, and accounting," a suite of security features included in the Cisco IOS XR software. For more information on the AAA concepts and configuration tasks, see *Cisco IOS XR System Security Configuration Guide* and *Cisco IOS XR System Security Command Reference.* For instructions to activate software packages, see *Cisco IOS XR System Management Configuration Guide, Release 3.4*

Displaying Details About User Accounts, User Groups, and Task IDs

Table 5-3 summarizes the EXEC mode commands used to display details about user accounts, user groups, and task IDs.

Table 5-3 Commands to Display Details About Users and User Groups

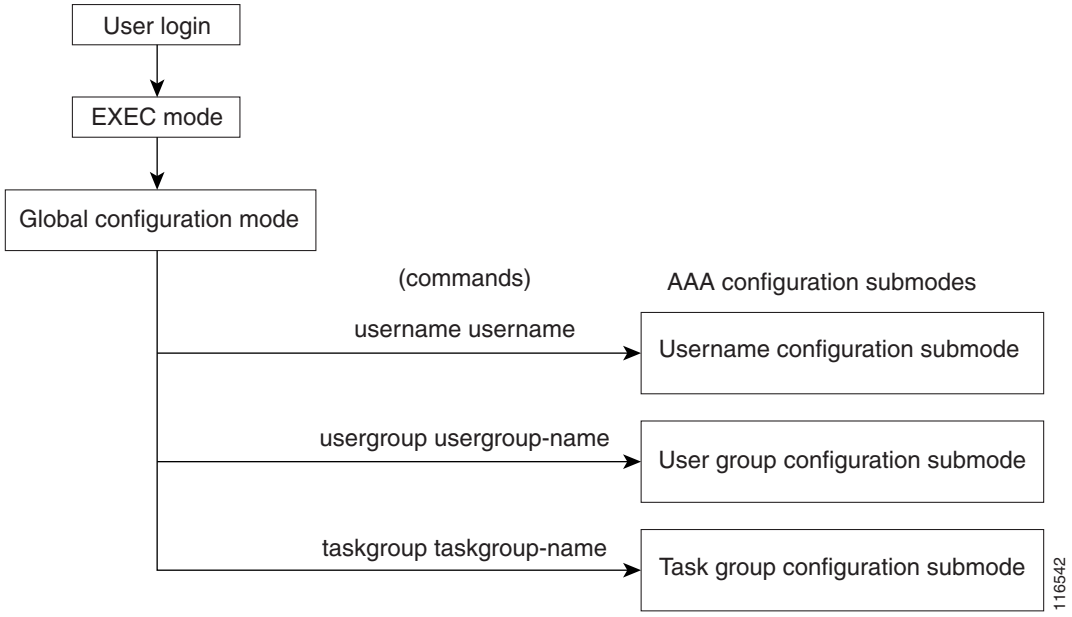
Command	Description
show aaa userdb *username*	Displays the task IDs and privileges assigned to a specific username. To display all users on the system, enter the command without a username.
show aaa usergroup *usergroup-name*	Displays the task IDs and privileges that belong to a user group. To display all groups on the system, enter the command without a group name.
show task supported	Displays all task IDs for the system. Only the root-system users, root-lr users, or users associated with the WRITE:AAA task ID can configure task groups.

Configuring User Accounts

User accounts, user groups, and task groups are created by entering the appropriate commands in one of the "AAA" configuration submodes, as shown in Figure 5-1.

This section describes the process to configure usernames. For instructions to configure user groups, task groups, and other AAA security features, see the *Cisco IOS XR System Security Configuration Guide.*

Figure 5-1 AAA Configuration Submodes



Creating Users and Assigning Groups

To create a user, assign a password, and assign the user to a group, perform the following procedure:

SUMMARY STEPS

1. **configure**
2. **username** *user-name*
3. **password** {**0** | **7**} *password*
   or
   secret {**0** | **5**} *password*
4. **group** *group-name*
5. Repeat Step 4 for each user group to be associated with the user specified in Step 2.
6. **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RP0/CPU0:router# configure`	Enters global configuration mode.
Step 2	**username** *user-name* **Example:** `RP/0/RP0/CPU0:router(config)# username user1`	Creates a name for a new user (or identifies a current user) and enters username configuration submode. • The *user-name* argument can be only one word. Spaces and quotation marks are not allowed.

Step 3	**password** {**0** | **7**} *password*
	or
	secret {**0** | **5**} *password*
	
	Example:
	`RP/0/RP0/CPU0:router(config-un)# password 0 pwd1`
	or
	`RP/0/RP0/CPU0:router(config-un)# secret 5 pwd1`
		Specifies a password for the user named in Step 2.
		• Use the **secret** command to create a secure login password for the user names specified in Step 2.
		• Entering **0** following the **password** command specifies that an unencrypted (clear-text) password follows. Entering **7** following the **password** command specifies that an encrypted password follows.
		• Entering **0** following the **secret** command specifies that a secure unencrypted (clear-text) password follows. Entering **5** following the **secret** command specifies that a secure encrypted password follows.
		• Type **0** is the default for the **password** and **secret** commands.

	Command or Action	Purpose
Step 4	**group** *group-name* **Example:** `RP/0/RP0/CPU0:router(config-un)# group sysadmin`	Assigns the user named in Step 2 to a user group. • The user takes on all attributes of the user group, as defined by the user group association to various task groups. • Each user must be assigned to at least one user group. A user may belong to multiple user groups.
Step 5	Repeat Step 4 for each user group to be associated with the user specified in Step 2.	—
Step 6	**commit** **Example:** `RP/0/RP0/CPU0:router(config-un)# commit`	Saves configuration changes and activates them as part of the running configuration.

Related Documents

For more information on configuration and management of users and user access privileges, see the following Cisco documents:

Related Topic	Document Title
Create users, assign users to user groups, create and modify user groups, and configure remote AAA access	*Cisco IOS XR System Security Configuration Guide*

Configuration Limiting

The Cisco IOS XR software places preset limits on the configurations you can apply to the running configuration of a router. These limits ensure that the router has sufficient system resources (such as RAM) for normal operations. Under most conditions, these preset limits are sufficient.

In some cases, for which a large number of configurations is required for a particular feature, it may be necessary to override the preset configuration limits. This override can be done only if configurations for another feature are low or unused. For example, if a router requires a large number of BGP configurations and Multiprotocol Label Switching (MPLS) is not being used at all, then the BGP limits can be increased to use the unused memory assigned to MPLS.

Caution Overriding the default configuration limits can result in a low-memory condition.

The following sections describe the limits you can configure, default and maximum values, and commands for configuring and displaying the configuration limits:

Static Route Configuration Limits

Table 5-4 summarizes the maximum limits for static routes, including the commands used to display and change the limits.

Table 5-4 Static Route Configuration Limits and Commands

Feature Limit Description	Default Maximum Limit	Absolute Maximum Limit	Configuration Command (Static Router Configuration Mode)	Show Current Settings Command (EXEC or Global Configuration Mode)
Maximum static IPv4 routes	4000	40,000	**maximum path ipv4** *n*	**show running-config router static**
Maximum static IPv6 routes	4000	40,000	**maximum path ipv6** *n*	**show running-config router static**

Examples

In the following example, the maximum number of static IPv4 routes is changed to 5000 and the new configuration is displayed.

```
RP/0/RP1/CPU0:router# configure
RP/0/RP1/CPU0:router(config)# router static
RP/0/RP1/CPU0:router(config-static)# maximum path ipv4 5000
RP/0/RP1/CPU0:router(config-static)# commit
RP/0/RP1/CPU0:router(config-static)# show running-config router static

router static
 maximum path ipv4 5000
 address-family ipv4 unicast
  0.0.0.0/0 172.29.52.1
 !
!
```

IS-IS Configuration Limits

Table 5-5 summarizes the maximum limits for IS-IS, including the commands used to display and change the limits.

Table 5-5 IS-IS Configuration Limits and Commands

Feature Limit Description	Default Maximum Limit	Absolute Maximum Limit	Configuration Command (Address Family Configuration Mode)	Show Current Settings Command (EXEC Mode)
Maximum number of prefixes redistributed into IS-IS	10,000	28,000	**maximum-redistributed-prefixes** *n*	**show isis adjacency**
Number of active parallel paths for each route on a Cisco CRS-1 router	8	32	**maximum-paths** *n*	**show isis route**
Number of active parallel paths for each route on a Cisco XR 12000 Series Router	8	16	**maximum-paths** *n*	**show isis route**

Examples

In the following example, the maximum number of active parallel paths for each route is increased to 10, and the maximum number of prefixes redistributed into IS-IS is increased to 12,000:

```
RP/0/RP1/CPU0:router# configure
RP/0/RP1/CPU0:router(config)# router isis 100 address-family ipv4
RP/0/RP1/CPU0:router(config-isis-af)# maximum-paths 10
RP/0/RP1/CPU0:router(config-isis-af)# maximum-redistributed-prefixes 12000
RP/0/RP1/CPU0:router(config-isis-af)# commit
RP/0/RP1/CPU0:Mar 30 14:11:07 : config[65739]: %LIBTARCFG-6-COMMIT : Configurati
on committed by user 'cisco'.   Use 'show configuration commit changes 1000000535' to view
the changes.
RP/0/RP1/CPU0:router(config-isis-af)#
```

OSPFv2 and v3 Configuration Limits

Table 5-6 summarizes the maximum limits for OSPF, including the commands used to display and change the limits.

Table 5-6 OSPFv2 and OSPFv3 Configuration Limits and Commands

Feature Limit Description	Default Maximum Limit	Absolute Maximum Limit	Configuration Command (Router Configuration Mode)	Show Current Settings Command (EXEC Mode)
Maximum number of interfaces that can be configured for an OSPF instance	255	1024	**maximum interfaces** *n*	**show ospf**
Maximum routes redistributed into OSPF	10,000	28,672	**maximum redistributed-prefixes** *n*	**show ospf** **Note** The maximum number of redistributed prefixes is displayed only if redistribution is configured.
Maximum number of parallel routes (maximum paths) on Cisco CRS-1 routers	32 (OSPFv2) 16 (OSPFv3)	32	**maximum paths** *n*	**show running-config router ospf** **Note** This command shows only changes to the default value. If the **maximum paths** command does not appear, the router is set to the default value.
Maximum number of parallel routes (maximum paths) on a Cisco XR 12000 Series Router	16	16	**maximum paths** *n*	**show running-config router ospf** **Note** This command shows only changes to the default value. If the **maximum paths** command does not appear, the router is set to the default value.

Examples

The following subsections provide the following examples:

- Maximum Interfaces for Each OSPF Instance, page 5-19
- Maximum Routes Redistributed into OSPF, page 5-20
- Number of Parallel Links (max-paths), page 5-21

Maximum Interfaces for Each OSPF Instance

In the following example, the **show ospf** command is used to display the maximum number of OSPF interfaces:

```
RP/0/RP1/CPU0:router# show ospf
 Routing Process "ospf 100" with ID 0.0.0.0
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 It is an area border router
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Initial LSA throttle delay 500 msecs
 Minimum hold time for LSA throttle 5000 msecs
```

```
 Maximum wait time for LSA throttle 5000 msecs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Maximum number of configured interfaces 255
--More--
```

The following example configures the maximum interface limit on a router:

```
RP/0/RP1/CPU0:router# configure
RP/0/RP1/CPU0:router(config)# router ospf 100
RP/0/RP1/CPU0:router(config-router)# maximum interfaces 600
RP/0/RP1/CPU0:router(config-router)# end
Uncommitted changes found, commit them? [yes]: y
RP/0/RP1/CPU0:Mar 30 16:12:39 : config[65740]: %LIBTARCFG-6-COMMIT : Configurati
on committed by user 'cisco'.   Use 'show configuration commit changes 1000000540' to view
the c
hanges.
RP/0/RP1/CPU0:Mar 30 16:12:39 : config[65740]: %SYS-5-CONFIG_I : Configured from
 console by cisco

RP/0/RP1/CPU0:router# show ospf

 Routing Process "ospf 100" with ID 0.0.0.0
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 It is an area border router
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Initial LSA throttle delay 500 msecs
 Minimum hold time for LSA throttle 5000 msecs
 Maximum wait time for LSA throttle 5000 msecs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Maximum number of configured interfaces 600
--More--
```

Maximum Routes Redistributed into OSPF

In the following example, the **maximum redistributed-prefixes** command is used to set the maximum routes redistributed into OSPF:

```
RP/0/RP1/CPU0:router# configure
RP/0/RP1/CPU0:router(config)# router ospf 100
RP/0/RP1/CPU0:router(config-router)# maximum redistributed-prefixes 12000
RP/0/RP1/CPU0:router(config-router)# end
Uncommitted changes found, commit them? [yes]: y
RP/0/RP1/CPU0:Mar 30 16:26:52 : config[65740]: %LIBTARCFG-6-COMMIT : Configurati
on committed by user 'cisco'.   Use 'show configuration commit changes 1000000541' to view
the changes.
RP/0/RP1/CPU0:Mar 30 16:26:52 : config[65740]: %SYS-5-CONFIG_I : Configured from
 console by cisco
RP/0/RP1/CPU0:router#
```

Number of Parallel Links (max-paths)

In the following example, the **maximum paths** command is used to set the maximum number of parallel routes:

```
RP/0/RP1/CPU0:router# configure
RP/0/RP1/CPU0:router(config)# router ospf 100
RP/0/RP1/CPU0:router(config-router)# maximum paths 10
RP/0/RP1/CPU0:router(config-router)# end
Uncommitted changes found, commit them? [yes]: y
RP/0/RP1/CPU0:Mar 30 18:05:13 : config[65740]: %LIBTARCFG-6-COMMIT : Configurati
on committed by user 'cisco'.   Use 'show configuration commit changes 1000000542' to view
the changes.
RP/0/RP1/CPU0:Mar 30 18:05:13 : config[65740]: %SYS-5-CONFIG_I : Configured from
 console by cisco
RP/0/RP1/CPU0:router#
```

BGP Configuration Limits

The maximum number of BGP neighbors (peers) that can be configured is 1024. This number cannot be changed through configuration. Any attempt to configure additional neighbors beyond the limit fails.

To prevent neighbors (peers) from flooding BGP with advertisements, a limit is placed on the number of prefixes that can be accepted from a peer for each supported address family.

You can override the default limits for an address family with the **maximum-prefix** command. Table 5-7 summarizes the maximum configuration limits for BGP.

Table 5-7 BGP Configuration Limits and Commands

Feature Limit Description	Default Maximum Limit	Absolute Maximum Limit	Configuration Command (Router Configuration Mode)	Show Current Settings Command (EXEC Mode)
Maximum number of neighbors (peers)	1024	1024	None. This limit cannot be changed or exceeded.	None
IPv4 unicast maximum prefixes that can be received from a neighbor	524,288	4,294,967,295	**maximum-prefix** *n*	**show bgp neighbor** *IP_address*
IPv4 multicast maximum prefixes that can be received from a neighbor	131,072	4,294,967,295	**maximum-prefix** *n*	**show bgp neighbor** *IP_address*
IPv6 unicast maximum prefixes that can be received from a neighbor	131,072	4,294,967,295	**maximum-prefix** *n*	**show bgp neighbor** *IP_address*
Maximum equal-cost parallel routes to external peers	1	8	**maximum-paths** *n*	**show running-config** **Note** This command shows only changes to the default value. If the **maximum paths** command does not appear, the router is set to the default value.

A cease-notification message is sent to the neighbor and the peering with the neighbor is terminated when the number of prefixes received from the peer for a given address family exceeds the maximum limit (either set by default or configured by the user) for that address family.

However, if the **warning-only** keyword (for the **maximum-prefix** command) is configured, the Cisco IOS XR software sends only a log message, but continues peering with the sender. If the peer is terminated, the peer stays down until the **clear bgp** command is issued.

The same set of actions (sending cease notification followed by the termination of the peering) is taken for a neighbor with which peering has already been established if you decide to configure a maximum that is less than the number of prefixes that have already been received from the neighbor.

Examples

The following example shows how to set the BGP configuration limits:

```
RP/0/RP1/CPU0:router# configure
RP/0/RP1/CPU0:router(config)# router bgp 100
RP/0/RP1/CPU0:router(config-bgp)# neighbor 10.1.1.1
RP/0/RP1/CPU0:router(config-bgp-nbr)# remote-as 1
RP/0/RP1/CPU0:router(config-bgp-nbr)# address-family ipv4 unicast
RP/0/RP1/CPU0:router(config-bgp-nbr-af)# maximum-paths 4
RP/0/RP1/CPU0:router(config-bgp-nbr-af)# maximum-prefix 100000
RP/0/RP1/CPU0:router(config-bgp-nbr-af)# commit
RP/0/RP1/CPU0:Mar 30 19:13:16 : config[65740]: %LIBTARCFG-6-COMMIT : Configurati
on committed by user 'cisco'.   Use 'show configuration commit changes 1000000544' to view
the c
hanges.
RP/0/RP1/CPU0:Mar 30 19:13:17 : config[65740]: %SYS-5-CONFIG_I : Configured from
 console by cisco
RP/0/RP1/CPU0:router(config-bgp-nbr-af)#
```

Routing Policy Language Line and Policy Limits

Two limits for Routing Policy Language (RPL) configurations exist:

1. Lines of configuration: The number of lines entered by the user, including the beginning and ending statements (that is “route-policy”). The lines of configuration for sets are also included.
2. Number of RPL policies: The number of policies that can be configured on the router. Policies are counted only once: Multiple use of the same policy counts as a single policy toward the limit 1.

The limits for RPL lines and policies are summarized in Table 5-8. You can change the default values up to the absolute maximum, but you cannot change the value to a number less than the number of items that are currently configured.

Table 5-8 Maximum Lines of RPL: Configuration Limits and Commands

Limit Description	Default Maximum Limit	Absolute Maximum Limit	Configuration Command (Global Configuration Mode)	Show Current Settings Command (EXEC Mode)
Maximum number of RPL lines	65,536	131,072	**rpl maximum lines** *n*	**show rpl maximum lines**
Maximum number of RPL policies	3500	5000	**rpl maximum policies** *n*	**show rpl maximum policies**

Examples

In the following example, the **show rpl maximum** command is used in EXEC mode to display the current setting for RPL limits and number of each limit currently in use. A summary of the memory used by all of the defined policies is also shown below the limit settings.

```
RP/0/RP1/CPU0:router# show rpl maximum

                             Current    Current       Max
                              Total      Limit       Limit
-------------------------------------------------------------
Lines of configuration            0      65536     131072
Policies                          0       3500       5000
Compiled policies size (kB)       0
RP/0/RP1/CPU0:router#
```

In the next example, the **rpl maximum** command changes the currently configured line and policy limits. The **show rpl maximum** command displays the new settings.

```
RP/0/RP1/CPU0:router# configure
RP/0/RP1/CPU0:router(config)# rpl maximum policies 4000
RP/0/RP1/CPU0:router(config)# rpl maximum lines 80000
RP/0/RP1/CPU0:router(config)# commit
RP/0/RP1/CPU0:Apr  1 00:23:44.062 : config[65709]: %LIBTARCFG-6-COMMIT : Configu
ration committed by user 'UNKNOWN'.   Use 'show configuration commit changes 1000000010'
to vi
ew the changes.
RP/0/RP1/CPU0:router(config)# exit
RP/0/RP1/CPU0:Apr  1 00:23:47.781 : config[65709]: %SYS-5-CONFIG_I : Configured
from console by console
RP/0/RP1/CPU0:router# show rpl maximum

                             Current    Current       Max
                              Total      Limit       Limit
-------------------------------------------------------------
Lines of configuration            0      80000     131072
Policies                          0       4000       5000
Compiled policies size (kB)       0
RP/0/RP1/CPU0:router#
```

Multicast Configuration Limits

Table 5-9 summarizes the maximum limits for multicast configuration, including the commands used to display and change the limits.

Table 5-9 Multicast Configuration Limits and Commands

Feature Limit Description	Default Maximum Limit	Absolute Maximum Limit	Configuration Command	Show Current Settings Command (EXEC Mode)
Internet Group Management Protocol (IGMP) Limits				
Maximum number of groups used by IGMP and accepted by a router	50,000	75,000	**maximum groups** *n* (router IGMP configuration mode)	**show igmp summary**
Maximum number of groups for each interface accepted by a router	20,000	40,000	**maximum groups** *n* (router IGMP interface configuration mode)	**show igmp summary**
Multicast Source Discovery Protocol (MSDP) Limits				
Maximum MSDP Source Active (SA) entries	20,000	75,000	**maximum external-sa** *n* (router MSDP configuration mode)	**show msdp summary**
Maximum MSDP SA entries that can be learned from MSDP peers	20,000	75,000	**maximum peer-external-sa** *n* (router MSDP configuration mode)	**show msdp summary**
Protocol Independent Multicast (PIM) Limits				
Maximum PIM routes supported	100,000	200,000	**maximum routes** *n* (router PIM configuration mode)	**show pim summary**
Maximum PIM egress states	300,000	600,000	**maximum route-interfaces** *n* (router PIM configuration mode)	**show pim summary**
Maximum PIM registers	20,000	75,000	**maximum register-states** *n* (router PIM configuration mode)	**show pim summary**
Maximum number of PIM group map ranges learned from Auto-RP	500	5000	**maximum group-mappings autorp** *n* (router PIM configuration mode)	**show pim summary**

MPLS Configuration Limits

Table 5-10 summarizes the maximum limits for MPLS configuration, including the commands used to display and change the limits.

Table 5-10 MPLS Configuration Limits and Commands

Limit Description	Default Maximum Limit	Absolute Maximum Limit	Configuration Command (Global Configuration Mode)	Show Current Settings Command (EXEC Mode)
Maximum traffic engineer (TE) tunnels head	2500	65536	**mpls traffic-eng maximum tunnels** *n*	**show mpls traffic-eng maximum tunnels**

Other Configuration Limits

Table 5-11 summarizes the maximum limits for additional configuration limits, including the commands used to display and change the limits.

Table 5-11 Additional Configuration Limits and Commands

Limit Description	Default Maximum Limit	Absolute Maximum Limit	Configuration Command (Global Configuration Mode)	Show Current Settings Command (EXEC Mode)
IPv4 ACL (access list and prefix list)	5000	16000	**ipv4 access-list maximum acl threshold** *n*	**show access-lists ipv4 maximum**
IPv4 ACE (access list and prefix list)	200,000	350,000	**ipv4 access-list maximum ace threshold** *n*	**show access-lists ipv4 maximum**
IPv6 ACL (access list and prefix list)	1000	16000	**ipv6 access-list maximum acl threshold** *n*	**show access-lists ipv6 maximum**
IPv6 ACE (access list and prefix list)	50,000	350,000	**ipv6 access-list maximum ace threshold** *n*	**show access-lists ipv6 maximum**

CHAPTER 6

CLI Tips, Techniques, and Shortcuts

This chapter describes techniques for using the command-line interface (CLI) of the Cisco IOS XR software.

Contents

The chapter contains the following sections:

Note Commands can be entered in uppercase, lowercase, or mixed case. Only passwords are case sensitive. However, the Cisco Systems documentation convention presents commands in lowercase.

CLI Tips and Shortcuts

The following sections describe tips and shortcuts useful when using the CLI:

Entering Abbreviated Commands

You can abbreviate commands and keywords to the number of characters that allow a unique abbreviation. For example, the **configure** command can be abbreviated as **config** because the abbreviated form of the command is unique. The router accepts and executes the abbreviated command.

Using the Question Mark (?) to Display On-Screen Command Help

Use the question mark (**?**) to learn what commands are available and the correct syntax for a command. Table 6-1 summarizes the options for on-screen help.

Tip The space (or lack of a space) before the question mark (**?**) is significant. If you include a space before the question mark, the system displays all available options for a command or CLI mode. If you do not include a space, the system displays a list of commands that begin with a particular character string.

Table 6-1 On-Screen Help Commands

Command	Description

partial-command?	Enter a question mark (**?**) at the end of a partial command to list the commands that begin with those characters.
	`RP/0/RP0/CPU0:router# co?`
	`configure copy`
	Note Do not include a space between the command and question mark.

?	Lists all commands available for a particular command mode.

command ?	Include a space before the question mark (**?**) to list the keywords and arguments that belong to a command.
	`RP/0/RP0/CPU0:router# configure ?`
	`exclusive Configure exclusively from this terminal`
	`terminal Configure from the terminal`
	`<cr>`
	Note For most commands, the `<cr>` symbol indicates that you can execute the command with the syntax already entered. For the preceding example, press **Return** to enter global configuration mode.

command keyword ?	Enter a question mark (?) after the keyword to list the next available syntax option for the command.
	`RP/0/RP0/CPU0:router# show aaa ?`
	`taskgroup Show all the local taskgroups configured in the system`
	`userdb Show all local users with the usergroups each belong to`
	`usergroup Show all the local usergroups configured in the system`
	Note Include a space between the keyword and question mark.

The following example shows how to add an entry to access list 99. The added entry denies access to all hosts on subnet 172.0.0.0 and ignores bits for IPv4 addresses that start within the range of 0 to 255. The following steps provide an example of on-screen command help:

Step 1 Enter the **access-list** command, followed by a space and a question mark, to list the available options for the command:

```
RP/0/0/CPU0:router(config)# ipv4 access-list ?

  log-update  Control access lists log updates
  maximum     Out of resources configration
  WORD        Access list name - maximum 32 characters
```

Note The number ranges (within the angle brackets) are inclusive ranges.

Step 2 Enter the access list name **list1**, followed by a space and another question mark, to display the arguments that apply to the keyword and brief explanations:

```
RP/0/0/CPU0:router(config)# ipv4 access-list list1 ?

  <1-2147483646>  Sequence number for this entry
  deny            Specifies packets to reject
  permit          Specifies packets to forward
  remark          Comment for access list
  <cr>
RP/0/0/CPU0:router(config)#ipv4 access-list list1
```

Step 3 Enter the **deny** option and a question mark to see more command options:

```
RP/0/0/CPU0:router(config)#ipv4 access-list list1 deny ?

  <0-255>  An IPv4 Protocol Number
  A.B.C.D  Source IP address or prefix
  ahp      Authentication Header Protocol
  any      Any source host
  eigrp    Cisco's EIGRP Routing Protocol
  esp      Encapsulation Security Payload
  gre      Cisco's GRE Tunneling
  host     A single source host
  icmp     Internet Control Message Protocol
  igmp     Internet Gateway Message Protocol
  igrp     Cisco's IGRP Routing Protocol
  ipinip   IP in IP tunneling
  ipv4     Any IPv4 Protocol
  nos      KA9Q NOS Compatible IP over IP Tunneling
  ospf     OSPF Routing Protocol
  pcp      Payload Compression Protocol
  pim      Protocol Independent Multicast
  sctp     Stream Control Transmission Protocol
  tcp      Transport Control Protocol
  udp      User Datagram Protocol
RP/0/0/CPU0:router(config)#ipv4 access-list list1 deny
```

Generally, uppercase letters represent variables (arguments).

Step 4 Enter an IP address, followed by a space and a question mark (?), to list additional options:

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list list1 deny 172.31.134.0 ?

  A.B.C.D    Wildcard bits
  log        Log matches against this entry
  log-input  Log matches against this entry, including input interface
  <cr>

RP/0/RP0/CPU0:router(config)# ipv4 access-list list1 deny 172.31.134.0
```

The <cr> symbol by itself indicates that there are no more keywords or arguments.

Step 5 Press **Return** to execute the command:

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list list1 deny 172.31.134.0
```

Note The configuration does not become active until you enter the **commit** command to add the target configuration to the running configuration.

Completing a Partial Command with the Tab Key

If you cannot remember a complete command name or want to reduce the amount of typing you have to perform, enter the first few letters of the command, then press the Tab key. If only one command begins with that character string, the system completes the command for you. If the characters you entered indicate more than one command, the system beeps to indicate that the text string is not unique and the system provides a list of commands that match the text entered.

In the following example, the CLI recognizes **conf** as a unique string in EXEC mode and completes the command when Tab is pressed:

```
RP/0/RP0/CPU0:router# conf<Tab>

RP/0/RP0/CPU0:router# configure
```

The CLI displays the full command name. You must then press **Return** to execute the command. This feature allows you to modify or reject the suggested command.

In the next example, the CLI recognizes two commands that match the text entered:

```
RP/0/RP1/CPU0:router#co<Tab>
configure  copy
RP/0/RP1/CPU0:router#con<Tab>
RP/0/RP1/CPU0:router#configure
```

Tip If your keyboard does not have a Tab key, press Ctrl-I instead.

Identifying Command Syntax Errors

If an incorrect command is entered, an error message is returned with the caret (^) at the point of the error. In the following example, the caret appears where the character was typed incorrectly in the command:

```
RP/0/0/CPU0:router# configure termiMal
                                   ^
% Invalid input detected at '^' marker.
```

Note The percent sign (%) indicates the line in which the error message occurred.

To display the correct command syntax, enter the "?" after the command:

```
RP/0/0/CPU0:router# configure ?
  exclusive  Configure exclusively from this terminal
  terminal   Configure from the terminal
  <cr>
```

Using the no Form of a Command

Almost every configuration command has a **no** form. Depending on the command, the **no** form may enable or disable a feature. For example, when configuring an interface, the **no shutdown** command brings up the interface, and the **shutdown** command shuts down the interface. The **username** command creates a new user, and the **no username** command deletes a user when entered with a valid username.

The Cisco IOS XR software command reference publications provide the complete syntax for the configuration commands and describe what the **no** form of a command does. See the "Related Documents" section on page x for more information.

Editing Command Lines that Wrap

The CLI provides a wraparound feature for commands that extend beyond a single line on the screen. When the cursor reaches the right margin, the command line shifts ten spaces to the left. The first ten characters of the line are not shown, but it is possible to scroll back and check the syntax at the beginning of the command. To scroll back, press Ctrl-B or the left arrow key repeatedly, or press Ctrl-A to return directly to the beginning of the line.

In the following example, the **ipv4 access-list** command entry is too long to display on one line. When the cursor reaches the end of the line, the line is shifted to the left and redisplayed. The dollar sign ($) after the command prompt indicates that the line has been scrolled to the left and the beginning of the command is hidden.

```
RP/0/0/CPU0:router(config)# $s-list 101 permit tcp 172.31.134.5 255.255.255.0 172.31.135.0
```

In the next example, Ctrl-A is used to display the beginning of the command line, and the dollar sign at the end of the command line shows the command has been scrolled to the right and the end of the command is hidden.

```
RP/0/0/CPU0:router(config)# ipv4 access-list 101 permit tcp 172.31.134.5 255.255.255.0 17$
```

In the next example, the right arrow key has been used to scroll to the right. Notice that dollar sign symbols appear at both ends of the line, which indicates that command information is hidden from the beginning and end of the command.

```
RP/0/0/CPU0:router(config)# $ccess-list 101 permit tcp 172.31.134.5 255.255.255.0 172.31.$
```

By default, the Cisco IOS XR software uses a terminal screen 80 columns wide. To adjust for a different screen width, use the **terminal width** command in EXEC mode.

Use line wrapping with the command history feature to recall and modify previous complex command entries.

Displaying System Information with show Commands

The **show** commands display information about the system and its configuration. The following sections describe some common **show** commands and provide techniques to manage the output from those commands:

Common show Commands

Some of the most common **show** commands are described in Table 6-2.

Table 6-2 Common show Commands in Cisco IOS XR Software

Command	Description	Command Mode
show version	Displays system information.	EXEC or administration EXEC mode
show configuration	Displays the uncommitted configuration changes made during a configuration session.	Global or administration configuration mode
show running-config (EXEC or global configuration mode)	Displays the current running configuration for the SDR to which you are connected.	EXEC or global configuration mode
show running-config (administration EXEC or administration configuration mode)	Displays the current running configuration that applies to the entire router or multishelf system.	administration EXEC or administration configuration mode

Table 6-2 Common show Commands in Cisco IOS XR Software (continued)

Command	Description	Command Mode
show tech-support	Collects a large amount of system information for troubleshooting. You can provide this output to technical support representatives when reporting a problem.	EXEC or administration EXEC mode
show platform (EXEC mode)	Displays information about cards and modules assigned to the SDR to which you are connected.	EXEC mode
show platform (administration EXEC mode)	Displays information about all cards and modules in the router.	administration EXEC mode
show environment	Displays hardware information for the system, including fans, LEDs, power supply voltage and current, and temperatures. Enter **show environment ?** to see additional command options.	EXEC mode or administration EXEC mode

For more information on the use of these commands, see the "Related Documents" section on page x.

Browsing Display Output when the --More-- Prompt Appears

When command output requires more than one screen, such as for the **?**, **show**, or **more** command, the output is presented one screen at a time, and a `--More--` prompt is displayed at the bottom of the screen.

To display additional command output, do one of the following:

- Press **Return** to display the next line.
- Press the space bar to display the next screen of output.

The following example shows one screen of data and the `--More--` prompt:

```
RP/0/RP0/CPU0:router# show ?

  aaa                   Show AAA configuration and operational data
  adjacency             Adjacency information
  aliases               Display alias commands
  alphadisplay          Shows the message being displayed on the alpha display
  aps                   SONET APS information
  arm                   IP ARM information
  arp                   ARP table
  as-path-access-list   List AS path access lists
  asic-errors           ASIC error information
  atc                   Attractor Cache related
  auto-rp               Auto-RP Commands
  bgp                   BGP show commands
  buffer-manager        Show all buffer manager memory related information
  bundle                Show hardware related information for Bundles.
  calendar              Display the system calendar
  cdp                   CDP information
  cef                   Cisco Express Forwarding
  cetftp                HFR control plane ethernet TFTP server
  checkpoint            Show checkpoint services
  cinetd                cinetd daemon
  clns                  Display CLNS related information
  clock                 Display the system clock
  commit                Show commit information
 --More--
```

Tips If you do not see the `--More--` prompt, try entering a value for the screen length with the **terminal length** command in EXEC mode. Command output is not paused if the **length** value is set to zero. The following example shows how to set the terminal length:

```
RP/0/RP1/CPU0:router# terminal length 20
```

For information on searching or filtering CLI output, see the "Filtering show Command Output" section on page 6-10.

Halting the Display of Screen Output

To interrupt screen output and terminate a display, press Ctrl-C, as shown in the following example:

```
RP/0/RP0/CPU0:router# show running-config
<Ctrl-C>
```

Redirecting Output to a File

By default, CLI command output is displayed on screen. CLI command output can be redirected to a user-specified file by entering a filename and location after the **show** command syntax. The following command syntax is used to redirect output to a file:

show *command* | `file` *filename*

This feature enables you to save any **show** command output in a file for further analysis and reference. When you choose to redirect command output, consider the following guidelines:

- If the full path of the file is not specified, the default directory for your account is used. You should always save your target configuration files to this location.
- If the saved output is to be used as a configuration file, the filename should end with the `cfg` suffix for easy identification. This suffix is not required, but can help locate target configuration files. Example: `myconfig.cfg`

In the following example, a target configuration file is saved to the default user directory:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# show configure | file disk0:myconfig.cfg
RP/0/RP0/CPU0:router(config)# abort
RP/0/RP0/CPU0:router#
```

Narrowing Output from Large Configurations

Displaying a large running configuration can produce thousands of lines of output. To limit the output of a **show** command to only the items you want to view, use the procedures in the following sections:

- Limiting show Command Output to a Specific Feature or Interface, page 6-9
- Using Wildcards to Display All Instances of an Interface, page 6-9

Limiting show Command Output to a Specific Feature or Interface

Entering keywords and arguments in the **show** command limits the **show** output to a specific feature or interface.

In the following example, only information about the static IP route configuration is displayed:

```
RP/0/RP1/CPU0:router# show running-config router static
router static
 address-family ipv4 unicast
  0.0.0.0/0 10.21.0.1
  0.0.0.0/0 pos0/1/0/1 10.21.0.1
 !
!
```

In the following example, the configuration for a specific interface is displayed:

```
RP/0/RP0/CPU0:router# show running-config interface POS 0/1/0/1

interface pos0/1/0/1
 ipv4 address 10.21.54.31 255.255.0.0
 !
```

Using Wildcards to Display All Instances of an Interface

To display the configuration for all instances, enter the asterisk (*) wildcard character.

Note See the "Using Wildcards to Identify Interfaces in show Commands" section on page 6-11 for more information.

In the following example, a configuration for all Packet-over-SONET/SDH (POS) interfaces is displayed:

```
RP/0/RP1/CPU0:router# show running-config interface pos *

interface POS0/1/0/0
 ipv4 address 10.2.3.4 255.255.255.0
 pos
  crc 32
 !
 shutdown
 keepalive disable
!
interface POS0/1/0/1
 ipv4 address 10.2.3.5 255.255.255.0
 pos
  crc 32
 !
 shutdown
 keepalive disable
!
interface POS0/1/0/2
 ipv4 address 10.2.3.6 255.255.255.0
 pos
  crc 32
 !
 shutdown
 keepalive disable
!
```

```
interface POS0/1/0/3
 ipv4 address 10.2.3.7 255.255.255.0
 pos
  crc 32
 !
 shutdown
 keepalive disable
!

 --More--
```

Filtering show Command Output

Output from the **show** commands can generate a large amount of data. To display only a subset of information, enter the "pipe" character (|) followed by a keyword (**begin**, **include**, **exclude**, or **file)** and a regular expression. Table 6-3 shows the filtering options for the **show** command.

Table 6-3 show Command Filter Options

Command	Description
show *command* | **begin** *regular-expression*	Begins unfiltered output of the **show** command with the first line that contains the regular expression.
show *command* | **exclude** *regular-expression*	Displays output lines that do not contain the regular expression.
show *command* | **include** *regular-expression*	Displays output lines that contain the regular expression.
show *command* | **file** *device0:path/file*	Writes the output lines that contain the regular expression to the specified file on the specified device.

In the following example, the **show interface** command includes only lines in which the expression "protocol" appears:

```
RP/0/RP0/CPU0:router# show interface | include protocol

Null0 is up, line protocol is up
0 drops for unrecognized upper-level protocol
POS0/2/0/0 is administratively down, line protocol is administratively down
0 drops for unrecognized upper-level protocol
POS0/2/0/1 is administratively down, line protocol is administratively down
0 drops for unrecognized upper-level protocol
POS0/2/0/2 is administratively down, line protocol is administratively down
0 drops for unrecognized upper-level protocol
POS0/2/0/3 is administratively down, line protocol is administratively down
0 drops for unrecognized upper-level protocol
MgmtEthernet0/RP0/CPU0/0 is administratively down, line protocol is administratively
down
MgmtEthernet0/RP0/CPU0/0 is administratively down, line protocol is administratively
down
0 drops for unrecognized upper-level protocol
```

Note Filtering is available for submodes, complete commands, and anywhere that <cr> appears in the "**?**" output.

Adding a Filter at the --More-- Prompt

You can specify a filter at the `--More--` prompt of a **show** command output by entering a forward slash (/) followed by a regular expression. The filter remains active until the command output finishes or is interrupted (using Ctrl-Z or Ctrl-C). The following rules apply to this technique:

- If a filter is specified at the original command or previous `--More--` prompt, a second filter cannot be applied.
- The use of the keyword **begin** does not constitute a filter.
- The minus sign (–) preceding a regular expression displays output lines that do not contain the regular expression.
- The plus sign (+) preceding a regular expression displays output lines that contain the regular expression.

In the following example, the user adds a filter at the `--More--` prompt to show only the lines in the remaining output that contain the regular expression "ip."

```
RP/0/RP0/CPU0:router# show configuration running | begin line

Building configuration...
line console
 exec-timeout 120 120
!
logging trap
--More--
/ip
filtering...
ip route 0.0.0.0 255.255.0.0 pos0/2/0/0
interface pos0/2/0/0
 ip address 172.19.73.215 255.255.0.0
end
```

Tip On most systems, Ctrl-Z can be entered at any time to interrupt the output and return to EXEC mode.

For more information, see Appendix A, "Understanding Regular Expressions, Special Characters, and Patterns."

Wildcards, Templates, and Aliases

This section contains the following topics:

Using Wildcards to Identify Interfaces in show Commands

Wildcards (*) identify a group of interfaces in **show** commands. Table 6-4 provides examples of wildcard usage to identify a group of interfaces.

Table 6-4 Examples of Wildcard Usage

Wildcard Syntax	Description
*	Specifies all interfaces
pos*	Specifies all POS interfaces in the system
pos0/1/*	Specifies all POS interfaces in rack 0, slot 1
pos0/3/4.*	Specifies all subinterfaces for POS0/3/4

Note The wildcard (*) must be the last character in the interface name.

Example

In the following example, the configuration for all POS interfaces in rack 0, slot 1 is displayed:

```
RP/0/RP1/CPU0:router# show running-config interface pos0/1/*

interface POS0/1/0/0
 ipv4 address 10.2.3.4 255.255.255.0
 pos
  crc 32
 !
 keepalive disable
interface POS0/1/0/1
 ipv4 address 10.2.3.5 255.255.255.0
 pos
  crc 32
 !
 keepalive disable
interface POS0/1/0/2
 ipv4 address 10.2.3.6 255.255.255.0
 pos
  crc 32
 !
 keepalive disable
interface POS0/1/0/3
 ipv4 address 10.2.3.7 255.255.255.0
 pos
  crc 32
 !
 keepalive disable

 --More--
```

In the following example, the state of all POS interfaces is displayed:

```
RP/0/RP1/CPU0:router# show interfaces pos* brief

                Intf        Intf         LineP              Encap  MTU       BW
                Name        State        State               Type (byte)    (Kbps)
--------------------------------------------------------------------------------
           PO0/1/0/0          up           up                 HDLC  4474   2488320
           PO0/1/0/1          up           up                 HDLC  4474   2488320
           PO0/1/0/2          up           up                 HDLC  4474   2488320
           PO0/1/0/3          up           up                 HDLC  4474   2488320
           PO0/1/0/4          up           up                 HDLC  4474   2488320
           PO0/1/0/5          up           up                 HDLC  4474   2488320
           PO0/1/0/6          up           up                 HDLC  4474   2488320
           PO0/1/0/7          up           up                 HDLC  4474   2488320
           PO0/1/0/8          up           up                 HDLC  4474   2488320
           PO0/1/0/9          up           up                 HDLC  4474   2488320
          PO0/1/0/10          up           up                 HDLC  4474   2488320
          PO0/1/0/11          up           up                 HDLC  4474   2488320
          PO0/1/0/12          up           up                 HDLC  4474   2488320
          PO0/1/0/13          up           up                 HDLC  4474   2488320
          PO0/1/0/14          up           up                 HDLC  4474   2488320
          PO0/1/0/15          up           up                 HDLC  4474   2488320
```

Creating Configuration Templates

Configuration templates allow you to create a name that represents a group of configuration commands. After a template is defined, it can be applied to interfaces by you or other users. As networks scale to large numbers of nodes and ports, the ability to configure multiple ports quickly using templates can greatly reduce the time it takes to configure interfaces.

The two primary steps in working with templates are creating templates and applying templates. The following procedure describes how to create a configuration template.

SUMMARY STEPS

1. **configure**
2. **template** *template-name* [(**$***parameter* **$***parameter...*)] [*config-commands*]
3. Enter the template commands.
4. **end-template**
5. **commit**
6. **show running-config template** *template-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure** **Example:** `Router# configure`	Enters global configuration mode.
Step 2	**template** *template-name* [**($***parameter* **$***parameter...***)**] [*config-commands*] **Example:** `RP/0/RP0/CPU0:router(config)# template tmplt_1`	Enters template configuration mode and creates a template. • *template-name*: Unique name for the template to be applied to the running configuration. • *parameter*: (Optional) Actual values of the variables specified in the template definition. Up to five parameters can be specified within parentheses. Each parameter must begin with the **$** character. Templates can be created with or without parameters. • *config-commands*: (Optional) Global configuration commands to be added to the template definition. Any name in a command (such as the server name, group name, and so on) can be parameterized. This means that those parameters can be used in the template commands (starting with $) and replaced with real arguments when applied. • To remove the template, use the **no** form of this command.
Step 3	Enter the template commands. **Example:** `RP/0/RP0/CPU0:router(config-TPL)# hostname test`	Defines the template commands.
Step 4	**end-template** **Example:** `RP/0/RP0/CPU0:router(config-TPL)# end-template`	Ends the template definition session and exits template configuration mode. • When you end the template session, you are returned to global configuration mode.
Step 5	**commit** **Example:** `RP/0/RP0/CPU0:router(config-TPL)# commit`	Applies the target configuration commands to the running configuration.
Step 6	**show running-config template** *template-name* **Example:** `RP/0/RP0/CPU0:router# show running-config template tmplt_1`	Displays the details of the template.

Examples

In the following example, a simple template is defined. The template contents are then displayed with the **show running-config template** *template-name* command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# template jbtest
RP/0/RP0/CPU0:router(config-TPL)# hostname test
RP/0/RP0/CPU0:router(config-TPL)# end-template
RP/0/RP0/CPU0:router(config)# commit
RP/0/RP0/CPU0:router(config)# show running-config template jbtest

template jbtest
 hostname test
end-template
```

In the next example, a template is defined, and the template requires a parameter. The template contents are then displayed with the **show running-config template** *template-name* command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# template test2 (hostname)
RP/0/RP0/CPU0:router(config-TPL)# hostname $hostname
RP/0/RP0/CPU0:router(config-TPL)# end-template
RP/0/RP0/CPU0:router(config)# commit
RP/0/RP0/CPU0:router(config)# show running-config template test2

template test2 (hostname )
 hostname $hostname
end-template
```

Applying Configuration Templates

To apply a template, enter the **apply-template** *template-name* [(*parameter*)] command in global configuration mode and consider the following guidelines:

- Only one template can by applied at a time.
- If the same template is applied multiple times, the most recent application overwrites the previous ones.
- Provide the exact number of parameters for the template.
- Templates are applied as a “best effort” operation; only valid changes are committed. If any command in the template fails, that command is discarded.
- After a template is applied, the **show configuration** command displays the target configuration changes. The target configuration must be committed (with the **commit** command) to become part of the running configuration.

Examples

In the following example, a simple template is defined. The template contents are then displayed with the **show running-config template** *template-name* command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# apply-template jbtest
RP/0/RP0/CPU0:router(config) show configuration

Building configuration...
hostname test
end
```

In the next example, a template with one parameter is applied and the show configuration command displays the result:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# apply-template test2 (router)
RP/0/RP0/CPU0:router(config)# show configuration

Building configuration...
hostname router
end
```

Aliases

Cisco IOS XR software lets you define command line aliases for any physical or logical entity in a router. After you define the alias, it can be used in the CLI to reference the real entity.

To create a command alias, enter the **alias** command in global configuration or administration configuration mode:

alias *alias-name* [(*parameter1 parameter2...*)] *command-syntax* [$*parameter1*] [*command-syntax* [$*parameter2*]}

Table 6-5 defines the **alias** command syntax.

Table 6-5 alias Command Syntax

Syntax	Specifies that the Alias Is Created for
alias-name	Name of the command alias. An alias name can be a single word or multiple words joined by a dash (–).
command-syntax	Original command syntax. Valid abbreviations of the original command syntax can be entered for the *command-syntax* argument.
(*parameterx*)	Argument or keyword that belongs to the command you specified for the *command-syntax* argument. When the parameter is entered in parenthesis after the alias name, the alias requires a parameter name. To associate the parameter with a command within the alias, enter the $ character preceding the parameter name.

Multiple commands can be supported under a single command alias, and multiple variables can be supported for each command. If multiple commands are specified under a single alias, then each command is executed in the order in which it is listed in the **alias** command.

In the following example, an alias named *my-cookie* is created for the Management Ethernet interface, and then the new alias is specified to enter interface configuration mode:

```
RP/0/0/CPU0:router(config)# alias my-cookie mgmtEth 0/0/CPU0/0


RP/0/0/CPU0:router(config)# interface my-cookie
RP/0/0/CPU0:router(config)# interface mgmtEth 0/0/CPU0/0
RP/0/0/CPU0:router(config-if)#
```

After you enter a command with an alias, the router displays the command you entered with the alias value so that you can verify that alias value.

To delete a specific alias, enter the **no** form of the **alias** command with the alias name.

Keystrokes Used as Command Aliases

The system can be configured to recognize particular keystrokes (key combination or sequence) as command aliases. In other words, a keystroke can be set as a shortcut for executing a command. To enable the system to interpret a keystroke as a command, use the Ctrl-V or Esc, Q key combinations before entering the command sequence.

Command History

The Cisco IOS XR software lets you display a history of the most recently entered and deleted commands. You can also redisplay the command line while a console message is being shown. The following sections describe the command history functionality:

- Recalling Previously Entered Commands, page 6-17
- Recalling Deleted Entries, page 6-18
- Redisplaying the Command Line, page 6-18

Note To roll back to a previously committed configuration, see the "Managing Configuration History and Rollback" section on page 5-3.

Recalling Previously Entered Commands

The Cisco IOS XR software records the ten most recent commands issued from the command line in its history buffer. This feature is particularly useful for recalling long or complex commands or entries, including access lists.

To recall commands from the history buffer, use one of the commands or key combinations listed in Table 6-6.

Table 6-6 Command History

Command or Key Combination	Purpose
Ctrl-P or the up arrow key	Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Ctrl-N or the down arrow key	Returns to more recent commands in the history buffer after recalling commands with Ctrl-P or the up arrow key. Repeat the key sequence to recall successively more recent commands.

Recalling Deleted Entries

The Cisco IOS XR CLI also stores deleted commands or keywords in a history buffer. The buffer stores the last ten items that have been deleted using Ctrl-K, Ctrl-U, or Ctrl-X. Individual characters deleted using Backspace or Ctrl-D are not stored.

Table 6-7 identifies the keystroke combinations used to recall deleted entries to the command line.

Table 6-7 Keystroke Combinations to Recall Deleted Entries

Command or Key Combination	Recalls the
Ctrl-Y	Most recent entry in the buffer (press the keys simultaneously).
Esc, Y	Previous entry in the history buffer (press the keys sequentially).

Note The Esc, Y key sequence does not function unless the Ctrl-Y key combination is pressed first. If the Esc, Y is pressed more than ten times, the history cycles back to the most recent entry in the buffer.

Redisplaying the Command Line

If the system sends a message to the screen while a command is being entered, the current command line entry can be redisplayed using the Ctrl-L or Ctrl-R key combination.

Key Combinations

The following sections provide information on key combinations:

Key Combinations to Move the Cursor

Table 6-8 shows the key combinations or sequences you can use to move the cursor around on the command line to make corrections or changes. When you use cursor control keys, consider the following guidelines:

- Ctrl indicates the Control key, which must be pressed simultaneously with its associated letter key.
- Esc indicates the Escape key, which must be pressed first, followed by its associated letter key.
- Keys are not case sensitive.

Table 6-8 Key Combinations Used to Move the Cursor

Keystrokes	Function	Moves the Cursor
Left arrow or Ctrl-B	Back character	One character to the left.When you enter a command that extends beyond a single line, you can press the left arrow or Ctrl-B keys repeatedly to scroll back toward the system prompt and verify the beginning of the command entry, or you can press the Ctrl-A key combination.
Right arrow or Ctrl-F	Forward character	One character to the right.
Esc, B	Back word	Back one word.
Esc, F	Forward word	Forward one word.
Ctrl-A	Beginning of line	To the beginning of the line.
Ctrl-E	End of line	To the end of the command line.

Keystrokes to Control Capitalization

Letters can be capitalized or uncapitalized using simple key sequences. Table 6-9 describes the keystroke combinations used to control capitalization.

Note Cisco IOS XR commands are generally case insensitive and typically all in lowercase.

Table 6-9 Keystrokes Used to Control Capitalization

Keystrokes	Purpose
Esc, C	Capitalizes the letter at the cursor.
Esc, L	Changes the word at the cursor to lowercase.
Esc, U	Capitalizes letters from the cursor to the end of the word.

Keystrokes to Delete CLI Entries

Table 6-10 describes the keystrokes used to delete command line entries.

Table 6-10 Keystrokes for Deleting Entries

Keystrokes	Deletes
Delete or Backspace	The character to the left of the cursor.
Ctrl-D	The character at the cursor.
Ctrl-K	All characters from the cursor to the end of the command line.
Ctrl-U or Ctrl-X	All characters from the cursor to the beginning of the command line.
Ctrl-W	The word to the left of the cursor.
Esc, D	From the cursor to the end of the word.

Transposing Mistyped Characters

To transpose mistyped characters, use the Ctrl-T key combination.

CHAPTER 7

Troubleshooting the Cisco IOS XR Software

This chapter describes the tools and procedures used to identify the source of hardware and software problems. This chapter also provides instructions on gathering data for further analysis by Cisco customer support representatives.

Contents

This chapter contains the following sections:

Additional Sources for Information

For additional information on troubleshooting, see the following sources:

- If the Cisco IOS XR software does not start and display the EXEC mode prompt, see *Cisco IOS XR ROM Monitor Guide*.
- The Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.

  http://www.cisco.com/public/support/tac/home.shtml
- The "Related Documents" section on page x.

Basic Troubleshooting Commands

The following sections describe some basic techniques used to determine connectivity to another device and display information on the configuration and operation of a router.

Using show Commands to Display System Status and Configuration

Use **show** commands to check the status of various Cisco IOS XR software subsystems and services. Table 7-1 lists some of the common **show** commands.

To display a complete list of the available show commands, enter the **show ?** command to access the on-screen help system.

Note Different **show** commands are available in different command modes, and the same **show** command can show different results in different command modes.

Table 7-1 Common show Commands in Cisco IOS XR Software

Command	Description
show variables boot (EXEC and administration EXEC modes)	Displays the boot variables.
show configuration (Global configuration and administration configuration modes)	Displays the uncommitted configuration changes made during a configuration session. This command can be entered in any configuration mode.
show context (and show exception) (EXEC and administration EXEC modes)	Displays context information about all recent reloads.
show controller (Administration EXEC mode)	Displays hardware controller information.
show controllers (EXEC mode)	Displays hardware controller information.
show debug (EXEC and administration EXEC modes)	Displays debug flags enabled from the current terminal.
show environment [*options*] (EXEC and administration EXEC modes)	Displays hardware information for the physical components and systems, including fans, LEDs, power supply voltage and current information, and temperatures. To view the command options, enter the **show environment ?** command.

Table 7-1 Common show Commands in Cisco IOS XR Software (continued)

Command	Description
show exception (EXEC and administration EXEC modes)	Displays all exception dump configurations.
show install (EXEC and administration EXEC modes)	Displays installed and active software packages.
show interfaces (EXEC mode)	Displays interface status and configuration.
show logging (EXEC and administration EXEC modes)	Displays the contents of logging buffers.
show memory (EXEC and administration EXEC modes)	Displays memory statistics.
show platform (EXEC and administration EXEC modes)	Displays information about node status on the router. To display the nodes assigned to an SDR, enter this command in EXEC mode. To display all the nodes in a router, enter this command in administration EXEC mode.
show processes blocked (EXEC and administration EXEC modes)	Displays blocked processes.
show redundancy (EXEC and administration EXEC modes)	Display the status of the primary (active) route processor (RP) and the standby (redundant) RP.
show running-config [*command*] (EXEC and administration EXEC modes)	Displays the current running configuration.
show tech-support (EXEC and administration EXEC modes)	Collects a large amount of system information for troubleshooting. The output should be provided to technical support representatives when a problem is reported. Because of the impact the command can have on a running system, it is reserved for users assigned to the cisco-support task ID.
show user [**group** | **tasks** | **all**] (EXEC mode)	Displays the username for the current logged-in user. Use this command to also display the groups and associated task IDs assigned to the account.
show version (EXEC and administration EXEC modes)	Displays basic system information.

Using the ping Command

Use the **ping** command to diagnose network connectivity. In EXEC mode, enter a hostname or an IP address as an argument to this command. In administration EXEC mode, you can use the fabric or the control Ethernet network (in a multishelf system) to ping other nodes.

The **ping** command sends an echo request packet to a destination, then awaits a reply. Ping output can help you evaluate path-to-destination reliability, delays over the path, and whether the destination can be reached or is functioning.

Each exclamation point (!) indicates receipt of a reply. A period (.) indicates the network server timed out while waiting for a reply. Other characters may appear in the ping output display, depending on the protocol type.

Examples

In the following example, a successful ping attempt is shown:

```
RP/0/RP0/CPU0:router# ping 10.233.233.233

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.233.233.233, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/7 ms
```

In the next example, an unsuccessful ping attempt is shown:

```
RP/0/RP0/CPU0:router# ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

The following example shows the output of ping through the fabric:

```
RP/0/RP1/CPU0:CRS-8_P1(admin)# ping fabric location 0/6/5

Src node:        529  :  0/RP1/CPU0
Dest node:       109  :  0/6/5
Local node:      529  :  0/RP1/CPU0
Packet cnt:        1  Packet size:   128  Payload ptn type: default (0)
Hold-off (ms):   300  Time-out(s):     2  Max retries: 5

Running Fabric node ping.
Please wait...
Src: 529:, Dest: 109, Sent: 1, Rec'd: 1, Mismatched: 0
Min/Avg/Max RTT: 20000/20000/20000
Fabric node ping succeeded for node: 109
```

Using the traceroute Command

Use the **traceroute** command in EXEC mode to discover the routes that packets take when traveling to their destination. Enter a hostname or an IP address as an argument to this command.

This command works by taking advantage of the error messages generated by routers when a datagram exceeds its time-to-live (TTL) value.

The **traceroute** command starts by sending probe datagrams with a TTL value of 1, causing the first router to discard the probe datagram and send back an error message. The **traceroute** command sends several probes at each TTL level and displays the round-trip time for each.

The **traceroute** command sends one probe at a time. Each outgoing packet may result in one or two error messages. A *time exceeded* error message indicates that an intermediate router has seen and discarded the probe. A *destination unreachable* error message indicates that the destination node has received the probe and discarded it because it could not deliver the packet. If the timer times out before a response comes in, the **traceroute** command prints an asterisk (*).

The **traceroute** command terminates when the destination responds, the maximum TTL is exceeded, or the user interrupts the trace with the escape sequence.

Examples

In the following example, the route for an IP address is displayed:

```
RP/0/RP0/CPU0:router# traceroute 10.233.233.233

Type escape sequence to abort.
Tracing the route to 10.233.233.233

 1  172.25.0.2 11 msec  2 msec  1 msec
 2  192.255.254.254 1 msec  *  2 msec
```

Using debug Commands

Debug commands are used to diagnose and resolve network problems. Use **debug** commands to troubleshoot specific problems or during troubleshooting sessions.

Use **debug** commands to turn on or off debugging for a specific service or subsystem. When debugging is turned on for a service, a debug message is generated each time the debugging code section is entered. The following sections provide information on debugging:

- Displaying a List of Debug Features, page 7-6
- Enabling Debugging for a Feature, page 7-6
- Disabling Debugging for a Service, page 7-7
- Displaying Debugging Status, page 7-7

Caution Debug commands can generate a very large amount of output and can render the system unusable. Use **debug** to troubleshoot specific problems or during specific troubleshooting sessions on systems that are not in production.

Displaying a List of Debug Features

To display a list of the available debug features, enter the debug mode and enter a **?** for on-screen help. The set of debug mode features is different in EXEC and administration EXEC modes. In the following example, EXEC mode is the entry point to debug mode:

```
RP/0/RP0/CPU0:router# debug
RP/0/RP0/CPU0:router(debug)# ?

  aaa                 AAA Authentication, Authorization and Accounting
  adjacency           Adjacency debug
  adjacency           platform AIB information
  aib                 AIB information
  alarm-logger        Turn on alarm debugging
  arm                 IP Address Repository Manager
  arp                 IP ARP transactions
  asic-errors         Debug ASIC erors
  asic-scan           Debug Asic Scan
--More--
```

In the next example, administration EXEC mode is the entry point to debug mode:

```
RP/0/RP1/CPU0:CRS-8_P1# admin
RP/0/RP1/CPU0:CRS-8_P1(admin)# debug
RP/0/RP1/CPU0:CRS-8_P1(admin-debug)# ?
  cctl          Chassis control driver process debug
  cetftp        Control ethernet TFTP (CE-TFTP) server process debug
  cpuctrl       Debug Cpuctrl Driver
  describe      Describe a command without taking real actions
  diagnostic    Diagnostic debugging
  dsc           dsc debug: all, fsm, table, cfg, and api
  dumper        Admin Debug Dumper
  exit          Exit from this submode
  fabric        Fabric debugging
  fabricq       Debug Fabric Queue Manager
  fia           Debug the Fabric Interface ASIC (FIA) driver
  gsp           Admin Debug gsp
  ingressq      Debug Ingress Queue Manager
  install       Install debug information
  inv           Inventory manager process debug
  invd          Inventory debug: all, trap, dll mem
  invmgr        Inventory Manager client API interface debug
  ntp           NTP information
  oird          oird all, event, message
  pair          DRP Pairing debug: Display debugging messages of drp_pairing
  shelfmgr      Shelfmgr debug: all, heartbeat, boot, fsm, init and eah
  sysdb         Configure SysDB debug settings
  upgrade-fpd   Debug upgrade fpd
 --More--
```

Enabling Debugging for a Feature

To enable debugging for a feature, enter the **debug** command in EXEC or administration EXEC mode and then enable the feature for debugging. For example:

```
RP/0/RP0/CPU0:router# debug
RP/0/RP0/CPU0:router(debug)# aaa all
RP/0/RP0/CPU0:router(debug)# exit
```

You can also enter the complete command from EXEC mode, as shown in the following example:

```
RP/0/RP0/CPU0:router# debug aaa all
```

Displaying Debugging Status

Enter the **show debug** command to display the debugging features enabled for your terminal session. The terminal session is labeled *tty* and represents your connection to the router through a specific port, which might be the console port, auxiliary port, or Management Ethernet interface. In the following example, the command display indicates that debugging is enabled for two features (AAA and ipv4 io icmp) from a terminal session on the console port of RP1:

```
RP/0/RP0/CPU0:router# show debug

####  debug flags set from tty 'con0_RP1_CPU0'  ####
aaa all flag is ON
ipv4 io icmp flag is ON

RP/0/RP0/CPU0:router# no debug aaa all
RP/0/RP0/CPU0:router# show debug

####  debug flags set from tty 'con0_RP1_CPU0'  ####
ipv4 io icmp flag is ON
```

The preceding example is for a Cisco CRS-1 router. On a Cisco XR 12000 Series Router, the slot number of the tty ID is 0 or 1 instead of RP0 or RP1.

Enter the **show debug conditions** command to display the conditional debugging status. For example:

```
RP/0/RP0/CPU0:router# show debug conditions

####  debug conditions set from tty 'con0_RP1_CPU0'  ####
interface  condition is ON for interface 'POS0/2/0/1'
```

Disabling Debugging for a Service

Use the **no** form of the **debug** command or the **undebug** command to turn off debugging for a service or subsystem.

In the following example, the **no debug** command disables debugging for the AAA feature:

```
RP/0/RP0/CPU0:router# no debug aaa all
RP/0/RP0/CPU0:router# show debug

####  debug flags set from tty 'con0_RP1_CPU0'  ####
ipv4 io icmp flag is ON
```

You can also turn off debugging from the undebug mode, as shown in the following example:

```
RP/0/RP0/CPU0:router# undebug
RP/0/RP0/CPU0:router(undebug)# aaa all
RP/0/RP0/CPU0:router(undebug)# exit
```

Disabling Debugging for All Services Started at the Active Terminal Session

Use the **undebug all** or **no debug all** command to turn off all debugging started by the active terminal session. For example, if you enter either of these commands while connected to the router through the console port on the active RP, all debug sessions started from that console port are disabled. In the following example, debugging for all services is disabled and then verified:

```
RP/0/RP0/CPU0:router# undebug all
RP/0/RP0/CPU0:router# show debug
No matching debug flags set
```

Disabling Debugging for All Services Started at All Terminal Sessions

Use the **undebug all all-tty** command to turn off debugging for all services that have been started from all terminal sessions. For example if you enter this command while connected to the router through the console port on the active RP, all debug sessions started from all ports are disabled. In the following example, debugging for all services and ports is disabled and then verified:

```
RP/0/0/CPU0:router# undebug all all-tty
RP/0/0/CPU0:router# show debug

No matching debug flags set
```

Configuration Error Messages

The following sections contain information on configuration error messages:

Configuration Failures During a Commit Operation

A target configuration is added to the running configuration of a router when the **commit** command is entered. During this operation, the changes are automatically verified by the other components in the system. If successful, the configuration becomes part of the running configuration. If some configuration items fail, an error message is returned.

To display the configuration items that failed and see the cause of each failure, enter the **show configuration failed** command.

Note The **show configuration failed** command can be entered in either the EXEC mode or any configuration mode. In any mode, the configuration failures from the most recent **commit** operation are displayed.

In the following example, a configuration error occurs when an invalid commit operation is attempted:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# taskgroup bgp
RP/0/RP0/CPU0:router(config-tg)# description this is a test of an invalid taskgroup
RP/0/RP0/CPU0:router(config-tg)# commit

% Failed to commit one or more configuration items. Please use 'show configurati
on failed' to view the errors
```

To display the configuration items that failed, including a description of the error, enter the **show configuration failed** command:

```
RP/0/RP0/CPU0:router(config-tg)# show configuration failed

!! CONFIGURATION FAILED DUE TO SEMANTIC ERRORS
taskgroup bgp
!!% Usergroup/Taskgroup names cannot be taskid names
!
```

You can also display the failed configuration items without the error description by entering the **show configuration failed noerror** command:

```
RP/0/RP0/CPU0:router(config-tg)# show configuration failed noerror

!! CONFIGURATION FAILED DUE TO SEMANTIC ERRORS
taskgroup bgp
```

Configuration Errors at Startup

Configuration errors that occurred during system startup can be displayed with the **show configuration failed startup** command. For example:

```
RP/0/RP0/CPU0:router# show configuration failed startup

!! CONFIGURATION FAILED DUE TO SYNTAX ERRORS
ntp
xml agent corba
http server
```

Memory Warnings in Configuration Sessions

The Cisco IOS XR software automatically monitors and manages the system resources in a router. Under normal operating conditions, memory problems should not occur.

When a low-memory issue does occur, it is often in the form of a low-memory warning during a configuration session. Low-memory conditions can be caused by multiple, large configurations being added to the router at a single time. Users can remove the source of a problem by removing configurations.

The following sections describe the commands used to display memory usage in a router and what to do if a low-memory warning appears:

Understanding Low-Memory Warnings in Configuration Sessions

The Cisco IOS XR software monitors memory usage in the Cisco CRS-1 router. If system memory becomes low, an error message is displayed when you attempt to enter configuration mode.

An "out-of-memory" error message is displayed during one of the following situations:

- When a user attempts to enter configuration mode.
- During a configuration session when the memory shortage occurs.
- When a user attempts to load a target configuration from a large file that results in a memory shortage.
- During a commit operation that results in the low-memory warning message. The commit operation is denied and only lr-root users can perform commit operations to remove configurations.

Caution Never ignore a low-memory warning. These warnings indicate a memory state that could affect system operations if not addressed.

"WARNING! MEMORY IS IN MINOR STATE"

If the system memory begins to run low, the following minor memory warning is displayed when you enter a new configuration mode.

```
WARNING! MEMORY IS IN MINOR STATE
```

Although users are allowed to enter configuration mode, they should immediately reduce memory usage using the tools described in the "Removing Configurations to Resolve Low-Memory Warnings" section on page 7-12.

Failure to take action can result in a worsening situation and eventual impact to router operations.

"ERROR! MEMORY IS IN SEVERE (or CRITICAL) STATE"

When the memory is in a severe or critical state, router operation and performance is likely to be affected. Regular users are not allowed to enter configuration mode. Only lr-root owners can enter configuration mode to free memory by removing configurations.

In some situations, the **commit** command is not allowed. Users with lr-root access can still use the **commit force** command to apply configurations that reduce memory usage. Reducing memory usage normally means removing configurations, but a user can also add configurations that reduce memory usage. For example, configuring the **shutdown** command on an interface could cause numerous routes to be purged from Border Gateway Protocol (BGP), the Routing Information Base (RIB), and Forwarding Information Base (FIB) configurations.

Caution The **commit force** command should be used only to apply configurations that reduce memory usage. Adding configurations that increase memory usage could result in serious loss of router operation.

Displaying System Memory Information

To display a high level summary of system memory, enter the **show memory summary** command. Table 7-1 describes the meaning of each heading.

```
RP/0/RP0/CPU0:router# show memory summary

Physical Memory: 2048M total
 Application Memory : 1787M (1509M available)
 Image: 132M (bootram: 132M)
 Reserved: 128M, IOMem: 0, flashfsys: 0
 Total shared window: 0
RP/0/RP1/CPU0:router#
```

To display general memory usage for the device as a whole and by process, enter the **show memory** command. Table 7-1 describes the meaning of each heading.

```
RP/0/RP0/CPU0:router# show memory

Physical Memory: 2048M total
 Application Memory : 1787M (1510M available)
 Image: 132M (bootram: 132M)
 Reserved: 128M, IOMem: 0, flashfsys: 0
 Total shared window: 0

kernel: jid 1
Address         Bytes           What
000d2000        12288           Program Stack
00112000        12288           Program Stack
Total Allocated Memory: 0
Total Shared Memory: 0

pkg/bin/wd-mbi: jid 72
Address         Bytes           What
4817f000        4096            Program Stack (pages not allocated)
48180000        516096          Program Stack (pages not allocated)
481fe000        8192            Program Stack
48200000        8192            Program Text
 --More--
```

Table 7-2 Heading Descriptions for show memory Command Output

Heading	Description
Physical Memory	Amount of physical memory installed on the device.
Application Memory	Memory available for the system to use (total memory minus image size, reserved, IOMem, and flashfsys).
Image	Size of the bootable image.
Reserved	Reserved for packet memory.
IOMem	IO memory—Currently used as a backup for packet memory.
flashfsys	Flash file system memory.
Process and JID	Process and job ID.
Address	Starting address in memory.
Bytes	Size of memory block.
What	Block description.

Removing Configurations to Resolve Low-Memory Warnings

To resolve most low-memory problems, you should remove the configurations from the router that are consuming the most memory. Often, memory problems occur when a large new configuration is added to the system. The following sections provide information to resolve low-memory issues:

Clearing a Target Configuration

A low-memory warning can occur when a large configuration file is loaded into a target configuration session. To remove the target configuration, enter the **clear** command to discard the changes. For example:

```
RP/0/RP0/CPU0:router(config)# clear
```

Caution Committing a target configuration that has caused a low-memory warning can make the system unstable. Clearing a target configuration is a preventive measure to not let the system go into a worse memory state due to additional configuration. In addition, all other active configuration sessions can be closed to minimize the churn.

Removing Committed Configurations to Free System Memory

You can reduce memory usage by removing configurations from the router, as shown in the following procedure:

Step 1 Enter the **show memory summary** command in EXEC mode to display the overall system memory:

```
RP/0/RP0/CPU0:router# show memory summary

Physical Memory: 2048M total
 Application Memory : 1787M (1511M available)
 Image: 132M (bootram: 132M)
 Reserved: 128M, IOMem: 0, flashfsys: 0
 Total shared window: 0
```

Step 2 Enter the **show configuration commit history** command in EXEC or administration EXEC mode to see if a large configuration forced the router over the limit.

The output from this command does not show the details of the entries, but allows you to display a larger list of the commit events that occurred. To display the commitIDs to which you can roll back, use the **show configuration commit history** command.

```
RP/0/RP0/CPU0:router# show configuration commit history

SNo. Label/ID    User      Line        Client      Time Stamp
~~~~ ~~~~~~~~    ~~~~      ~~~~        ~~~~~~      ~~~~~~~~~~
1    1000000144  user      vty0        CLI         00:16:51 UTC Thu Dec 11 2003
2    1000000143  user      vty0        CLI         00:04:32 UTC Thu Dec 11 2003
3    1000000142  user      0.0.0.0     XMLAgent    21:58:36 UTC Wed Dec 10 2003
4    1000000141  user      0.0.0.0     XMLAgent    21:46:07 UTC Wed Dec 10 2003
5    1000000140  cisco     con0_RP1_C  CLI         21:43:30 UTC Wed Dec 10 2003
6    1000000139  user      0.0.0.0     XMLAgent    21:40:13 UTC Wed Dec 10 2003
7    1000000138  user      0.0.0.0     XMLAgent    21:34:48 UTC Wed Dec 10 2003
8    1000000137  cisco     con0_RP1_C  CLI         21:32:10 UTC Wed Dec 10 2003
9    1000000136  user      0.0.0.0     XMLAgent    21:30:13 UTC Wed Dec 10 2003
10   1000000135  cisco     con0_RP1_C  CLI         19:45:04 UTC Wed Dec 10 2003
```

Step 3 Enter the **show configuration commit changes** command followed by a commitID number to display the configuration changes for a commit session (commitID). For example:

```
RP/0/RP0/CPU0:router# show configuration commit changes 1000000053

Building configuration...
interface preconfigure MgmtEth0/RP1/CPU0/0
 ipv4 address 10.8.50.10 255.255.0.0
 proxy-arp
!
router static
 address-family ipv4 unicast
  172.255.254.254/32 12.8.0.1
 !
!
end
```

Step 4 Remove the configuration using the appropriate configuration commands. In some situations, the **commit** command is not allowed. Users with lr-root access can still use the **commit force** command, but this command should be used only to remove configurations. The addition of new configurations seriously impacts router operation.

For more information, see the "Managing Configuration History and Rollback" section on page 5-3.

Rolling Back to a Previously Committed Configuration

You can roll back the system to a previous committed configuration, as described in the "Managing Configuration History and Rollback" section on page 5-3.

Clearing Configuration Sessions

Active configuration sessions and their associated target configurations can consume system memory. Users with the appropriate access privileges can display the open configuration sessions of other users and terminate those sessions, if necessary (see Table 7-3).

Table 7-3 Session Commands

Command	Description
show configuration sessions	Displays the active configuration sessions.
clear configuration sessions *session-id*	Clears a configuration session.

In the following example, the open configuration sessions are displayed with the **show configuration sessions** command. The **clear configuration sessions** command is then used to clear a configuration session.

```
RP/0/RP0/CPU0:router# show configuration sessions

Session                   Line        User      Date                      Lock
00000211-002c409b-00000000  con0_RP1_CPU0  UNKNOWN   Mon Feb  2 01:02:09 2004

RP/0/RP0/CPU0:router# clear configuration sessions 00000211-002c409b-00000000

session ID '00000211-002cb09b-00000000' terminated
```

Contacting TAC for Additional Assistance

If you remove configurations and the low-memory condition remains, you may need to contact TAC for additional assistance. See the "Additional Sources for Information" section on page 7-1.

Interfaces Not Coming Up

The router interfaces are directly used in processing network traffic, so their status information is crucial to understanding how the device is functioning. This section contains information on the EXEC mode commands used to verify that the router interfaces are operational. The basic commands used in this process are summarized in Table 7-4.

Table 7-4 show interface Commands

Command	Description
show interfaces	Displays detailed information about all interfaces installed or configured on the device, whether or not they are operational.
show interfaces *type instance*	Specifies a particular interface, rather than displaying information for all interfaces, as in the following example: `show interface POS0/1/0/0`
show ipv4 interface **show ipv6 interface**	Displays basic, IP-related information for all available interfaces.
show ipv4 interface brief **show ipv6 interface brief**	Quickly displays the most critical information about the interfaces, including the interface status (up or down) and the protocol status.

Verifying the System Interfaces

Perform the following steps to verify the system interfaces.

Step 1 Enter the **show platform** command in administration EXEC to verify that all nodes are in the "IOS XR RUN" state:

```
RP/0/RP0/CPU0:router(admin)# show platform

Node            Type            PLIM            State           Config State
--------------------------------------------------------------------------------
0/1/SP          MSC(SP)         N/A             IOS XR RUN      PWR,NSHUT,MON
0/1/CPU0        MSC             16OC48-POS/DPT  IOS XR RUN      PWR,NSHUT,MON
0/2/SP          MSC(SP)         N/A             IOS XR RUN      PWR,NSHUT,MON
0/2/CPU0        MSC             16OC48-POS/DPT  IOS XR RUN      PWR,NSHUT,MON
0/3/SP          MSC(SP)         N/A             IOS XR RUN      PWR,NSHUT,MON
0/3/CPU0        MSC             16OC48-POS/DPT  IOS XR RUN      PWR,NSHUT,MON
0/RP0/CPU0      RP(Active)      N/A             IOS XR RUN      PWR,NSHUT,MON
0/RP1/CPU0      RP(Standby)     N/A             IOS XR RUN      PWR,NSHUT,MON
0/SM0/SP        FC/S(SP)        N/A             IOS XR RUN      PWR,NSHUT,MON
0/SM1/SP        FC/S(SP)        N/A             IOS XR RUN      PWR,NSHUT,MON
0/SM2/SP        FC/S(SP)        N/A             IOS XR RUN      PWR,NSHUT,MON
0/SM3/SP        FC/S(SP)        N/A             IOS XR RUN      PWR,NSHUT,MON
```

Note Line cards in Cisco CRS-1 routers are called modular services cards (MSCs). The **show platform** command output is different for Cisco CRS-1 routers and Cisco XR 12000 Series Routers. When this command is entered in EXEC mode, the display shows only those nodes assigned to the SDR.

Step 2 Enter the **show ipv4 interface brief** command to verify IP address configuration and protocol status:

```
RP/0/RP0/CPU0:router# show ipv4 interface brief

Interface                      IP-Address      Status              Protocol
POS0/1/0/0                     unassigned      Shutdown            Down
POS0/1/0/1                     unassigned      Shutdown            Down
POS0/1/0/2                     unassigned      Shutdown            Down
POS0/1/0/3                     unassigned      Shutdown            Down
POS0/1/0/4                     unassigned      Shutdown            Down
POS0/1/0/5                     unassigned      Shutdown            Down
POS0/1/0/6                     unassigned      Shutdown            Down
POS0/1/0/7                     unassigned      Shutdown            Down
POS0/1/0/8                     unassigned      Shutdown            Down
POS0/1/0/9                     unassigned      Shutdown            Down
POS0/1/0/10                    unassigned      Shutdown            Down
POS0/1/0/11                    unassigned      Shutdown            Down
POS0/1/0/12                    unassigned      Shutdown            Down
POS0/1/0/13                    unassigned      Shutdown            Down
POS0/1/0/14                    unassigned      Shutdown            Down
POS0/1/0/15                    unassigned      Shutdown            Down
POS0/2/0/0                     10.10.1.101     Down                Down
POS0/2/0/1                     unassigned      Shutdown            Down
POS0/2/0/2                     unassigned      Shutdown            Down
POS0/2/0/3                     unassigned      Shutdown            Down
TenGigE0/3/0/0                 unassigned      Shutdown            Down
TenGigE0/3/0/2                 unassigned      Shutdown            Down
MgmtEth0/RP0/CPU0/0            unassigned      Shutdown            Down
```

Step 3 Configure the interfaces, as shown in the following examples.

Note You must enter the **commit** command to make the new configuration part of the active running configuration. If you end the configuration session, you are automatically prompted to commit the changes, as shown in the second example:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface pos0/2/0/1
RP/0/RP0/CPU0:router(config-if)# ipv4 address 10.1.1.1 255.0.0.0
RP/0/RP0/CPU0:router(config-if)# no shutdown
RP/0/RP0/CPU0:router(config-if)# commit
RP/0/RP0/CPU0:router(config-if)# end
RP/0/RP0/CPU0:router#

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface pos0/2/0/2
RP/0/RP0/CPU0:router(config-if)# ipv4 address 10.1.1.2 255.255.0.0
RP/0/RP0/CPU0:router(config-if)# no shutdown
RP/0/RP0/CPU0:router(config-if)# end
Uncommitted changes found, commit them? [yes]: yes
RP/0/RP0/CPU0:router#
```

Step 4 Enter the **show ipv4 interface brief** command to verify that the interfaces are “Up” in the Status column:

```
RP/0/RP0/CPU0:router# show ipv4 interface brief

Interface                  IP-Address      Status                Protocol
POS0/1/0/0                 unassigned      Shutdown              Down
POS0/1/0/1                 unassigned      Shutdown              Down
POS0/1/0/2                 unassigned      Shutdown              Down
POS0/1/0/3                 unassigned      Shutdown              Down
POS0/1/0/4                 unassigned      Shutdown              Down
POS0/1/0/5                 unassigned      Shutdown              Down
POS0/1/0/6                 unassigned      Shutdown              Down
POS0/1/0/7                 unassigned      Shutdown              Down
POS0/1/0/8                 unassigned      Shutdown              Down
POS0/1/0/9                 unassigned      Shutdown              Down
POS0/1/0/10                unassigned      Shutdown              Down
POS0/1/0/11                unassigned      Shutdown              Down
POS0/1/0/12                unassigned      Shutdown              Down
POS0/1/0/13                unassigned      Shutdown              Down
POS0/1/0/14                unassigned      Shutdown              Down
POS0/1/0/15                unassigned      Shutdown              Down
POS0/2/0/0                 10.10.1.101     Up                    Up
POS0/2/0/1                 10.1.1.1        Up                    Up
POS0/2/0/3                 10.1.1.2        Shutdown              Down
POS0/2/0/3                 unassigned      Shutdown              Down
TenGigE0/3/0/0             unassigned      Shutdown              Down
TenGigE0/3/0/2             unassigned      Shutdown              Down
MgmtEth0/RP0/CPU0/0        unassigned      Shutdown              Down
```

Step 5 If the interface is in the "Shutdown/Down" state, as shown in the previous example, perform the following tasks:

a. Verify that the status of the interface is "Shutdown":

```
RP/0/RP0/CPU0:router# show running-config interface POS0/2/0/3

interface pos0/2/0/3
 shutdown
 keepalive disable
!
```

b. Bring the interface up with the following commands:

```
RP/0/RP0/CPU0:router(config)# controller pos 0/2/0/3
RP/0/RP0/CPU0:router(config-sonet)# no shutdown
RP/0/RP0/CPU0:router(config-sonet)# commit
RP/0/RP0/CPU0:router(config-sonet)# exit
RP/0/RP0/CPU0:router(config)# interface pos 0/2/0/3
RP/0/RP0/CPU0:router(config-if)# no shutdown
RP/0/RP0/CPU0:router(config-if)# commit
RP/0/RP0/CPU0:router(config-if)# end
RP/0/RP0/CPU0:router#
```

Step 6 If the interface state is still displayed as "Down," verify that the physical cable connections are correctly installed. The following message indicates that the interface has either a bad connection or no connection:

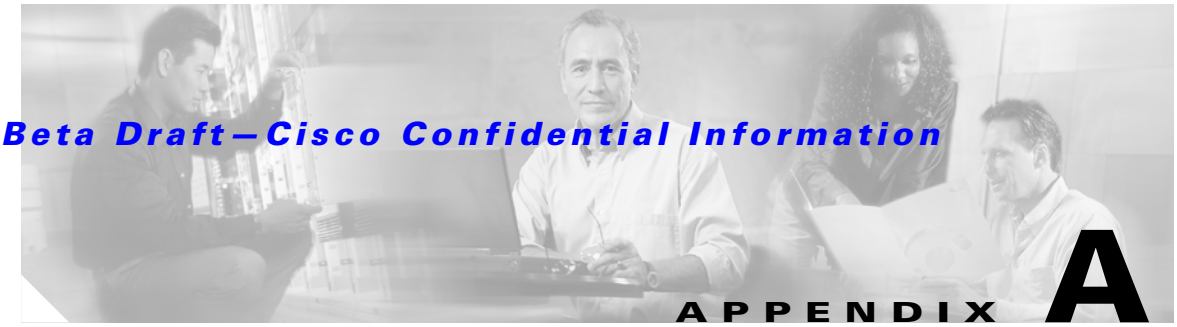
```
LC/0/0/1:Sep 29 15:31:12.921 : plim_4p_oc192[183]: %SONET-4-
ALARM : SONET0_1_1_0: SLOS
```

Step 7 Verify again that the interface is up by entering the **show ipv4 interface brief** command:

```
RP/0/RP0/CPU0:router# show ipv4 interface brief

Interface                      IP-Address      Status              Protocol
POS0/1/0/0                     unassigned      Shutdown            Down
POS0/1/0/1                     unassigned      Shutdown            Down
POS0/1/0/2                     unassigned      Shutdown            Down
POS0/1/0/3                     unassigned      Shutdown            Down
POS0/1/0/4                     unassigned      Shutdown            Down
POS0/1/0/5                     unassigned      Shutdown            Down
POS0/1/0/6                     unassigned      Shutdown            Down
POS0/1/0/7                     unassigned      Shutdown            Down
POS0/1/0/8                     unassigned      Shutdown            Down
POS0/1/0/9                     unassigned      Shutdown            Down
POS0/1/0/10                    unassigned      Shutdown            Down
POS0/1/0/11                    unassigned      Shutdown            Down
POS0/1/0/12                    unassigned      Shutdown            Down
POS0/1/0/13                    unassigned      Shutdown            Down
POS0/1/0/14                    unassigned      Shutdown            Down
POS0/1/0/15                    unassigned      Shutdown            Down
POS0/2/0/0                     10.10.1.101     Up                  Up
POS0/2/0/1                     10.1.1.1        Up                  Up
POS0/2/0/2                     10.1.1.2        Up                  Up
POS0/2/0/3                     unassigned      Shutdown            Down
TenGigE0/3/0/0                 unassigned      Shutdown            Down
TenGigE0/3/0/2                 unassigned      Shutdown            Down
MgmtEth0/RP0/CPU0/0            unassigned      Shutdown            Down
```

Step 8 Repeat these steps for every interface, until every interface shows both Status and Protocol as "Up."



APPENDIX A

Understanding Regular Expressions, Special Characters, and Patterns

This appendix describes the regular expressions, special or wildcard characters, and patterns that can be used with filters to search through command output. The filter commands are described in the "Filtering show Command Output" section on page 6-10. The following sections describe features you can use with filters:

Regular Expressions

A regular expression is a pattern (a phrase, number, or more complex pattern):

- Regular expressions are case sensitive and allow for complex matching requirements. Simple regular expressions include entries like Serial, misses, or 138.
- Complex regular expressions include entries like 00210... , (is), or [Oo]utput.

A regular expression can be a single-character pattern or multiple-character pattern. That is, a regular expression can be a single character that matches the same single character in the command output or multiple characters that match the same multiple characters in the command output. The pattern in the command output is referred to as a string.

The simplest regular expression is a single character that matches the same single character in the command output. Letter (A–Z and a–z), digits (0–9), and other keyboard characters (such as ! or ~) can be used as a single-character pattern.

Special Characters

Certain keyboard characters have special meaning when used in regular expressions. Table A-1 lists the keyboard characters that have special meaning.

Table A-1 Characters with Special Meaning

Character	Special Meaning
.	Matches any single character, including white space.
*	Matches 0 or more sequences of the pattern.
+	Matches 1 or more sequences of the pattern.
?	Matches 0 or 1 occurrences of the pattern.
^	Matches the beginning of the string.
$	Matches the end of the string.
_ (underscore)	Matches a comma (,), left brace ({), right brace (}), left parenthesis (( ), right parenthesis ( )), the beginning of the string, the end of the string, or a space.

To use these special characters as single-character patterns, remove the special meaning by preceding each character with a backslash (\). In the following examples, single-character patterns matching a dollar sign, an underscore, and a plus sign, respectively, are shown.

\$ _ \+

Character Pattern Ranges

A range of single-character patterns can be used to match command output. To specify a range of single-character patterns, enclose the single-character patterns in square brackets ([ ]). Only one of these characters must exist in the string for pattern-matching to succeed. For example, **[aeiou]** matches any one of the five vowels of the lowercase alphabet, while **[abcdABCD]** matches any one of the first four letters of the lowercase or uppercase alphabet.

You can simplify a range of characters by entering only the endpoints of the range separated by a dash (–), as in the following example:

[a–dA–D]

To add a dash as a single-character pattern in the search range, include another dash and precede it with a backslash:

[a–dA–D\–]

A bracket (]) can also be included as a single-character pattern in the range:

[a–dA–D\–\]]

Invert the matching of the range by including a caret (^) at the start of the range. The following example matches any letter except the ones listed:

[^a–dqsv]

The following example matches anything except a right square bracket (]) or the letter d:

[^\]d]

Multiple-Character Patterns

Multiple-character regular expressions can be formed by joining letters, digits, and keyboard characters that do not have a special meaning. With multiple-character patterns, order is important. The regular expression **a4%** matches the character **a** followed by a **4** followed by a **%**. If the string does not have a4%, in that order, pattern matching fails.

The multiple-character regular expression **a.** uses the special meaning of the period character to match the letter a followed by any single character. With this example, the strings ab, a!, and a2 are all valid matches for the regular expression.

Put a backslash before the keyboard characters that have special meaning to indicate that the character should be interpreted literally. Remove the special meaning of the period character by putting a backslash in front of it. For example, when the expression **a\.** is used in the command syntax, only the string a. is matched.

A multiple-character regular expression containing all letters, all digits, all keyboard characters, or a combination of letters, digits, and other keyboard characters is a valid regular expression. For example: **telebit 3107 v32bis**.

Complex Regular Expressions Using Multipliers

Multipliers can be used to create more complex regular expressions that instruct Cisco IOS XR software to match multiple occurrences of a specified regular expression. Table A-2 lists the special characters that specify “multiples” of a regular expression.

Table A-2 Special Characters Used as Multipliers

Character	Description
*	Matches 0 or more single-character or multiple-character patterns.
+	Matches 1 or more single-character or multiple-character patterns.
?	Matches 0 or 1 occurrences of a single-character or multiple-character pattern.

The following example matches any number of occurrences of the letter a, including none:

a*

The following pattern requires that at least one occurrence of the letter a in the string be matched:

a+

The following pattern matches the string bb or bab:

ba?b

The following string matches any number of asterisks (*):

******

To use multipliers with multiple-character patterns, enclose the pattern in parentheses. In the following example, the pattern matches any number of the multiple-character string ab:

(ab)*

As a more complex example, the following pattern matches one or more instances of alphanumeric pairs:

([A-Za-z][0-9])+

The order for matches using multipliers (*, +, and ?) is to put the longest construct first. Nested constructs are matched from outside to inside. Concatenated constructs are matched beginning at the left side of the construct. Thus, the regular expression matches A9b3, but not 9Ab3 because the letters are specified before the numbers.

Pattern Alternation

Alternation can be used to specify alternative patterns to match against a string. Separate the alternative patterns with a vertical bar (|). Only one of the alternatives can match the string. For example, the regular expression **codex|telebit** matches the string codex or the string telebit, but not both codex and telebit.

Anchor Characters

Anchoring can be used to match a regular expression pattern against the beginning or end of the string. Regular expressions can be anchored to a portion of the string using the special characters shown in Table A-3.

Table A-3 Special Characters Used for Anchoring

Character	Description
^	Matches the beginning of the string.
$	Matches the end of the string.

For example, the regular expression **^con** matches any string that starts with con, and **sole$** matches any string that ends with sole.

In addition to indicating the beginning of a string, the ^ can be used to indicate the logical function “not” when used in a bracketed range. For example, the expression **[^abcd]** indicates a range that matches any single letter, as long as it is not the letters a, b, c, and d.

Underscore Wildcard

Use the underscore to match the beginning of a string (^), the end of a string ($), parentheses (( )) , space ( ), braces ({ }), comma (,), and underscore (_). The underscore can be used to specify that a pattern exists anywhere in the string. For example, **_1300_** matches any string that has 1300 somewhere in the string and is preceded by or followed by a space, brace, comma, or underscore. Although **_1300_** matches the regular expression {1300_, it does not match the regular expressions 21300 and 13000t.

The underscore can replace long regular expression lists. For example, instead of specifying **^1300( ) ( )1300$ {1300, ,1300, {1300} ,1300, (1300**, simply specify **_1300_**.

Parentheses Used for Pattern Recall

Use parentheses with multiple-character regular expressions to multiply the occurrence of a pattern. The Cisco IOS XR software can remember a pattern for use elsewhere in the regular expression.

To create a regular expression that recalls a previous pattern, use parentheses to indicate memory of a specific pattern and a backslash (\) followed by a digit to reuse the remembered pattern. The digit specifies the occurrence of a parenthesis in the regular expression pattern. When there is more than one remembered pattern in the regular expression, \1 indicates the first remembered pattern, \2 indicates the second remembered pattern, and so on.

The following regular expression uses parentheses for recall:

a(.)bc(.)\1\2

This regular expression matches an a followed by any character (call it character number 1), followed by bc followed by any character (character number 2), followed by character number 1 again, followed by character number 2 again. So, the regular expression can match aZbcTZT. The software remembers that character number 1 is Z and character number 2 is T, and then uses Z and T again later in the regular expression.

GLOSSARY

A

AAA — authentication, authorization, and accounting. A network security service that provides the primary framework to set up access control on a Cisco CRS-1 router or access server. AAA is an architectural framework and modular means of configuring three independent but closely related security functions in a consistent manner.

ACL — access control list. A list kept by routers to control access to or from the router for a number of services (for example, to prevent packets with a certain IP address from leaving a particular interface on the router).

active — Denotes a card or process that performs a system task; in a redundant configuration, there is an inactive standby card or process available to become active. Active cards or processes are also sometimes denoted as primary.

active RP — The RP that is active in a redundant pair of RPs.

active software configuration — The software configuration marked as active for a node.

active software set — The set of Cisco IOS XR software packages activated in one or more nodes in a router.

algorithm — A well-defined rule or process for arriving at a solution to a problem. In networking, algorithms commonly are used to determine the best route for traffic from a particular source to a particular destination.

APS — automatic protection switching. A method that allows transmission equipment to recover automatically from failures, such as a cut cable.

ASIC — application-specific integrated circuit. A chip designed for use in a specific hardware device. An ASIC is a chip designed for a special application, such as a particular kind of transmission protocol.

B

bandwidth — The amount of data that can be sent in a fixed amount of time. For digital devices, the bandwidth is usually expressed in bits per second (Bps) or bytes per second.

BGP — Border Gateway Protocol. A routing protocol used between autonomous systems. It is the routing protocol that makes the internet work. BGP is a distance-vector routing protocol that carries connectivity information and an additional set of BGP attributes. These attributes allow for a rich set of policies for deciding the best route to use to reach a given destination.

C

card type The type of the card inserted in a slot.

CDP Cisco Discovery Protocol. CDP runs on all Cisco devices so that these devices can learn about neighboring devices and exchange information. CDP uses a well-known multicast MAC address. During system initialization, the application-specific integrated circuit (ASIC) is configured to forward these packets to the Cisco IOS XR software CPU, which processes the packets.

Cisco.com The Cisco website

CLI command-line interface. A text-based user interface to an operating system. A command-line interface is a user interface to a computer operating system or an application in which the user responds to a visual prompt by typing a command on a specified line, receives a response from the system, and then enters another command, and so forth. Typically, most of the UNIX-based systems today offer both a command-line interface and graphical user interface (GUI). See also *GUI*.

committed/saved software configuration The configuration stored in the system for a particular node. The RP loads the committed configuration into memory at startup.

configuration register In Cisco routers, a 16-bit, user-configurable value that determines how the router functions during initialization. The configuration register can be stored in hardware or software. In hardware, the bit position is set using a jumper. In software, the bit position is set by specifying a hexadecimal value using configuration commands. A hexadecimal or decimal value that represents the 16-bit configuration register value that you want to use the next time the router is restarted. The value range is from 0x0 to 0xFFFF (0 to 65535 in decimal).

control plane The control plane oversees the operation of the data plane, allocating resources, providing information, and handling errors to allow data plane operations to be continuous and efficient.

CORBA Common Object Request Broker Architecture. Specification that provides the standard interface definition between OMG-compliant objects. CORBA allows applications to communicate with one another no matter where they are located or who has designed them.

CoS class of service. An indication of how an upper-layer protocol requires a lower-layer protocol to treat its messages. In SNA subarea routing, CoS definitions are used by subarea nodes to determine the optimal route to establish a given session. A CoS definition comprises a virtual route number and transmission priority field. Repetitive, regularly timed signals are used to control synchronous processes.

CWI Craft Works Interface. Graphical user interface (GUI) used to configure and operate a router. The CWI client runs in a web browser.

D

DDTS distributed defect tracking system. A method to track software errors and resolutions.

DHCP Dynamic Host Configuration Protocol. Provides a mechanism for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them.

DIMM dual in-line memory module. Small circuit boards carrying memory integrated circuits, with signal and power pins on both sides of the board, in contrast to single-in-line memory modules (SIMMs).

disk0 Name of the flash disk on which the Cisco IOS XR software is stored.

disk1 Name of the optional flash disk on which the Cisco IOS XR software can be stored in preparation for installation or upgrade.

DNS Domain Name System. Mechanism used in the Internet and on private intranets for translating names of host computers into addresses. The DNS also allows host computers not directly on the Internet to have a registered name in the same style.

DPT Dynamic Packet Transport. DPT rings are dual, counter-rotating fiber rings. Both fibers are used concurrently to transport both data and control traffic.

DSC designated shelf controller. The RP or RP pair that controls a standalone router or a multishelf system. The DSC is selected from among the route processors (RPs) installed in the router or multishelf system.

E

eBGP external Border Gateway Protocol. BGP sessions are established between routers in different autonomous systems. eBGPs communicate among different network domains.

ECC error correction code. ECC is used to correct errors within memories on the Cisco CRS-1 router.

egress Outgoing channel.

Ethernet Baseband LAN specification invented by Xerox Corporation and developed jointly by Xerox, Intel, and Digital Equipment Corporation. Ethernet networks use CSMA/CD and run over a variety of cable types at 10 Mbps. Ethernet standards are defined by the IEEE 802.3 specification.

F

fabric Connectivity between all line cards. Also referred to as switch fabric.

fabric cable Fabric cables are optical array cables that interconnect the fabric components in each chassis of a Cisco CRS-1 Carrier Routing System Multishelf System. Each fabric cable contains 72 fiber-optic strands, which are packaged as 6 ribbon cables with 12 fibers in each ribbon cable.

FC fan controller. Two fan controller cards are installed in every line card chassis as a redundant pair to manage the fan assemblies; a BITS timing connector exists on the fan controller card.

FIB Forwarding Information Base. Database that stores information about switching of data packets. A FIB is based on information in the Routing Information Base (RIB). It is the optimal set of selected routes that are installed in the line cards for forwarding. See also *RIB*.

flooding Traffic-passing technique used by switches and bridges in which traffic received on an interface is sent out all the interfaces of that device except the interface on which the information was originally received.

forwarding Process of sending a frame toward its ultimate destination by way of an internetworking device.

FRR fast reroute. Automatically reroutes traffic on a label switch path (LSP) if a node or link in an LSP fails. FRR reduces the loss of packets traveling over an LSP.

FTP File Transfer Protocol. Application protocol, part of the TCP/IP protocol stack, used for transferring files between network nodes. FTP is defined in RFC 959.

G

GE Gigabit Ethernet. Standard for a high-speed Ethernet, approved by the IEEE 802.3z standards committee in 1996.

Gigabit Ethernet Standard for a high-speed Ethernet, approved by the IEEE 802.3z standards committee in 1996.

GUI graphical user interface. A user environment that uses pictorial and textual representations of the input and output of applications and the hierarchical or other data structure in which information is stored. Such conventions as buttons, icons, and windows are typical, and many actions are performed using a pointing device (such as a mouse). Microsoft Windows and the Apple Macintosh are prominent examples of platforms using a GUI. See also *CLI*.

H

HA High availability is defined as the continuous operation of systems. For a system to be available, all components, including application and database servers, storage devices, and the end-to-end network, need to provide continuous service.

HDLC high-level data link control. ISO communications protocol used in X.25 packet-switching networks. HDLC provides error correction at the data link layer and contains the following subsets: LAPB and SDLC.

hexadecimal A number system having 16 as its base. This number representation uses the digits 0–9, with their usual meaning, plus the letters A–F (or a–f) to represent hexadecimal digits with values of (decimal) 10 to 15. The far right digit counts ones, the next counts multiples of 16, then 16^2 = 256, and so on.

Hexadecimal is more succinct than binary for representing bit masks, machines addresses, and other low-level constants but it is still reasonably easy to split a hex number into different bit positions. For example, the top 16 bits of a 32-bit word are the first four hex digits.

hop Passage of a data packet between two network nodes (for example, between two routers). See also *hop count*.

hop count Routing metric used to measure the distance between a source and a destination.

HTTP Hypertext Transfer Protocol. Used by web browsers and web servers to transfer files, such as text and graphic files. HTTP is the set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. Relative to the TCP/IP suite of protocols (which are the basis for information exchange on the Internet), HTTP is an application protocol.

I

ICMP Internet Control Message Protocol. Network layer Internet (TCP/IP) protocol that reports errors and provides other information relevant to IP packet processing.

IEP IP explicit path. List of IP addresses, each representing a node or link in the explicit path.

IETF Internet Engineering Task Force. Task force consisting of over 80 working groups responsible for developing Internet standards. The IETF operates under the auspices of ISOC.

IGMP Internet Group Management Protocol. Governs the management of multicast groups in a TCP/IP network. Used by IP hosts to report their multicast group memberships to an adjacent multicast router.

IGP Interior Gateway Protocol. Internet protocol used to exchange routing information within an autonomous system. Examples of common Internet IGPs include IGRP, OSPF, and RIP. See also *OSPF* and *RIP*.

ingress Incoming channel.

installed software set The set of Cisco IOS XR software packages installed on a router.

IOS XR The Cisco operating system used on the Cisco CRS-1 router and Cisco XR 12000 Series Router.

IP Internet Protocol. Network layer protocol in the TCP/IP stack offering a connectionless internetwork service. IP provides features for addressing, type-of-service specification, fragmentation and reassembly, and security.

IPv4 IP Version 4. Network layer for the TCP/IP protocol suite. A connectionless, best-effort packet switching protocol.

IPv6 IP Version 6. Replacement for IPv4. A next-generation IP protocol. IPv6 is backward compatible with and designed to fix the shortcomings of IPv4, such as data security and maximum number of user addresses. IPv6 increases the address space from 32 to 128 bits, providing for an unlimited number of networks and systems. It also supports quality of service (QoS) parameters for real-time audio and video.

IPX Internetwork Packet Exchange. NetWare network layer (Layer 3) protocol used for transferring data from servers to workstations. IPX is similar to IP and XNS.

IS-IS Intermediate System-to-Intermediate System. OSI link-state hierarchical routing protocol based on DECnet Phase V routing, whereby ISs (routers) exchange routing information based on a single metric to determine network topology.

K

keepalive interval Period of time between each keepalive message sent by a network device.

keepalive message Message sent by one network device to inform another network device that the virtual circuit between the two is still active.

L

Layer 2 Layer 2 refers to the data link layer of the commonly referenced multilayered communication model, Open Systems Interconnection (OSI). The data link layer contains the address inspected by a bridge or switch. Layer 2 processing is faster than layer 3 processing, because less analysis of the packet is required.

Layer 3 Layer 3 refers to the network layer of the commonly referenced multilayered communication model, Open Systems Interconnection (OSI). The network layer is concerned with knowing the address of the neighboring nodes in the network, selecting routes and quality of service, and recognizing and forwarding to the transport layer incoming messages for local host domains.

A router is a Layer 3 device, although some newer switches also perform Layer 3 functions. The Internet Protocol (IP) address is a Layer 3 address.

LC line card. Line cards in the Cisco CRS-1 system are referred to as modular services cards (MSCs).

LDP label distribution protocol. A standard protocol between MPLS-enabled routers to negotiate the labels (addresses) used to forward packets. The Cisco proprietary version of this protocol is the Tag Distribution Protocol (TDP).

LIB Label Information Base. The table that contains the labels in use on the node.

loopback Send the outgoing signals back to the receiving side for testing.

M

MAC address Standardized data link layer address that is required for every port or device that connects to a LAN. Other devices in the network use these addresses to locate specific ports in the network and to create and update routing tables and data structures. MAC addresses are 6 bytes long and are controlled by the IEEE. Also known as a hardware address, MAC layer address, and physical address.

mask Pattern of bits used to reject or accept bit patterns in another set of data.

MBI minimum boot image. Software image containing a kernel and minimum set of drivers and components to boot a node.

Mbps megabits per second. A bit rate expressed in millions of binary bits per second. 1 megabit = 2^{20} bits, or 1,048,576 bits.

MIB Management Information Base. Database of network management information that is used and maintained by a network management protocol like Simple Network Management Protocol (SNMP). The value of an MIB object can be changed or retrieved using SNMP commands, usually through a GUI network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

MPLS Multiprotocol Label Switching. Switching method that forwards IP traffic using a label. This label instructs the routers and switches in the network where to forward the packets based on pre-established IP routing information

MPLS TE Multiprotocol Label Switching traffic engineering. A switching method that forwards IP traffic using a label. This label instructs the routers and switches in the network where to forward the packets based on pre-established IP routing information.

MSC modular services card. Module in which the ingress and egress packet processing and queueing functions are carried out in the Cisco CRS-1 architecture. Up to 16 MSCs are installed in a line card chassis; each MSC must have an associated physical line interface module (PLIM) (of which there are several types to provide a variety of physical interfaces). The MSC and PLIM mate together on the line card chassis midplane. See also *PLIM*.

MSCs are also referred to as line cards.

MTU maximum transmission unit. Maximum packet size, in bytes, that a particular interface can handle.

multicast Multicast is a feature that refers to single packets copied by the network and sent to a specific subset of network addresses. These addresses are specified in the Destination Address Field. See also *unicast*.

N

netboot Loading software images from a network server, such as TFTP.

node A card installed and running on the router.

NSF nonstop forwarding. Packets keep flowing during events such as failover, process restarts, and the upgrade or downgrade of software packages. Nonstop forwarding is the ability of a router to continue to forward traffic toward a router that may be recovering from a transient failure and the ability of a router recovering from a transient failure in the control plane to continue correctly forwarding traffic sent to it by a peer.

NTP Network Time Protocol. Protocol built on top of TCP that ensures accurate local time-keeping with reference to radio and atomic clocks located on the Internet. This protocol is capable of synchronizing distributed clocks within milliseconds over long time periods.

NVRAM nonvolatile RAM. Static random access memory that is made into nonvolatile storage by having a battery permanently connected.

O

OC-x Optical carrier, where x=3, 12, 48, or 192, relating to the various speeds within a SONET network.

OIR online insertion and removal. Feature that permits the addition, replacement, or removal of cards without interrupting the system power, entering console commands, or causing other software or interfaces to shut down. Sometimes called hot-swapping or power-on servicing.

OSI Open Systems Interconnection. International standardization program created by ISO and ITU-T to develop standards for data networking that facilitate multivendor equipment interoperability.

OSPF Open Shortest Path First. Link-state, hierarchical Interior Gateway Protocol (IGP) routing algorithm proposed as a successor to Routing Information Protocol (RIP) in the Internet community. OSPF features include least-cost routing, multipath routing, and load balancing. OSPF was derived from an early version of the Intermediate System-to-Intermediate System (IS-IS) protocol. See also *IGP* and *RIP*.

P

package A group of software components installed on the router.

packet Logical grouping of information that includes a header containing control information and (usually) user data. Packets most often are used to refer to network layer units of data.

Packet over SONET/SDH POS. Packet over SONET/SDH enables core routers to send native IP packets directly over SONET or SDH frames.

PAP Password Authentication Protocol. Authentication protocol that allows PPP peers to authenticate one another. The remote router attempting to connect to the local router is required to send an authentication request. Unlike Challenge Handshake Authentication Protocol (CHAP), PAP passes the password and the hostname or username in the clear (unencrypted). PAP does not itself prevent unauthorized access but merely identifies the remote end. The router or access server then determines whether that user is allowed access. PAP is supported only on PPP lines. See also *PPP*.

PCMCIA Personal Computer Memory Card International Association. Standard for credit card-size memory or I/O device.

PIE package installation envelope. An installable software file with the suffix *pie*. A PIE may be a package or a Software Maintenance Upgrade (SMU). A PIE is used to deliver Cisco IOS XR software. A PIE may contain a single component, group of components (called a package), or set of packages. When a PIE contains more than one component, it is called a “Composite PIE.”

PLIM Physical layer interface module. Provides the physical interface for a line card. Also handles media-specific functions, such as framing, clock recovery, channelization, and optical signaling for line interfaces connecting to a Cisco CRS-1 router.

PM performance monitoring. Provides a variety of automatic functions to aid in the maintenance and operation of the network. PM is continuous, in-service monitoring of transmission quality that uses software-provisionable performance parameters. Performance parameters are measured for all four layers of the SONET signal: physical, section, line, and STS path.

POS Packet over SONET/SDH. POS enables core routers to send native IP packets directly over Synchronous Optical Network (SONET) or Synchronous Digital Hierarchy (SDH) frames.

PPP Point-to-Point Protocol. Successor to SLIP that provides router-to-router and host-to-network connections over synchronous and asynchronous circuits. Whereas SLIP was designed to work with IP, PPP was designed to work with several network layer protocols, such as IP, IPX, and ARA. PPP also has built-in security mechanisms, such as CHAP and PAP. PPP relies on two protocols: LCP and NCP.

primary RP The first route processor configured for DSC or logical router operation. If a second RP is configured as a redundant RP, it becomes the secondary RP.

Q

QoS quality of service. A set of parameters that describes a flow of data, such as guaranteed bandwidth, delay, and delivery guarantee.

R

RCP remote copy protocol. A protocol that allows users to copy files to and from a file system residing on a remote host or server on the network. The RCP protocol uses TCP to ensure the reliable delivery of data.

RIB Routing Information Base. This is the set of all available routes from which to choose the FIB. The RIB essentially contains all routes available for selection. Essentially, it is the sum of all routes learned by dynamic routing protocols, all directly attached networks (that is. networks to which a given router has interfaces connected), and any additional configured routes, such as static routes.

RIP Routing Information Protocol. A simple routing protocol that is part of the TCP/IP protocol suite and the most common IGP in the Internet. RIP determines a route based on the smallest hop count between source and destination. It is a distance vector protocol that broadcasts routing information to neighboring routers. It is known to use excessive bandwidth. See also *hop count* and *IGP*.

ROM Monitor ROM Monitor is a bootstrap program that initializes the hardware and boots the system when a router is powered on or reset. ROM Monitor mode is also known as “ROMMON,” which reflects the CLI prompts for the mode.

```
rommon B1> (Cisco CRS-1 routers)
```

or

```
rommon1> (Cisco XR 12000 Series Routers)
```

ROMMON See ROM Monitor.

router Network layer device that uses one or more routing metrics to determine the optimal path along which network traffic should be forwarded. Routers forward packets from one network to another based on network layer information.

routing Process of finding a path to a destination host. Routing is very complex in large networks because of the many potential intermediate destinations a packet might traverse before reaching its destination host.

routing metric A routing algorithm determines that one route is better than another. This information is stored in routing tables. Metrics include bandwidth, communication cost, delay, hop count, load, MTU, path cost, and reliability. Sometimes referred to simply as a metric. See also *algorithm*.

routing protocol Protocol that accomplishes routing through the implementation of a specific routing algorithm. Examples of routing protocols include BGP, OSPF, and IS-IS.

routing table Table stored in a router or some other internetworking device that keeps track of routes to particular network destinations and, in some cases, metrics associated with those routes.

RP route processor. Cards that contain run-control software on the router. Two RPs are installed as a redundant pair in dedicated slots in the front of each line card chassis.

RPF Reverse Path Forwarding. Multicasting technique in which a multicast datagram is forwarded from all but the receiving interface if the receiving interface is the one used to forward unicast datagrams to the source of the multicast datagram.

RSVP Resource Reservation Protocol. Protocol that supports the reservation of resources across an IP network. Applications running on IP end systems can use RSVP to indicate to other nodes the nature (bandwidth, jitter, maximum burst, and so on) of the packet streams they want to receive. RSVP depends on IPv6. Also known as Resource Reservation Setup Protocol. See also *IPv6*.

running configuration The router configuration currently in effect. Although the user can save multiple versions of the router configuration for future reference, only one copy of the running configuration exists in the router at any given time.

Rx The receiver end of a fabric link. All links are unidirectional. See also *Tx*.

S

SCFC shelf controller/fan controller. Combines shelf controller function and fan controller function on one card. Two are installed in each fabric chassis.

SDH Synchronous Digital Hierarchy. European standard that defines a set of rate and format standards that are sent using optical signals over fiber. SDH is similar to SONET, with a basic SDH rate of 155.52 Mbps, designated at STM-1.

SDR secure domain router. A collection of line cards and route processors that form a complete router. Each router contains its own instance of dynamic routing, IP stack, system database, interface manager, and event notification system.

SDRAM synchronous dynamic random access memory. A form of dynamic RAM that adds a separate clock signal to the control signals.

shelf controller The hardware component that manages the configuration and health of a fabric chassis within the Cisco CRS-1 router.

shelf manager The shelf manager process runs on a router or switch, doing platform-dependent functions, including handling OIR events. Shelf manager is formerly called platform manager.

SMU Software Maintenance Upgrade. A “point fix” for a critical problem. SMUs are delivered as PIE files and are used to update software packages.

SNMP Simple Network Management Protocol. SNMP is the protocol governing network management and the monitoring of network devices and their functions. It is not necessarily limited to TCP/IP networks.

SNMPv3 Simple Network Management Protocol Version 3. An interoperable standards-based protocol for network management. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network.

software configuration A list of packages activated for a particular node. A software configuration consists of a boot package and additional feature packages.

SONET Synchronous Optical Network. A standard format for transporting a wide range of digital telecommunications services over optical fiber. SONET is characterized by standard line rates, optical interfaces, and signal formats. See also *SDH*.

SP service processor. An SP on each card maintains an internal management connection to the shelf controller for the rack. The SP is referred to in CLI commands to identify the nodeID for fabric, alarm and fan controller cards.

Example:

```
RP/0/RPO/CPU:router# admin show controllers fabric connectivity location 0/SM0/SP
```

SPE Synchronous Payload Envelope. Portion of the SONET frame containing overhead information (POH and user data).

SPF shortest path first. Routing algorithm that iterates on length of path to determine a shortest-path spanning tree. Commonly used in link-state routing algorithms. Sometimes called Dijkstra's algorithm.

SSH Secure Shell. A protocol that provides a secure remote connection to a router through a Transmission Control Protocol (TCP) application.

SSL secure socket layer. A secure socket between two entities with authentication.

standby Denotes an inactive card or process that waits to become active; standby cards or processes are also sometimes denoted as backup.

startup configuration The router configuration designated to be applied on the next router startup.

subinterface Virtual interfaces created on a hardware interface. These software-defined interfaces allow for segregation of traffic into separate logical channels on a single hardware interface and better utilization of the available bandwidth on the physical interface.

switchover A switch between the active and standby cards. The switchover can be initiated by command, or it can occur automatically when the active card fails.

system reload Reload of a router node.

system restart Soft reset of a router node. This involves restarting all processes running on that node.

T

TAC Cisco Technical Assistance Center.

TACACS Terminal Access Controller Access Control System. Authentication protocol, developed by the DDN community, that provides remote access authentication and related services, such as event logging. User passwords are administered in a central database rather than in individual routers, providing an easily scalable network security solution.

tar A tar file is a file produced by the UNIX tar program, which packages multiple files in a single file for distribution as a single unit. Each tar file has a *tar* filename extension.

target configuration A "two-stage" configuration of the Cisco IOS XR software running configuration. This allows users to make changes to the running configuration and accept these changes by entering the **commit** command.

task ID An identifier that determines user access to a given command or series of commands. A user must be a member of a group with the appropriate task IDs assigned to it to execute the related commands.

Tbps terabits per second. The amount of data that can be sent in a fixed amount of time. 1 terabit = 2^{40} bits, or 1,099,511,627,776 bits.

TCP Transmission Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack.

Telnet Standard terminal emulation protocol in the TCP/IP protocol stack. Telnet is used for remote terminal connection, enabling users to log in to remote systems and use resources as if they were connected to a local system. Telnet is defined in RFC 854.

terabyte A unit of computer memory or data storage capacity equal to 1024 gigabytes (2^{40} bytes). Approximately 1 trillion bytes.

TFTP Trivial File Transfer Protocol. A simplified version of FTP that allows files to be transferred from one computer to another over a network, usually without the use of client authentication (for example, username and password).

Note: some TFTP servers (such as Sun Solaris) may not support file sizes larger that 32 MB.

trap Message sent by an SNMP agent to an NMS, a console, or a terminal to indicate the occurrence of a significant event, such as a specifically defined condition or a threshold that was reached.

tunnel Secure communication path between two peers, such as two routers.

Tx The transmitter end of a fabric link. All links are unidirectional. See also Rx.

U

UDP User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP is defined in RFC 768.

unicast Message sent to a single network destination.

unicast transmission A unicast transmission sends one copy of each packet to each member of the group. This method is inefficient because the same information must be carried multiple times, requiring extra bandwidth.

V

VCSEL vertical cavity surface emitting laser.

vm A vm file is a Cisco IOS XR software file that can be installed from ROM Monitor mode. A vm file is typically used to install the Cisco IOS XR software when the software has not yet been installed or has been corrupted.

VPN Virtual Private Network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses “tunneling” to encrypt all information at the IP level.

W

WRED Weighted Random Early Detection. Queueing method that ensures that high-precedence traffic has lower loss rates than other traffic during times of congestion.

X

XML Extensible Markup Language. A standard maintained by the World Wide Web Consortium (W3C) that defines a syntax that lets you create markup languages to specify information structures. Information structures define the type of information, for example, subscriber name or address, not how the information looks (bold, italic, and so on). External processes can manipulate these information structures and publish them in a variety of formats. XML allows you to define your own customized markup language.

XML agent A process on the router that is sent XML requests by XML clients and is responsible for carrying out the actions contained in the request and returning an XML response back to the client. The XML Agent for CORBA is an example of an XML agent provided on the Cisco CRS-1 router.

XML client An external application that sends an XML request to the router and receives XML responses to those requests.

XML operation A portion of an XML request that specifies an operation that the XML client would like the XML agent to perform.

XML operation provider The router code that carries out a particular XML operation including parsing the operation XML, performing the operation, and assembling the operation XML response

XML request An XML document sent to the router containing a number of requested operations to be carried out.

XML response The response to an XML request.

XML schema An XML document specifying the structure and possible contents of XML elements that can be contained in an XML document.

Symbols

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

W

X