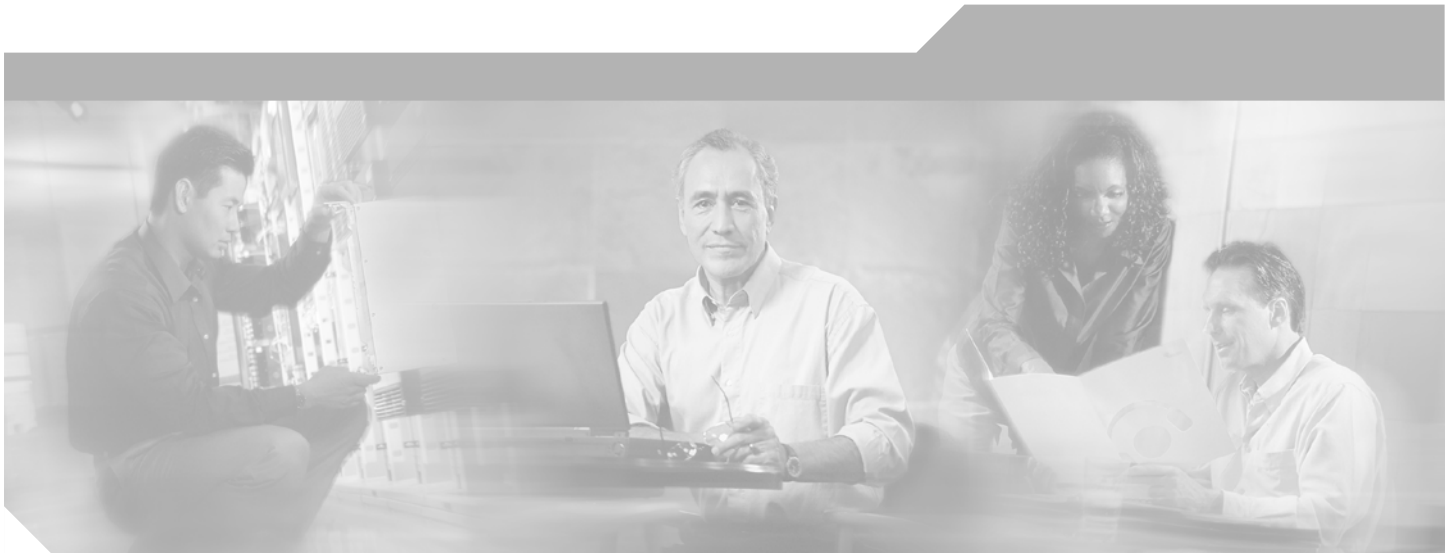

Cisco IOS XR Command Modes Reference

Cisco IOS XR Software Release 3.3

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-8536-01

Cisco IOS XR Multicast Configuration Guide

CONTENTS

Preface

This reference contains descriptions of the modes that are available in the user command-line interface (CLI) that is supported by Cisco IOS XR software.

The first chapter describes the command and configuration modes used in the CLI. These descriptions include short summaries and example applications of the modes.

The second chapter of this reference contains a table that identifies each CLI mode by the appearance of the prompt. For each mode, this table includes an example of how you enter mode.

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-8536-01	April 2006	Initial release of the document.

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/univercd/home/home.htm

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

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/

Cisco Marketplace:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments 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 can perform these tasks:

- 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 and notices for Cisco products is available at this URL:

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from 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 might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on

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

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

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support 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, 365 days a year, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support 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 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 TAC 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 TAC 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)—Your 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 operation 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 your network is impaired, but 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.

- Cisco Marketplace provides a variety of Cisco books, reference guides, 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

- *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

- 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

Cisco IOS XR Command Mode Descriptions

This document describes the command and configuration modes used in the Cisco IOS XR command line interface (CLI). The availability of configuration modes depends on the software packages that are installed on your system and on which router platform you are using. For more information on a particular configuration mode, refer to the command reference or configuration that is related to the mode described in this module.

This module describes the command modes in the following sections:

Following the mode definitions in this module, the next module contains a table that identifies the router prompts in alphabetical order. This table shows where the prompt exists in the CLI and how you get to the prompt. It also has examples of command sequences that could get you to a particular prompt.

Base Command Modes

Base command modes are used for navigating the CLI and performing basic router startup, configuration, and monitoring tasks.

EXEC Mode

Prompt: (router)

The default command mode for the CLI is EXEC mode. In general, the EXEC commands let you connect to remote devices, change terminal settings on a temporary basis, perform basic tests, and list system information. Most CLI commands in EXEC mode do not change system operation. The most common EXEC commands are **show** commands (to display router configuration or operational data) and **clear** commands (to clear or reset system counters).

ROM Monitor Mode

Prompt: rommon B*n*>

If your router or access server does not find a valid system image to load, the user interface enters read-only memory (ROM) monitor mode. ROM monitor (ROMMON) mode can also be accessed by interrupting the boot sequence during startup. From ROM monitor mode, you can boot the device or perform diagnostic tests.

To enter ROM monitor mode, use the Break (Ctrl-C) during the first 60 seconds of startup. The router prompt consists of an angle bracket by itself or "rommon" followed by the letter B a number, and an angle bracket: `>` or `rommon B1>`. The number after the B increments upon each user-entry.

Setup Mode

Setup mode is not actually a command mode. Setup mode is an interactive facility that lets you perform first-time configuration and other basic configurations on all routers. The facility prompts you to enter basic information needed to start a router functioning. Setup mode uses the system configuration dialog, which guides you through the configuration process. It prompts you first for global parameters and then for interface parameters. The values shown in brackets next to each prompt are the default values.

To enter setup mode after the router has been configured for the first time, use the **setup** command in admin EXEC mode. The router prompt for setup mode is indicated by a configuration question, followed by the default answer in brackets and a colon (:), as shown in the following example:

```
Continue with configuration dialog? [yes]:
Enter host name [Router]:
```

User Configuration Modes

The remaining sections of this module describe each mode you can access during regular operation.

Address Family Configuration Mode

Prompts:

- For BGP: (config-bgp-af)
- For OSPF: (config-ospfv-af)
- For OSPFv3: (config-ospfv3-af)
- For EIGRP: (config-eigrp-af)

For IS-IS, see Router Address Family Configuration Mode.

Enter one of the address family configuration modes from router configuration mode. Address family configuration mode is available for the BGP, OSPF, OSPFv3, and EIGRP protocols. This mode is the highest-level address family configuration mode. This mode is also called *global address family* configuration mode.

For BGP only, address family configuration is available in four modes. In addition to this section, see also Address Family Group Configuration Mode, Neighbor Address Family Configuration Mode, or Neighbor Group Address Family Configuration Mode.

For example, first enter BGP router configuration mode, then address family configuration mode:

```
RP/0/RP0/CPU0:router(config)# router bgp 1
RP/0/RP0/CPU0:router(config-bgp)# address-family ipv6 unicast
RP/0/RP0/CPU0:router(config-bgp-af)#
```

Address Family Group Configuration Mode

Prompt: (config-bgp-afgrp)

Enter address family group configuration mode from router configuration mode for BGP. In this group configuration mode, you can configure characteristics of an address family group that a neighbor uses. Furthermore, neighbors inherit the configuration parameters of the entire address family group.

For example, create an address family group with the name newgroup1 and an address family of IPv4 unicast. The CLI subsequently enters address family group configuration mode. In address family group mode, you configure the next-hop-self feature, so that all neighbors that use address family newgroup1 inherit the next-hop-self configuration:

```
RP/0/RP0/CPU0:router(config)# router bgp 100
RP/0/RP0/CPU0:router(config-bgp)# af-group newgroup1 address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-bgp-afgrp)# next-hop-self
```

Administration Configuration Mode

Prompt: (admin-config)

Enter administration configuration (admin config) mode from administration EXEC mode. The primary application of administration configuration mode is to let you:

- Configure service domain routers (SDRs).
- Control individual card slots. For example, you can turn power on or off at a slot.

For SDRs, this mode is used primarily to display system-wide parameters, configure the administration plane over the control Ethernet, and configure SDRs on a multishelf a system. These operations are available at the root level.

For example, first enter the administration EXEC mode, and then use the **configure** command to enter administration configuration mode:

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

Administration EXEC Mode

Prompt: (admin)

Enter administration executive (admin EXEC) mode from EXEC mode. The admin EXEC mode applies primarily to secure domain routers (SDRs). When SDRs have been configured, the EXEC mode provides visibility into only one SDR, so you must enter administration EXEC mode to see all system parameters. To display system-wide parameters, configure the administration plane over the control Ethernet, and configure SDRs on multishelf systems, use administration EXEC mode and administration configuration mode.

For example, enter the admin EXEC mode:

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

APS Group Configuration Mode

Prompt: (config-aps)

Enter automatic protection switching (APS) group configuration mode by using the **aps group** command in global configuration mode. The SONET/SDH APS feature offers recovery from fiber (external) or equipment (interface and internal) failures at the SONET/SDH line layer. The **aps group** command either creates a new group or identifies an existing group. The group numbers have a range of 1 to 255. APS requires the creation of an APS group for each protection port and its corresponding working port.

For example, use the **authenticate** command in APS group configuration mode to specify abctown as the authentication string for APS group 1:

```
RP/0/RP0/CPU0:router(config)# aps group 1
RP/0/RP0/CPU0:router(config-aps)# authenticate abctown
```

For example, configure SONET port 0/2/0/2 to be a local protection channel in APS group 1:

```
RP/0/RP0/CPU0:router(config)# aps group 1
RP/0/RP0/CPU0:router(config-aps)# channel 0 local SONET 0/2/0/2
```

For example, configure the remote channel with IP address 192.168.1.1 to be the working channel for APS group 1:

```
RP/0/RP0/CPU0:router(config)# aps group 1
RP/0/RP0/CPU0:router(config-aps)# channel 1 remote 192.168.1.1
```

Area Configuration Mode

Prompt: (config-ospf-ar)

Enter area configuration mode from router configuration mode. The pertinent router modes for area configuration apply to OSPF and OSPFv3. Commands that run in area configuration mode (such as the **interface** and **authentication** commands), are automatically bound to that area.

For example, after you enter router configuration mode for OSPF, create area 0. The CLI enters area configuration mode where, in this example, you specify Packet-over-SONET/SDH (POS) interface 0/2/0/0. By definition of an area, interface 0/2/0/0 is bound to area 0:

```
RP/0/RP0/CPU0:router(config)# router ospf 1
RP/0/RP0/CPU0:router(config-router)# area 0
RP/0/RP0/CPU0:router(config-ospf-ar)# interface POS 0/2/0/0
```

BGP Confederation Peers Configuration Mode

Prompt: (config-bgp-confed-peers)

Enter BGP confederation peer configuration mode by using the **bgp confederation peers** command in BGP router configuration mode. In this mode, you can specify multiple autonomous systems (one autonomous-system-number) on each command line.

For example, configure multiple autonomous systems in BGP confederation peer configuration mode:

```
RP/0/RP0/CPU0:router(config)# router bgp 1095
RP/0/RP0/CPU0:router(config-bgp)# bgp confederation peers
RP/0/RP0/CPU0:router(config-bgp-confed-peers)# 1096
RP/0/RP0/CPU0:router(config-bgp-confed-peers)# 1097
RP/0/RP0/CPU0:router(config-bgp-confed-peers)# 1098
```

Class Map Configuration Mode

Prompt: (config-cmap)

Enter class map configuration mode from global configuration mode by using the **class-map** command. Use the **class-map command** to create a new class map or identify an existing map. The CLI then goes into class map configuration mode so you can create the quality of service (QoS)-related configuration of the class map. For details on policies and classes in QoS, see *Quality of Service Commands on Cisco IOS XR Software* or *Cisco IOS XR Modular Quality of Service Configuration Guide*.

For example, create a class map with the name class1:

```
RP/0/RP0/CPU0:router(config)# class-map class1
RP/0/RP0/CPU0:router(config-cmap)#
```

Crypto IPSec Transport

Prompt: (config-transport)

Enter IP Security (IPSec) transport configuration mode by using the **crypto ipsec transport** command in global configuration mode. IPSec protects the Upper Layer Protocol (ULP) header and the payload. IPSec transport mode supports end-to-end security (in which security endpoints match the host endpoints). All transport mode IPSec traffic must be configured in crypto ipsec transport mode.

For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

For example, enter IPSec transport configuration mode, and then configure a crypto profile:

```
RP/0/RP0/CPU0:router(config)# crypto ipsec transport
RP/0/RP0/CPU0:router(config-transport)# profile pn1
```

Distributed Route Processor Pairing Mode

Prompt: (admin-config-pairing:*drp_name*)

Enter pairing configuration mode for distributed route processors (DRPs) by using the **pairing c**ommand in administrative configuration mode. After you name a new or existing DRP pair, the CLI enters DRP pairing configuration mode. The prompt for this mode contains the name of the DRP pair.

For example, create a DRP pair, and assign two DRP nodes to the pair name:

```
RP/0/RP1/CPU0:router# admin
RP/0/RP1/CPU0:router(admin)# config
RP/0/1/CPU0:router(admin-config)# pairing drp1
RP/0/1/CPU0:router(admin-config-pairing:drp1)# location 0/3/* 0/4/*
```

DWDM Controller Mode

Prompt: (config-dwdm)

Enter controller mode for dense wave division multiplexing (DWDM) by using the **controller dwdm** command in global configuration mode and then configure parameters for a particular DWDM instance.

For example, enter the controller mode for DWDM on interface 0/6/0/0:

```
RP/0/0/CPU):router(config)# controller dwdm 0/6/0/0
RP/0/RP0/CPU0:router(config-dwdm)#
```

Explicit Path Configuration Mode

Prompt: (config-expl-path)

Enter explicit path configuration mode from global configuration mode by using the **explicit-path** command. This mode applies to the Multiprotocol Label Switching (MPLS) traffic engineering (TE) feature. After the CLI enters explicit path Multiprotocol configuration mode, use the **disable**, **exclude-address**, **next-address**, or **show explicit-paths** command to modify or display the IP explicit path that you identified to the **explicit-path** command.

For example, exclude IP addresses 192.168.3.2 and 192.168.4.2 from IP explicit path 200:

```
RP/0/RP0/CPU0:router(config)# explicit-path identifier 200
RP/0/RP0/CPU0:router(config-expl-path)# exclude-address 192.168.3.2
RP/0/RP0/CPU0:router(config-expl-path)# exclude-address 192.168.4.2
```

For example, remove IP address 192.168.3.2 from the excluded addresses for path 200:

```
RP/0/RP0/CPU0:router(config)# explicit-path identifier 200
RP/0/RP0/CPU0:router(config-expl-path)# no index 1
```

For example, disable explicit path 200:

```
RP/0/RP0/CPU0:router(config)# explicit-path identifier 200
RP/0/RP0/CPU0:router(config-expl-path)# disable
```

Global Address Family Configuration Mode

Prompts: See "Address Family Configuration Mode" for OSPF and BGP or "Router Address Family Configuration Mode" for IS-IS.

Enter global address family configuration mode from the router configuration mode for a particular protocol: BGP, IS-IS, OSPF, or OSPFv3. Global address family configuration mode is the highest level of address family configuration. With BGP only, you can go to other levels for configuration of address family details. For more specific information, see "Address Family Configuration Mode" or "Router Address Family Configuration Mode" for IS-IS.

Global Configuration Mode

Prompt: (config)

Enter global configuration mode from executive (EXEC) mode by using the **configure** command. Global configuration commands generally apply to the whole system rather than just one protocol or interface. You can enter all other configuration submodes listed in this section from global configuration mode.

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

HSRP Interface Configuration Mode

Prompt: (config-hsrp-if)

Enter interface configuration mode for Hot Standby Router Protocol (HSRP) by using an **interface** command in router HSRP configuration mode. In this mode, you can configure details of the HSRP for a specific interface.

For details on the application of this mode, see the *Cisco IOS XR IP Addresses and Services Configuration Guide*.

For example, configure "company1" as the authentication string required to allow interoperation of hot standby routers in group 1 on the Ten Gigabit Ethernet interface 0/2/0/1:

```
RP/0/RP0/CPU0:router(config)# router hsrp
RP/0/RP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1
RP/0/RP0/CPU0:router(config-hsrp-if)# hsrp 1 authentication company1
```

Interface Address Family Configuration Mode

Prompt: (config-isis-if-af)

Enter interface address family configuration mode from interface mode (for IS-IS) by using the **address-family** command. In interface address family configuration mode, only the **metric** command is supported. This command lets you assign a specific default cost to a link for routing decisions.

For example, enter router configuration mode for IS-IS, and then specify the Packet-over-SONET (POS/SDH) interface 0/1/0/1. In interface mode, use the **address-family** command to enter interface ipv4 unicast address family configuration mode. Configure the interface for a default link-state metric cost of 15:

```
RP/0/RP0/CPU0:router(config)# router isis isp
RP/0/RP0/CPU0:router(config-isis)# interface POS0/1/0/1
RP/0/RP0/CPU0:router(config-isis-if)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-isis-if-af)# metric 15
```

Interface Configuration Mode

Prompts:

- (config-if)
- (config-isis-if)

Enter interface configuration mode from global configuration mode. At this level and other interface submodes, a wide variety of capabilities are supported, and these capabilities depend on the installed software packages. This document describes the interface modes for specific functional areas.

For this example, the highest level interface configuration mode for Packet-over-SONET/SDH (POS) is entered for the interface identified by 0/2/0/4.

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

For example, enter IS-IS router configuration mode and then interface configuration mode for IS-IS. Specify an IS-IS network entity title (NET) of 49.0000.0000.0001.00. Thereafter, begin configuration of an IPv6 unicast address family:

```
RP/0/RP0/CPU0:router(config)# router isis isp
RP/0/RP0/CPU0:router(config-isis)# net 49.0000.0000.0001.00
RP/0/RP0/CPU0:router(config-isis)# interface POS0/3/0/0
RP/0/RP0/CPU0:router(config-isis-if)# address-family ipv6 unicast
```

Interface Configuration Mode (Protocol Areas)

Prompts:

- (config-ospf-ar-if)
- (config-eigrp-ar-if)

Enter area interface configuration mode from area configuration mode for OSPF, OSPFv3, or EIGRP. The commands in this mode apply to an interface within the area you specify at the area configuration prompt. Routing configurations, such as cost per link for the interface or the number of seconds from one hello packet transmission to the next hello transmission, can be specified for an interface.

For the first example, enter router configuration mode for OSPFv3, and specify area 0. Select interface 0/1/0/1, and assign a cost of 65 for routing decisions.

```
RP/0/RP0/CPU0:router(config)# router ospfv3 201
RP/0/RP0/CPU0:router(config-router)# area 0
RP/0/RP0/CPU0:router(config-ospf-ar)# interface POS 0/1/0/1
RP/0/RP0/CPU0:router(config-ospf-ar-if)# cost 65
```

For the second example, the protocol is an EIGRP instance numbered 1, and the router ID is 10.1.1.1. For POS interface 0/1/0/0, specify a hello interval of 10 seconds.

```
RP/0/RP0/CPU0:router(config)# router eigrp 1
RP/0/RP0/CPU0:router(config-eigrp)# address-family ipv4
RP/0/RP0/CPU0:router(config-eigrp)# router-id 10.1.1.1
RP/0/RP0/CPU0:router(config-eigrp-af)# interface POS 0/1/0/0
RP/0/RP0/CPU0:router(config-eigrp-af-if)# hello-interval 10
```

Interface IGMP Configuration Mode

Prompt: (config-igmp-if)

Enter interface configuration mode for Internet Group Management Protocol (IGMP) from router IGMP configuration mode by using **interface**. For details, see Router IGMP Configuration Mode.

For example, enter router configuration mode for IGMP, then enable explicit tracking for POS/SDH interface 0/1/0/0:

```
RP/0/RP0/CPU0:router(config)# router igmp
RP/0/RP0/CPU0:router(config-igmp)# interface pos 0/1/0/1
RP/0/RP0/CPU0:router(config-igmp-if)# explicit-tracking enable 1
```

Interface Management Configuration Mode

Prompt: (config-if)

Enter management configuration mode be using the **interface MgmtEth** command in global configuration mode.

For example, enter Ethernet management configuration mode for the instance 0/RP0/CPU0/0. For this interface, configure an IPv4 address of 192.168.100.3/24.

```
RP/0/RP0/CPU0:router(config)# interface MgmtEth 0/RP0/CPU0/0
RP/0/RP0/CPU0:router(config-if)# ipv4 address 192.168.100.3/24
```

Interface Mulitcasting Mode

Prompt: (config-mcast-ipv4-if)

Enter multicasting configuration mode for an interface using the **interface** command or other applicable command in multicast router configuration mode. See Multicast Routing Configuration Mode.

For example, enable multicast routing on all interfaces, and then disable the feature on Packet-over-SONET/SDH (POS) interface 0/1/0/0:

```
RP/0/RP0/CPU0:router# multicast-routing
RP/0/RP0/CPU0:router(config-mcast-ipv4)# interface all enable
RP/0/RP0/CPU0:router(config-mcast-ipv4)# interface pos 0/1/0/0
RP/0/RP0/CPU0:router(config-mcast-ipv4-if)# disable
```

Interface PIM Configuration Mode

Prompt: (config-pim-ipv4-if)

Enter the interface submode for Protocol Independent Management (PIM) by using the **interface** command in PIM configuration mode. For more details, see Router PIM Configuration Mode.

For example, configure the router to specify a designated router (DR) priority of 4 for Packet-over-SONET/SDH (POS) interface 0/1/0/0. Other interfaces on the router inherit DR priority 2.

```
RP/0/RP0/CPU0:router(config)# router pim
RP/0/RP0/CPU0:router(config-pim-ipv4)# dr-priority 2
RP/0/RP0/CPU0:router(config-pim-ipv4)# interface pos 0/1/0/0
RP/0/RP0/CPU0:router(config-pim-ipv4-if)# dr-priority 4
```

Interface Preconfiguration Mode

Prompt: (config-if-pre)

Enter the mode for preconfiguring a Packet-over-SONET/SDH interface from template configuration mode. For information on this action, see *Cisco IOS XR System Management Command Reference*.

For example, first create a template named pre-pos. This action places the CLI in template configuration mode. Use the **interface preconfigure** command with POS interface 0/1/0/0 to enter interface preconfiguration mode. For this interface, set the primary IPv4 address to be 10.3.32.154 255.0.0.0. To exit interface preconfiguration mode, use the **end-template** command.

```
RP/0/RP0/CPU0:router(config)# template pre-pos
RP/0/RP0/CPU0:router(config-tpl)# interface preconfigure pos0/1/0/0
RP/0/RP1/CPU0:router(config-if-pre)# ipv4 address 10.3.32.154 255.0.0.0
RP/0/RP1/CPU0:router(config-if-pre)# end-template
```

Interface RIP Configuration Mode

Prompt: (config-rip-if)

Enter interface configuration mode for RIP with the **interface** command in global configuration mode.

For example, send RIP v2 output messages on the POS interface 1/0/0/0:

```
RP/0/RP0/CPU0:router(config)# router rip
RP/0/RP0/CPU0:router(config-rip)# interface POS 1/0/0/0
RP/0/RP0/CPU0:router(config-rip-if)# broadcast-for-v2
```

Interface Session Border Controller Configuration Mode

Prompt: (config-if-sbc)

Enter the interface configuration mode for session border controller (SBC) by using the **interface sbc** command in global configuration mode. If the specified interface does not exist, this command creates it.

For example, create an interface named sbcControlIf:

```
RP/0/RP0/CPU0:router(config)# interface sbc sbcControlIf
RP/0/RP0/CPU0:router (config-if-sbc)#
```

Interface Tunnel Configuration Mode

Prompt: (config-if)

Enter interface configuration mode for tunnels from global configuration mode. Use the **tunnel-ipsec** command for this purpose. After the CLI enters interface configuration mode, the applicable commands for tunnels let you configure a source, destination, and profile. To specify the source address for a tunnel interface, use the **tunnel source** command in interface configuration mode. Use the **tunnel source** command to configure the source address or interface type and the instance for an IP Security tunnel. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

For example, configure the tunnel source to be 172.19.72.92:

```
RP/0/RP0/CPU0:router(config)# interface tunnel-ipsec0
RP/0/RP0/CPU0:router(config-if)# tunnel source 172.19.72.92
RP/0/RP0/CPU0:router(config-if)# tunnel destination 172.19.72.120
RP/0/RP0/CPU0:router(config-if)# profile pn1
```

IP SLA ICMP Echo Configuration Mode

Prompt: (config-ipsla-icmp-echo)

Enter the ICMP echo configuration mode for an IP SLA by using the **type icmp echo** command in IP SLA operation configuration mode.

For example, for IP SLA operation 1, enter ICMP echo configuration mode.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type icmp echo
RP/0/RP0/CPU0:router(config-ipsla-icmp-echo)#
```

IP SLA ICMP Path-Echo Configuration Mode

Prompt: (config-ipsla-icmp-path-echo)

Enter the mode for configuring (ICMP) path echo for IP service level agreement (IP SLA) Internet control messaging protocol (ICMP) by using the **type icmp path-echo** command in IP SLA operation configuration mode.

For example, specify the path for measuring the ICMP echo response time to be 20.25.22.1:

```
RP/0/RP0/CPU0:router(config)# ipsla operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type icmp path-echo
RP/0/RP0/CPU0:router(config-ipsla-icmp-path-echo)# lsr-path 20.25.22.1
```

IP SLA ICMP Path-Jitter Configuration Mode

Prompt: (config-ipsla-icmp-path-jitter)

Enter the mode for configuring the path jitter for IP service level agreement (IP SLA) Internet control messaging protocol (ICMP) by using the **type udp jitter** command in IP SLA operation configuration mode. You can also specify the address of a target device;

For example, use the **type udp jitter** command for IP SLA operation 1 to enter ICMP path jitter configuration mode, then use the **frequency** command to configure a probe period of 60 seconds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/RP0/CPU0:router(config-ipsla-udp-jitter)# frequency 60
```

IP SLA Operation Configuration Mode

Prompt: (config-ipsla-op)

Enter the IP service level agreements (SLAs) configuration mode by entering the **ipsla operation** command in global configuration mode. This command lets you configure numerous elements of an IP SLA. See the *IP Service Level Agreement Commands on Cisco IOS XR Software* module for details on the **ipsla operation** command.

For example, enter IP SLA operation configuration mode for the operation numbered:

```
RP/0/RP0/CPU0:router(config)# ipsla operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp echo
```

IP SLA Operation History Configuration Mode

Prompt: (config-ipsla-op-hist)

Enter the history configuration mode for IP SLA operation by using the **history** command in UDP echo configuration mode. In this mode, you can configure various history-related values by using the **lives**, **filter**, **buckets**, or **samples** command.

For example, enter history configuration mode for operation 1, and then use the **samples** command to specify that the history table hold 30 hops for operation 1:

```
RP/0/RP0/CPU0:router(config)# ipsla operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp echo
RP/0/RP0/CPU0:router(config-ipsla-udp-echo)# history
RP/0/RP0/CPU0:router(config-ipsla-op-hist)# samples 30
```

For example, enter history configuration mode for operation 1, and then use the **buckets** command to specify 30 history buckets for the duration of operation 1:

```
RP/0/RP0/CPU0:router(config)# ipsla operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp echo
RP/0/RP0/CPU0:router(config-ipsla-udp-echo)# history
RP/0/RP0/CPU0:router(config-ipsla-op-hist)# buckets 30
```

IP SLA Operation Statistics Configuration Mode

Prompt: (config-ipsla-op-stats)

Enter the mode for configuring IP SLA operation statistics by using the **statistics** command in IP SLA UDP jitter mode or IP SLA UDP path echo mode.

For example, for the IP SLA operation numbered 1, enter the **statistics** command in ICMP path-echo mode and then configure a maximum of 20 hops in an hour:

```
RP/0/RP0/CPU0:router(config)# ipsla operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type icmp path-echo
RP/0/RP0/CPU0:router(config-ipsla-icmp-path-echo)# statistics hourly
RP/0/RP0/CPU0:router(config-ipsla-op-stats)# maximum hops 20
```

For example, for the IP SLA operation numbered 1, enter the **statistics** command in UDP jitter mode and then configure 10 buckets for per hour:

```
RP/0/RP0/CPU0:router(config)# ipsla operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/RP0/CPU0:router(config-ipsla-udp-jitter)# statistics hourly
RP/0/RP0/CPU0:router(config-ipsla-op-stats)# buckets 10
```

IP SLA Reaction Condition Configuration Mode

Prompt: (config-ipsla-react-cond)

Enter the mode for configuring the condition of an IP SLA reaction by using the **react** command and one or more keywords in IP SLA reaction mode. For a description of these **react** keywords, see the *IP Service Level Agreement Commands on Cisco IOS XR Software* module in *Cisco IOS XR System Management Command Reference*.

The **react** command specifies the event that is to be monitored. In reaction condition mode, you can use the **action** command to specify a trigger or that the event is to be logged.

For example, enter reaction configuration mode for the IP SLA operation numbered 432. Specify that the reaction will be for connection loss, and then specify that the action is to log the event:

```
RP/0/RP0/CPU0:router(config)# ipsla reaction operation 432
RP/0/RP0/CPU0:router(config-ipsla-react)# react connection-loss
RP/0/RP0/CPU0:router(config-ipsla-react-cond)# action logging
```

IP SLA Reaction Configuration Mode

Prompt: (config-ipsla-react)

Enter IP SLA reaction configuration mode by using the **ipsla reaction operation** command in global configuration mode. In this mode, you can configure reactions for a variety of IP SPA events. For a description of the applicable keywords, events, and reactions, see the *IP Service Level Agreement Commands on Cisco IOS XR Software* module in *Cisco IOS XR System Management Command Reference*.

```
RP/0/RP0/CPU0:router(config)# ipsla reaction operation 432
RP/0/RP0/CPU0:router(config-ipsla-react)# react connection-loss
RP/0/RP0/CPU0:router(config-ipsla-react-cond)# action logging
```

IP SLA Responder Configuration Mode

Prompt: (config-ipsla-resp)

Enter IP SLA responder configuration mode by using the **ipsla responder** command in global configuration mode.

For example, enable the IP SLA responder for UDP echo or jitter operation by using the **ipsla responder** command, and then use the **type udp ipv4 address** command to configure a permanent port of 10001 for IP address 12.25.26.10:

```
RP/0/RP0/CPU0:router(config)# ipsla responder
RP/0/RP0/CPU0:router(config-ipsla-resp)# type udp ipv4 address 12.25.26.10 port 10001
```

IP SLA Schedule Configuration Mode

Prompt: (config-ipsla-sched)

Enter the scheduling configuration mode for an IP service level agreements (SLA) by entering the **ipsla schedule operation** command in global configuration mode.

For example, schedule SLA operation number 1 to be recurring:

```
RP/0/RP0/CPU0:router(config)# ipsla schedule operation 1
RP/0/RP0/CPU0:router(config-ipsla-sched)# recurring
```

IP SLA UDP Echo Configuration Mode

Prompt: (config-ipsla-udp-echo)

Enter the UDP echo configuration mode for IP SLA by using the **type udp echo** command in IP SLA operation mode. In UDP echo configuration mode, a substantial number of IP SLA UDP echo values can be configured. To see all applicable commands, refer to the IP SLA command module in the *Cisco IOS XR System Management Configuration Guide*.

For example, enter UDP echo configuration

```
RP/0/RP0/CPU0:router(config)# ipsla operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp echo
RP/0/RP0/CPU0:router(config-ipsla-udp-echo)# history
RP/0/RP0/CPU0:router(config-ipsla-op-hist)# buckets 30
```

For example, enter UDP echo configuration mode for the IP SLA operation numbered 1, and then enter UDP echo mode by using the **type udp echo** command. In this mode, use the **datasize request** command to set the protocol datasize in the payload of an operations request packet 512 bytes:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipsla operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp echo
RP/0/RP0/CPU0:router(config-ipsla-udp-echo)# datasize request 512
```

IP SLA UDP Jitter Configuration Mode

Prompt: (config-ipsla-udp-jitter)

Enter the mode for configuring jitter-related values for IP SLA UDP by using the **type udp jitter** command in IP SLA operation mode.

For example, use the **type udp jitter** command to enter UDP jitter configuration mode, and then use the **packet interval** command to specify that 30 milliseconds pass between transmission of packets:

```
RP/0/RP0/CPU0:router(config)# ipsla operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/RP0/CPU0:router(config-ipsla-udp-jitter)# packet interval 30
```

For example, use the **type udp jitter** command to enter IP SLA UDP jitter configuration mode for IP SLA operation 1, and then use the **control disable** command to disable control packets:

```
RP/0/RP0/CPU0:router(config)#ipsla operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/RP0/CPU0:router(config-ipsla-udp-jitter)# control disable
```

For example, use the **type udp jitter** command to enter IP SLA UDP jitter configuration mode for IP SLA operation 1, and then use the **frequency** command to specify a probe period of 60 seconds:

```
RP/0/RP0/CPU0:router(config)# ipsla operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type udp jitter
RP/0/RP0/CPU0:router(config-ipsla-udp-jitter)# frequency 60
```

IPv4 Access List Configuration Mode

Prompt: (config-ipv4-acl)

Enter IPv4 access list configuration mode from global configuration mode. In global configuration mode, you can create or modify an access list by specifying the name of the list as an argument to the **ipv4 access-list** command. The CLI automatically enters IPv4 access list configuration mode.

For example, specify a deny condition for an access list named Internetfilter:

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list Internetfilter
RP/0/RP0/CPU0:router(config-ipv4-acl)# 10 deny 192.168.34.0 0.0.0.255
RP/0/RP0/CPU0:router(config-ipv4-acl)# 20 deny 172.16.0.0 0.0.255.255
RP/0/RP0/CPU0:router(config-ipv4-acl)# 25 deny tcp host 172.16.0.0 eq bgp host
192.168.202.203 range 1300 1400
RP/0/RP0/CPU0:router(config-ipv4-acl)# permit 10.0.0.0 0.255.255.255
```

IPv4 Prefix List Configuration Mode

Prompt: (config-ipv4-pfx)

Enter IPv4 prefix list configuration mode by using the **ipv4 prefix-list** command in global configuration mode. For example, configure a list named list1 to accept a mask length of up to 24 bits in routes with the prefix 172.20.10.171/16:

```
RP/0/RP0/CPU0:router(config)# ipv4 prefix-list list1
RP/0/RP0/CPU0:router(config-ipv4-pfx)# permit 172.20.10.171/16 le 24
```

IPv4 VRF Address Family Command Mode

Prompts:

- (config-bgp-vrf-af)
- (config-eigrp-vrf-af)

Enter the command mode for an IPv4 VPN routing and forwarding (VRF) address family by using the **vrf** command in router configuration mode for the applicable routing protocol. This mode also supports configuration of static routes.

For example, after entering VRF configuration mode from router BGP configuration mode, specify IPv4 unicast configuration mode:

```
RP/0/RP0/CPU0:router(config-bgp)# vrf new1
RP/0/RP0/CPU0:router(config-bgp-vrf)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-bgp-vrf-af)#
```

For example, enter static router configuration mode and then specify a VRF named new1:

```
RP/0/RP0/CPU0:router(config)# router static
RP/0/RP0/CPU0:router(config-static)# vrf new1
RP/0/RP0/CPU0:router(config-static-vrf)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-static-vrf-afi)#
```

IPv6 Access List Configuration Mode

Prompt: (config-ipv6-acl)

Enter IPv6 access list configuration mode from global configuration mode. In global configuration mode, you can create or modify an access list by specifying the name of the list as an argument to the **ipv6 access-list** command. The CLI automatically enters IPv6 access list configuration mode.

For example, create an IPv6 access list named Internetfilter:

```
RP/0/RP0/CPU0:router(config)# ipv6 access-list Internetfilter
RP/0/RP0/CPU0:router(config-ipv6-acl)#
```

IPv6 Prefix List Configuration Mode

Prompt: (config-ipv6-pfx)

Enter IPv6 prefix list configuration mode by using the **ipv6 prefix-list** command in global configuration mode.

For example, use the **deny** command for a list named preflist1 to prevent OSPFv3 from installing routes that have 2001:e624 as the first 32 bits of the address:

```
RP/0/RP0/CPU0:router(config)# ipv6 prefix-list preflist1
RP/0/RP0/CPU0:router(config-ipv6-pfx)# deny 2001:e624::/32 le 128
```

For example, permit mask lengths of 8–24 bits in all of the address space:

```
RP/0/RP0/CPU0:router(config)# ipv6 prefix-list preflist1
RP/0/RP0/CPU0:router(config-ipv6_pfx)# permit 2000:1::1/64 ge 8 le 24
```

ISAKMP Group Configuration Mode

Prompt: (isakmp-group)

Enter the mode for configuring Internet Security Association and Key Management Protocol (ISAKMP) by using the **crypto isakmp client configuration group** command in global configuration mode. ISAKMP, Oakley, and Skeme are security protocols implemented by Internet Key Exchange (IKE).

IKE is a key management protocol standard that works with the IP Security (IPSec) standard. IPSec provides robust authentication and encryption of IP packets. IKE is a hybrid protocol that implements the Oakley key exchange and the Skeme key exchange inside the ISAKMP framework.

For example, configure split tunneling by using the **acl** command to specify which groups of access control lists (ACLs) represent the protected subnets for *split tunneling*. (Split tunneling is the ability to have a secure tunnel to the central site and simultaneously have clear text tunnels to the Internet.) In this case, split tunneling is applied to the group named cisco. Subsequently, all traffic sourced at the client and destined to the subnet 192.168.1.0 goes by way of the VPN tunnel:

```
RP/0/RP0/CPU0:router(config)# crypto isakmp client configuration group cisco
RP/0/RP0/CPU0:router(isakmp-group)# key cisco
RP/0/RP0/CPU0:router(isakmp-group)# acl group1
RP/0/RP0/CPU0:router(config)# ipv4 access-list group1 permit ip 192.168.1.0 0.0.0.255 any
```

ISAKMP Policy Configuration Mode

Prompt: (config-isakmp)

Enter ISAKMP policy configuration mode by using the **crypto isakmp policy** command in global configuration mode. In policy configuration mode, the available commands let you define a policy for Internet Key Exchange (IKE).

For example, create and configure policy number 15 with the characteristics shown:

```
RP/0/RP0/CPU0:router(config)# crypto isakmp policy 15
RP/0/RP0/CPU0:router(config-isakmp)# hash md5
RP/0/RP0/CPU0:router(config-isakmp)# authentication rsa-sig
RP/0/RP0/CPU0:router(config-isakmp)# group 2
RP/0/RP0/CPU0:router(config-isakmp)# lifetime 5000
RP/0/RP0/CPU0:router(config-isakmp)# description this is a sample IKE policy
RP/0/RP0/CPU0:router(config-isakmp)# exit
```

Key Chain Mode

Prompt: (config-*client*-keys)

Enter key chain mode by entering the **key chain** command in global configuration mode. In the prompt for this mode, the *client* is a protocol (such as IS-IS) or other type of client that uses a key.

For example, enter key chain mode for a client named isis-keys:

```
RP/0/RP0/CPU0:router(config)# key chain isis-keys
RP/0/RP0/CPU0:router(config-isis-keys)#
```

Keychain-Key Mode

Prompt: (config-*client*-keys-*key-id*)

Enter keychain-key mode by entering the **key** command in key chain configuration mode. In the prompt for this mode, the *client* is a protocol (such as IS-IS) or other type of client that is using the key identified by the *key-id* argument.

For example, create a key for IS-IS with a value for a *key-id* of 8:

```
RP/0/RP0/CPU0:router(config)# key chain isis-keys
RP/0/RP0/CPU0:router(config-isis-keys)# key 8
RP/0/RP0/CPU0:router(config-isis-keys-0x8)#
```

Line (Template) Configuration Mode

Prompt: (config-line)

Enter line (or line template) configuration mode by using a **line** command in global configuration mode. This mode applies in the environments for multicasting; IP addresses and services; and authentication, authorization, and accounting (AAA). For information on these areas, see *Cisco IOS XR Multicast Configuration Guide,* the *Cisco IOS XR IP Addresses and Services Configuration Guide*, or *Cisco IOS XR System Security Configuration Guide*.

For line template configuration, you can add a variety of characteristics to terminal services, such as setting up physical and virtual terminal connections, managing terminals, and configuring virtual terminal line (vty) pools.

For example, use the **width** command to set the width of the display terminal to 99 characters:

```
RP/0/RP0/CPU0:router(config)# line default
RP/0/RP0/CPU0:router(config-line)# width 99
```

For example, specify the default outgoing transport protocol to be the Secure Shell (SSH) protocol by using the **transport preferred** command:

```
RP/0/RP0/CPU0:router(config)# line default
RP/0/RP0/CPU0:router(config-line)# transport preferred ssh
```

LMP Datalink Adjacency Configuration Mode

Prompt: (config-mpls-ouni-if-adj)

Enter the configuration mode for LMP datalink adjacency from the interface mode of MPLS O-UNI.

For example, configure the transport network address (TNA) for an Optical User Network Interface (O-UNI) datalink. Configure the datalink for POS interface 0/1/0/1 to the TNA 194.169.4.7:

```
RP/0/RP0/CPU0:router(config)# mpls optical-uni
RP/0/RP0/CPU0:router(config-mpls-ouni)# interface pos 0/1/0/1
RP/0/RP0/CPU0:router(config-mpls-ouni-if)# lmp data-link adjacency
RP/0/RP0/CPU0:router(config-mpls-ouni-if-adj)# tna ipv4 194.169.4.7
```

LMP Neighbor Configuration Mode

Prompt: (config-ouni-nbr-*neighbor-name*)

Enter Link Management Protocol (LMP) neighbor configuration mode for Optical User Network Interface (O-UNI) by using the **lmp neighbor** command in MPLS O-UNI configuration mode. The LMP neighbor configuration prompt contains the name of the neighbor that you provide as an argument to the **lmp neighbor** command.

For example, configure a neighbor called router1 to have a node ID of 192.166.21.14:

```
RP/0/RP0/CPU0:router(config)# mpls optical-uni
RP/0/RP0/CPU0:router(config-mpls-ouni)# lmp neighbor router1
RP/0/RP0/CPU0:router(config-ouni-nbr-router1)# remote node-id 192.166.21.14
```

MPLS LDP Configuration Mode

Prompt: (config-ldp)

Enter MPLS Label Distribution Protocol (LDP) configuration mode from global configuration mode.

In an MPLS network, LDP provides a standard methodology for hop-by-hop (or dynamic label) distribution by assigning labels to routes that have been chosen by the underlying Interior Gateway Protocol (IGP) routing protocols. The resulting labeled paths, called label switch paths (LSPs), forward the labeled traffic across an MPLS backbone.

In MPLS LDP configuration mode, you can:

- Enter other modes (such as label mode or log configuration mode)
- Configure certain LDP features or parameters, such as MPLS graceful-restart, back-off of successive setup attempts, and logging of various services

For example, enter MPLS LDP configuration mode and then enable graceful restart. (To allow non-stop forwarding during an LDP communication failure and then trigger a restart, enable graceful restart.)

```
RP/0/RP0/CPU0:router(config)# mpls ldp
RP/0/RP0/CPU0:router(config-ldp)# graceful-restart
```

For example, specify an initial backoff of 30 seconds and a maximum backoff of 240 seconds. (Backoff prevents two incompatibly configured routers from engaging in unthrottled setup failures by delaying successive attempts with exponentially increasing delays.)

```
RP/0/RP0/CPU0:router(config)# mpls ldp
RP/0/RP0/CPU0:router(config-ldp)# backoff 30 240
```

MPLS LDP Interface Configuration Mode

Prompt: (config-ldp-if)

Enter MPLS LDP interface configuration mode from global configuration or MPLS LDP configuration mode to enable LDP on an interface or to configure interface-related LDP parameters.

For example, use **discovery transport-address** to specify IP address 10.10.3.1 as the transport address on POS interface 0/1/0/0:

```
RP/0/RP0/CPU0:router(config)# mpls ldp interface POS 0/1/0/0
RP/0/RP0/CPU0:router(config-ldp-if)# discovery transport-address 10.10.3.1
```

MPLS LDP Label Accept Configuration Mode

Prompt: (config-ldp-lbl-acpt)

Enter label accept configuration mode by using the **label accept** command in MPLS LDP configuration mode. In the label accept mode, you can control the receipt of labels (remote bindings) for a set of prefixes from a peer.

For example, first enter MPLS LDP configuration mode by using the **mpls ldp** command in global configuration mode. Next, enter the label accept mode by using the **label accept** command.

```
RP/0/RP0/CPU0:router(config)# mpls ldp
RP/0/RP0/CPU0:router(config-ldp)# label accept
RP/0/9/CPU0:LDP1(config-ldp-lbl-acpt)#
```

For example, configure an inbound label filtering policy. In this example, an LSR is configured to accept and retain the following label bindings and prefixes:

- Prefix 192.168.1.1 (pfx_acl_1) from peer 1.1.1.1
- Prefix 192.168.2.2 (pfx_acl_2) from peer 2.2.2.2
- Prefixes 192.168.1.1, 192.168.2.2, 192.168.3.3 (pfx_acl_3) from peer 3.3.3.3

```
RP/0/RP0/CPU0:router(config-ldp-lbl-acpt)# for pfx_acl_1 from 1.1.1.1
RP/0/RP0/CPU0:router(config-ldp-lbl-acpt)# for pfx_acl_2 from 2.2.2.2
RP/0/RP0/CPU0:router(config-ldp-lbl-acpt)# for pfx_acl_3 from 3.3.3.3
```

MPLS LDP Label Advertise Configuration Mode

Prompt: (config-ldp-lbl-advt)

Enter label advertise configuration mode by using the **label advertise** command in MPLS LDP configuration mode. In the label advertise mode, you can control the advertisement of local labels.

For the first example, disable the advertisement of all locally assigned labels to all peers:

```
RP/0/RP0/CPU0:router(config-ldp)# label advertise
RP/0/RP0/CPU0:router(config-ldp-lbl-advt)# disable
```

For example, send labels only for prefixes 10.1.1.0 and 20.1.1.0 (pfx_acl1) to all peers:

```
RP/0/RP0/CPU0:router(config-ldp)# label advertise
RP/0/RP0/CPU0:router(config-ldp-lbl-advt)# disable
RP/0/RP0/CPU0:router(config-ldp-lbl-advt)# for pfx_acl_1
```

MPLS LDP Label Configuration Mode

Prompt: (config-ldp-lbl)

Enter Label Distribution Protocol (LDP) label configuration mode from MPLS LDP configuration mode. In this mode, you can enter a submode to perform the configuration tasks of either controlling the advertisement of local labels (outbound label filtering) or controlling the receipt of labels (remote bindings) for a set of prefixes from a given peer (inbound label filtering). These available submodes are called label advertise mode and label accept mode. Moreover, LDP local label allocation configuration can also be entered directly under this mode.

For example, enter MPLS LDP label configuration submode and then configure local label allocation policy, or enter advertise or accept configuration submodes:

```
RP/0/RP0/CPU0:router(config)# mpls ldp label
RP/0/RP0/CPU0:router(config-ldp-lbl)#

RP/0/RP0/CPU0:router(config-ldp-lbl)# label allocate for pfx_acl

RP/0/RP0/CPU0:router(config-ldp-lbl)# accept
RP/0/RP0/CPU0:router(config-ldp-lbl-acpt)#

RP/0/RP0/CPU0:router(config-ldp-lbl)# advertise
RP/0/RP0/CPU0:router(config-ldp-lbl-advt)#
```

MPLS LDP Log Configuration Mode

Prompt: (config-ldp-log)

Enter MPLS LDP log configuration mode by using the **mpls ldp log** command in global configuration mode. In this mode, you can enable logging for several features. These logs can be enabled to accumulate information related to a neighbor, graceful-restart, or session-protection.

For example, enter LDP log configuration mode:

```
RP/0/9/CPU0:LDP1(config)# mpls ldp log
RP/0/9/CPU0:LDP1(config-ldp-log)#
```

MPLS OAM Configuration Mode

Prompt: (config-oam)

Enter the configuration mode for MPLS Operations, Administration, and Maintenance (OAM) by using the **mpls oam** command in EXEC mode. In MPLS OAM mode, for example, you can configure OAM tasks for learning the routes that packets follow when travelling to their destinations, setting the echo packet revision, and enabling label switched path (LSP) verification commands.

For example, enable MPLS OAM:

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

After entering MPLS OAM mode, disable the transmission of vendor extension type length and value (TLV) in the echo request, use the **echo disable-vendor extension** command in MPLS OAM configuration submode. For example, disable inclusion of the vendor extensions TLV in echo requests:

```
RP/0/RP0/CPU0:router(config-oam)# echo disable-vendor-extension
RP/0/RP0/CPU0:router(config-oam)#
```

MPLS O-UNI Configuration Mode

Prompt: (config-mpls-ouni)

Enter MPLS optical UNI (O-UNI) configuration mode by using the **mpls optical-uni** command in global configuration mode. The MPLS O-UNI mode is an intermediate mode to other modes, in which you can configure MPLS O-UNI. From MPLS O-UNI mode, you can go to either the interface submode or the neighbor submode of the MPLS O-UNI mode.

To configure or update a new or existing O-UNI-specific Link Management Protocol (LMP) neighbor and its associated parameters, use the **lmp neighbor** command in MPLS O-UNI configuration mode.

For example, create a neighbor called router1. The CLI enters LMP neighbor configuration mode from O-UNI configuration mode. In this neighbor submode, configure a node ID of 192.68.22.12.

```
RP2/0/RP0/CPU0:router(config)# mpls optical-uni
RP2/0/RP0/CPU0:router(config-mpls-ouni)# mpls optical-uni lmp neighbor router1
RP2/0/RP0/CPU0:router(config-ouni-nbr-router1)# remote node-id 192.68.22.12
```

MPLS O-UNI Interface Configuration Mode

Prompt: (config-mpls-ouni-if)

Enter the interface submode for MPLS optical UNI (O-UNI) by using the **interface** command in MPLS optical UNI mode.

For example, configure the POS interface 0/1/0/0 to be a passive end of an O-UNI:

```
RP/0/RP0/CPU0:router(config)# mpls optical-uni
RP/0/RP0/CPU0:router(config-mpls-ouni)# interface POS 0/1/0/1
RP/0/RP0/CPU0:router(config-mpls-ouni-if)# passive
```

MPLS TE Configuration Mode

Prompt: (config-mpls-te)

Enter MPLS traffic engineering (TE) configuration mode from global configuration mode. In most cases, this mode is a step to the interface submode of MPLS TE configuration. (See "MPLS TE Interface Configuration Mode.")

For example, remove interface 0/7/0/0 from the MPLS TE domain:

```
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# no interface pos 0/7/0/1
```

MPLS TE Interface Configuration Mode

Prompt: (config-mpls-te-if)

Enter MPLS TE interface configuration mode from MPLS TE configuration mode.

For this example, override the Interior Gateway Protocol (IGP) administrative weight (or cost) of interface 0/7/0/0 by using the **admin-weight** command to set the cost at 20:

```
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# interface pos 0/7/0/0
RP/0/RP0/CPU0:router(config-mpls-te-if)# admin-weight 20
```

Multicast Routing Configuration Mode

Prompt: (config-mcast-ipv4)

Enter multicast routing configuration mode from either EXEC mode or global configuration mode. (In the current release, the default address family is IPv4.) You can also configure multicasting details for a specific interface by entering the applicable commands in routing configuration mode.

For detailed information about multicast routing concepts, configuration tasks, and examples, refer to *Implementing Multicast Routing on Cisco IOS XR Software* configuration module.

For example, configure SSM service for the IP address range defined by access list 4:

```
RP/0/RP0/CPU0:router# ipv4 access-list 4 permit 224.2.151.141
RP/0/RP0/CPU0:router(config)# multicast-routing
RP/0/RP0/CPU0:router(config-mcast-ipv4)# ssm range 4
```

For example, enable multicast routing on all interfaces, and then disable the feature on Packet-over-SONET/SDH (POS) interface 0/1/0/0:

```
RP/0/RP0/CPU0:router# multicast-routing
RP/0/RP0/CPU0:router(config-mcast-ipv4)# interface all enable
RP/0/RP0/CPU0:router(config-mcast-ipv4)# interface pos 0/1/0/0
RP/0/RP0/CPU0:router(config-mcast-ipv4-if)# disable
```

Neighbor Address Family Configuration Mode

Prompt: (config-bgp-nbr-af)

In neighbor address family mode, you can specify address characteristics for a neighbor. To do so, enter neighbor configuration mode and then neighbor address family configuration mode.

For example, activate IPv4 multicast for neighbor 10.0.0.1, and then place the router in neighbor address family configuration mode for the IPv4 multicast address family:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router bgp 1
RP/0/RP0/CPU0:router(config-bgp)# neighbor 10.0.0.1
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 1
RP/0/RP0/CPU0:router(config-bgp-nbr)# address-family ipv4 multicast
RP/0/RP0/CPU0:router(config-bgp-nbr-af)#
```

Neighbor Configuration Mode

Prompts: (config-bgp-nbr)

Enter neighbor configuration mode from router BGP configuration mode. To configure BGP elements that apply to neighbors, you must enter neighbor configuration mode from router configuration mode with the assigned protocol of BGP.

For example, enter neighbor configuration mode for neighbor 10.0.0.1:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router bgp 1
RP/0/RP0/CPU0:router(config-bgp)# neighbor 10.0.0.1
RP/0/RP0/CPU0:router(config-bgp-nbr)#
```

Neighbor Group Address Family Configuration Mode

Prompt: (config-bgp-nbrgrp-af)

Enter neighbor group address family configuration mode from neighbor group configuration mode. With BGP, you can enter address family commands for one or more neighbors that are addressed as a group.

For example, create a neighbor group named rrclients. The CLI goes into neighbor group configuration mode. In neighbor group configuration mode, create a neighbor with an autonomous system number of 65534. The CLI enters address family configuration mode for this neighbor group.

```
RP/0/RP0/CPU0:router(config-bgp)# neighbor-group rrclients
RP/0/RP0/CPU0:router(config-bgp-nbrgrp)# remote-as 65534
RP/0/RP0/CPU0:router(config-bgp-nbrgrp)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-bgp-nbrgrp-af)#
```

Neighbor Group Configuration Mode

Prompt: (config-bgp-nbrgrp)

Enter neighbor group configuration mode from router configuration mode. For BGP, you can use neighbor group-related commands to apply a configuration to one or more neighbors.

For example, create the neighbor group rrclients. The CLI enters neighbor group configuration mode.

```
RP/0/RP0/CPU0:router(config-bgp)# neighbor-group rrclients
RP/0/RP0/CPU0:router(config-bgp-nbrgrp)#
```

NTP Configuration Mode

Prompt: (config-ntp)

Enter Network Time Protocol (NTP) configuration mode from global configuration mode. In NTP configuration mode, you can configure the NTP services for a router.

For example, configure the system to allow itself to be synchronized by a peer from an access list named access1 and to restrict access to allow time requests only from an access list named access2:

```
RP/0/RP0/CPU0:router(config)# ntp
RP/0/RP0/CPU0:router(config-ntp)# access-group peer access1
RP/0/RP0/CPU0:router(config-ntp)# access-group serve-only access2
```

For example, configure the router to use the IP address of Packet-over-SONET/SDH (POS) interface 0/0/0/1 as the source address of all outgoing NTP packets:

```
RP/0/RP0/CPU0:router(config)# ntp
RP/0/RP0/CPU0:router(config-ntp)# source POS 0/0/0/1
```

NTP Interface Configuration Mode

Prompt: (config-ntp-int)

Enter Network Time Protocol (NTP) interface configuration mode from global configuration mode. In NTP interface configuration mode, you can configure interface-specific details for NTP.

For example, configure Packet-over-SONET/SDH (POS) interface 0/0/0/1 to send NTP packets:

```
RP/0/RP0/CPU0:router(config)# ntp interface POS 0/0/0/1
RP/0/RP0/CPU0:router(config-ntp-int)# broadcast client
```

O-UNI LMP Datalink Adjacency Configuration Mode

Prompt: (config-mpls-ouni-if-adj)

Enter the optical UNI Link Management Protocol (LMP) datalink adjacency configuration mode from MPLS O-UNI interface configuration mode. For example, use the **neighbor** command to associate a neighbor named router1 with the datalink specified as POS interface 0/1/0/1:

```
RP/0/RP0/CPU0:router(config)# mpls optical-uni
RP/0/RP0/CPU0:router(config-mpls-ouni)# interface POS0/1/0/1
RP/0/RP0/CPU0:router(config-mpls-ouni-if)# lmp data-link adjacency
RP/0/RP0/CPU0:router(config-mpls-ouni-if-adj)# neighbor router1
```

O-UNI LMP Neighbor Adjacency Configuration Mode

Prompt: (config-mpls-ouni-if-adj)

Enter adjacency configuration mode for MPLS O-UNI neighbor interfaces by using the **lmp data-link adjacency** command in the interface submode of MPLS O-UNI configuration mode. For example, configure a remote interface ID of 2 for POS interface 0/2/0/0:

```
RP/0/RP0/CPU0:router(config)# mpls optical-uni
RP/0/RP0/CPU0:router(config-mpls-ouni)# interface pos 0/2/0/0
RP/0/RP0/CPU0:router(config-mpls-ouni-if)# lmp data-link adjacency
RP/0/RP0/CPU0:router(config-mpls-ouni-if-adj)# remote interface-id 2
```

O-UNI LMP Neighbor Configuration Mode

Prompt: (config-ouni-nbr-*neighbor*)

Enter O-UNI link management protocol (LMP) neighbor configuration mode by identifying a neighbor in MPLS O-UNI configuration mode. The name of the neighbor subsequently appears in the O-UNI LMP neighbor prompt. (Enter MPLS O-UNI configuration mode from global configuration mode.)

For example, configure a routed IPCC for a neighbor called router1, whose destination IP address is the node ID of the neighbor router1 on an interface determined dynamically by an IP routing protocol:

```
RP/0/RP0/CPU0:router(config)# mpls optical-uni
RP/0/RP0/CPU0:router(config-mpls-ouni)# lmp neighbor router1
RP/0/RP0/CPU0:router(config-ouni-nbr-router1)# ipcc routed
```

Peer Configuration Mode

Prompt: (config-msdp-peer)

Enter peer configuration mode Multicast Source Discovery Protocol (MSDP) by using the **peer** command in router MDSP configuration mode.

For example, configure the router named router.cisco.com to be the default peer to the local router:

```
RP/0/RP0/CPU0:router(config)# router msdp
RP/0/RP0/CPU0:router(config-msdp)# peer 172.16.2.3
RP/0/RP0/CPU0:router(config-msdp-peer)# default-peer router.cisco.com
```

Placement Program Mode

Prompt: (config-place)

Enter placement program mode for a route processor (RP) by using the **placement program** command in global configuration mode. This command lets you assign a process to an RP or DRP. In placement program mode, you can assign process affinities (preferences) by using the **affinity** command. To remove the assigned process placement, use the **no** form of this command.

For example, enter the placement program mode for the program called pim, and then configure affinity attributes for that program.

```
RP/0/RP0/CPU0:router(config)# placement program pim default
RP/0/RP0/CPU0:router(config-place)# affinity location-set current attract 100
```

Policy Map Class Configuration Mode

Prompt: (config-pmap-c)

Enter policy map class configuration mode by first entering policy map configuration mode from global configuration. In policy map mode, you can create or modify a class by using the **class** command, after which the CLI automatically goes into policy map class mode. These modes are part of the Quality of Service (QoS) feature. For more details on the policies and classes within the QoS feature, see *Quality of Service Commands on Cisco IOS XR Software* or *Cisco IOS XR Modular Quality of Service Configuration Guide*.

For example, first guarantee that 50 percent of the interface bandwidth goes to a class named class1, and then guarantee that 10 percent of the interface bandwidth to a class named class2:

```
RP/0/RP1/CPU0:router(config)# policy-map policy1
RP/0/RP1/CPU0:router(config-pmap)# class class1
RP/0/RP1/CPU0:router(config-pmap-c)# bandwidth percent 50
RP/0/RP1/CPU0:router(config-pmap-c)# exit
RP/0/RP1/CPU0:router(config-pmap)# class class2
RP/0/RP1/CPU0:router(config-pmap-c)# bandwidth percent 10
```

Policy Map Configuration Mode

Prompt: (config-pmap)

Enter policy map configuration mode from global configuration mode by using the **policy-map** command to create a policy map or modify an existing policy map. In policy map mode, you can create or modify a class by using the **class** command, after which the CLI automatically goes into policy map class mode. These modes are part of the Quality of Service (QoS) feature.

To attach a QoS policy to a specific POS interface, you must enter interface configuration mode from global configuration mode by identifying the interface and then using the **service-policy** command to attach an existing policy. For more details on the policies and classes within the QoS feature, see the *Quality of Service Commands on Cisco IOS XR Software* or the *Cisco IOS XR Modular Quality of Service Configuration Guide*.

For example, use the **policy-map** command to create a policy named policy1:

```
RP/0/RP1/CPU0:router(config)# policy-map policy1
RP/0/RP1/CPU0:router(config-pmap)#
```

POS Interface Configuration Mode

Prompt: (config-if-pos)

Enter the submode for Packet-over-SONET/SDH (POS) interface configuration by using the **pos** command in interface configuration mode.

For example, enter the POS interface configuration mode for 0/1/0/2:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/1/0/2
RP/0/RP0/CPU0:router(config-if)# pos
RP/0/RP0/CPU0:router(config-if-pos)# crc 32
```

Process Configuration Mode

The applicable process actions actually occur in administration EXEC mode. The object of these process actions are instances of OSPF or OSPFv3 processes. In admin EXEC mode, a variety of process control commands are available. See *Cisco IOS XR System Management Command Reference* or *Cisco IOS XR System Management Configuration Guide* for details on the **process** command options.

Profile Configuration Mode

Prompt: (config-*profilename*)

Enter profile configuration mode from global configuration mode by using the **crypto ipsec profile** command. In this mode, you can configure the IP Security (IPSec) profile, and the prompt shows the profile name you provide to the **crypto ipsec profile** command.

To apply extended authentication (Xauth) for Internet Key Exchange (IKE) interaction, use the **client authentication list** command in profile configuration mode.

For example, specify that AAA username and password storage location information is applied from the authentication list named list0 to a profile named sampleX:

```
RP/0/RP0/CPU0:router(config)# crypto ipsec profile sampleX
RP/0/RP0/CPU0:router(config-sampleX)# client authentication list list0
```

Public Key Chain Configuration Mode

Prompt: (config-pubkey-chain)

Enter public key chain configuration mode by using the **crypto key pubkey-chain rsa** command in global configuration mode. In public key chain configuration mode, you can specify the Rivest, Shamir, and Adelman (RSA) public keys for other IP Security (IPSec) peers that you subsequently configure manually. Specify the RSA public key by using either the **addressed-key** or the **named-key** command.

For example, first enter public key chain configuration mode by using the **crypto key pubkey-chain rsa** command in global config mode. Thereafter, use the **addressed-key** command, and then start specifying the key strings through the **key-string** command.

```
RP/0/RP0/CPU0:router(config)# crypto key pubkey-chain rsa
RP/0/RP0/CPU0:router(config-pubkey-chain)# addressed-key 10.5.5.1
RP/0/RP0/CPU0:router(config-pubkey-key)# address 10.5.5.1
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string 005C300D 06092A86 4886F70D 01010105
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string 00034B00 30480241 00C5E23B 55D6AB22
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string 04AEF1BA A54028A6 9ACC01C5 129D99E4
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string 64CAB820 847EDAD9 DF0B4E4C 73A05DD2
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string BD62A8A9 FA603DD2 E2A8A6F8 98F76E28
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string D58AD221 B583D7A4 71020301 0001
```

For example, enter public key chain configuration mode and then use the **named-key** command:

```
RP/0/RP0/CPU0:router(config)# crypto key pubkey-chain rsa
RP/0/RP0/CPU0:router(config-pubkey-chain)# named-key otherpeer.example.com

  address 10.5.5.1
  key-string  005C300D 06092A86 4886F70D 01010105
  key-string  005C300D 06092A86 4886F70D 01010105
  key-string  00034B00 30480241 00C5E23B 55D6AB22
  key-string  04AEF1BA A54028A6 9ACC01C5 129D99E4
  key-string 64CAB820 847EDAD9 DF0B4E4C 73A05DD2
  key-string BD62A8A9 FA603DD2 E2A8A6F8 98F76E28
  key-string D58AD221 B583D7A4 71020301 0001
  exit
  addressed-key 10.1.1.2 encryption
  key-string  00302017 4A7D385B 1234EF29 335FC973
  key-string  00302017 4A7D385B 1234EF29 335FC973
  key-string  2DD50A37 C4F4B0FD 9DADE748 429618D5
  key-string  18242BA3 2EDFBDD3 4296142A DDF7D3D8
  key-string  08407685 2F2190A0 0B43F1BD 9A8A26DB
  key-string  07953829 791FCDE9 A98420F0 6A82045B
```

```
key-string  90288A26 DBC64468 7789F76E EE21
exit
addressed-key 10.1.1.2 signature
key-string 0738BC7A 2BC3E9F0 679B00FE 098533AB
key-string  0738BC7A 2BC3E9F0 679B00FE 098533AB
key-string  01030201 42DD06AF E228D24C 458AD228
key-string  58BB5DDD F4836401 2A2D7163 219F882E
key-string  64CE69D4 B583748A 241BED0F 6E7F2F16
key-string  0DE0986E DF02031F 4B0B0912 F68200C4
key-string  C625C389 0BFF3321 A2598935 C1B1
exit
```

Public Key Configuration Mode

Prompt: (config-pubkey-key)

Enter public key configuration mode by using the **addressed-key** or **addressed-key-key** command in public key chain configuration mode.

For example, enter public key chain configuration mode. Use **addressed-key** to enter public key configuration mode for IP address 10.5.5.1. Specify address key strings for the remote peer at 10.5.5.1:

```
RP/0/RP0/CPU0:router(config)# crypto key pubkey-chain rsa
RP/0/RP0/CPU0:router(config-pubkey-chain)# addressed-key 10.5.5.1
RP/0/RP0/CPU0:router(config-pubkey-key)# address 10.5.5.1
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string 005C300D 06092A86 4886F70D 01010105
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string 00034B00 30480241 00C5E23B 55D6AB22
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string 04AEF1BA A54028A6 9ACC01C5 129D99E4
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string 64CAB820 847EDAD9 DF0B4E4C 73A05DD2
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string BD62A8A9 FA603DD2 E2A8A6F8 98F76E28
RP/0/RP0/CPU0:router(config-pubkey-key)# key-string D58AD221 B583D7A4 71020301 0001
```

QoS FAX Configuration Mode

Prompt: (config-sbc-sbe-qos-fax)

Enter QoS FAX configuration mode by using the **qos fax residential** command in mode.

For example, configure the QoS FAX profile to mark packets with a DSCP value.

```
RP/0/RP0/CPU0:router(config)# sbc MySbc sbe
RP/0/RP0/CPU0:router(config-sbc-sbe)# qos fax residential
RP/0/RP0/CPU0:router(config-sbc-sbe-qos-fax)# marking dscp
```

QoS Video Configuration Mode

Prompt: (config-sbc-sbe-qos-video)

Enter QoS video configuration mode by using the **qos video residential** command in mode.

For example, configure the QoS video profile to mark packets with a DSCP value.

```
RP/0/RP0/CPU0:router(config)# sbc MySbc sbe
RP/0/RP0/CPU0:router(config-sbc-sbe)# qos video residential
RP/0/RP0/CPU0:router(config-sbc-sbe-qos-video)# marking dscp
```

QoS Voice Configuration Mode

Prompt: (config-sbc-sbe-qos-voice)

Enter QoS video configuration mode by using the **qos voice residential** command in mode.

For example, configure the QoS voice profile to mark packets with a DSCP value.

```
RP/0/RP0/CPU0:router(config)# sbc MySbc sbe
RP/0/RP0/CPU0:router(config-sbc-sbe)# qos voice residential
RP/0/RP0/CPU0:router(config-sbc-sbe-qos-voice)# marking dscp
```

RADIUS Server Group Configuration Mode

Prompt: (config-sg-radius)

Enter RADIUS server group configuration mode from global configuration mode by using the **aaa group server radius** command. This command lets you group different server hosts into distinct lists.

For example, enter RADIUS server group configuration mode, and then specify the IP address of an external RADIUS server to be 192.168.60.15:

```
RP/0/RP0/CPU0:router(config)# aaa group server tacacs+
RP/0/RP0/CPU0:router(config-sg-tacacs+)# server 192.168.60.15
```

Route Distinguisher Configuration Mode

Prompt: (config-rd)

To create a route distinguisher (RD) and enter RD configuration mode, use the **rd-set** command in global configuration mode. An RD set is a 64-bit value prepended to an IPv4 address to create a globally unique Border Gateway Protocol (BGP) VPN-IPv4 address. The values for an RD can have a variety of formats. The example here shows ASN format with a wildcard character. This format can appear as, for example, 10002:255.255.0.0. For a list of all the formats, see the **rd-set** description in the command reference.

For example, create an RD called vpn-1 in ASN format. The **end-set** and **end-policy** commands are used to end the RD definition and the route policy configuration and then return to global configuration mode:

```
RP/0/RP0/CPU0:router(config)# rd-set vpn-1
RP/0/RP0/CPU0:router(config-rd)# 10.0.0.2:777
RP/0/RP0/CPU0:router(config-rd)# end-set
RP/0/RP0/CPU0:router(config-rd)# end-policy
```

Route-policy Configuration Mode

Prompt: (config-rpl)

Enter route-policy configuration mode by using the **route-policy** command in global configuration mode. In route-policy configuration mode, you can create or modify a route policy by entering successive commands and then terminating the configuration by entering the **end-policy** command.

For example, create a simple policy named drop-all. It directs the router to drop any route it encounters:

```
RP/0/RP0/CPU0:router(config)# route-policy drop-all
RP/0/RP0/CPU0:router(config-rpl)# drop
RP/0/RP0/CPU0:router(config-rpl)# end-policy
```

Router Address Family Configuration Mode

Prompt: (config-isis-af)

Enter IS-IS router address family configuration mode from router configuration mode. This mode is the highest address family configuration mode for IS-IS and is the entry point for other IS-IS address modes.

For example, first enter IS-IS router configuration mode, and then enter router address family configuration mode for IS-IS for address family IPv4 unicast:

```
RP/0/RP0/CPU0:router(config)# router isis isp
RP/0/RP0/CPU0:router(config-isis)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-isis-af)#
```

Router Configuration Mode

Prompts:

- For BGP: (config-bgp)
- For IS-IS: (config-isis)
- For OSPF: (config-ospfv)
- For OSPFv3: (config-ospfv3)
- For EIGRP: (config-eigrp)
- For RIP: (config-rip)
- For static route specification: (config-static)

Enter router configuration mode by using the **router** command with a routing protocol name in global configuration mode. The **router** command also lets you enter static route configuration mode.

Router configuration mode lets you select and configure a routing protocol, such as BGP, OSPF, or IS-IS. For example, the following generic command syntax shows how to enter router configuration mode:

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

For example, place the router configuration mode for BGP:

```
RP/0/RP0/CPU0:router# configuration
RP/0/RP0/CPU0:router(config)# router bgp 140
RP/0/RP0/CPU0:router(config-bgp)#
```

For example, enter the router configuration mode for static routes.

```
RP/0/0/CPU0:ios(config)# router static
RP/0/0/CPU0:ios(config-static)#
```

Router HSRP Configuration Mode

Prompt: (config-hsrp)

Enter router configuration mode for Hot Standby Router Protocol (HSRP) by using the **router vrrp** command in global configuration mode. This mode is used for entering HSRP interface configuration mode. See HSRP Interface Configuration Mode. For details on the application of this mode, see the *Cisco IOS XR IP Addresses and Services Configuration Guide*.

For example, enter HSRP router configuration mode by entering the command sequence **router hsrp**:

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

Router IGMP Configuration Mode

Prompt: (config-igmp)

To configure Internet Group Management Protocol (IGMP) for multicasting, use the router IGMP configuration mode or, for a specific interface, the interface IGMP configuration mode.

For detailed information about multicast routing concepts, configuration tasks, and examples, refer to *Cisco IOS XR Multicast Configuration Guide*.

For example, enter interface configuration mode for IGMP, and then configure explicit tracking for IGMPv3 on the Packet-over-SONET/SDH (POS) interface 0/1/0/1:

```
RP/0/RP0/CPU0:router(config)# router igmp
RP/0/RP0/CPU0:router(config-igmp)# interface pos 0/1/0/1
RP/0/RP0/CPU0:router(config-igmp-if)# explicit-tracking enable 1
```

Router MLD Configuration Mode

Prompt: (config-mld)

Enter the Multicast Listener Discovery (MLD) configuration mode by entering the **router mld** command in global configuration mode. MLD supports IPv6. (IGMP supports IPv4.) In MLD mode, you can limit the number of multicast access-group join requests for a POS interface.

For example, enter MLD configuration mode for interface 0/1/0/0:

```
RP/0/RP0/CPU0:router(config)# router mld
RP/0/RP0/CPU0:router(config-mld)# interface pos 0/1/0/1
RP/0/RP0/CPU0:router(config-mld-if)# access-group anygroup
```

Router MSDP Configuration Mode

Prompt: (config-msdp)

Enter the configuration mode for Multicast Source Discovery Protocol (MSDP) by entering the **router mdsp** command in global configuration mode.

For example, set the Cache SA State hold-time period to 200 seconds:

```
RP/0/RP0/CPU0:router(config)# router msdp
RP/0/RP0/CPU0:router(config-msdp)# cache-sa-holdtime 200
```

Router PIM Configuration Mode

Prompt: (config-pim-ipv4)

Enter router configuration mode for Protocol Independent Multicast (PIM) by using the **router pim** command in global configuration mode. You can also configure PIM for a specific interface by entering the **interface** command in router PIM configuration mode.

For detailed information about multicast routing concepts, configuration tasks, and examples, refer to *Cisco IOS XR Multicast Configuration Guide*.

For example, restrict the rendezvous point so that sources in the Source Specific Multicast range of addresses are not allowed to register with the RP. Configure these statements on the RP only.

```
RP/0/RP0/CPU0:router(config)# router pim
RP/0/RP0/CPU0:router(config-pim-ipv4)# accept-register no-ssm-range
```

Router VRRP Configuration Mode

Prompt: (config-vrrp)

Enter router configuration mode for Virtual Router Redundancy Protocol (VRRP) by using the **router vrrp** command in global configuration mode. This mode is used for entering VRRP interface configuration mode. See "VRRP Interface Configuration Mode."

For example, enter VRRP router configuration mode by entering the command sequence **router vrrp**:

```
RP/0/RP0/1:router(config)# router vrrp
RP/0/RP0/1:router(config-vrrp)#
```

RSVP Configuration Mode

Prompt: (config-rsvp)

Enter Resource Reservation Protocol (RSVP) configuration mode from global configuration mode by using the **rsvp** command. The mode is used to enter the interface submode for RSVP. For example, enter RSVP configuration mode:

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

RSVP Interface Configuration Mode

Prompt: (config-rsvp-if)

Enter Resource Reservation Protocol (RSVP) interface configuration mode either:

- From global configuration mode
- By using the **rsvp interface** command
- From RSVP configuration mode by using the **interface** command.

For example, limit the total bandwidth of all RSVP reservations on POS interface 0/3/0/0 to 7500 kbps, and let each single flow reserve a maximum of 1000 kbps:

```
RP/0/RP0/CPU0:router(config)# rsvp interface pos 0/3/0/0
RP/0/RP0/CPU0:router(config-rsvp-if)# bandwidth 7500 1000
```

Session Border Controller Configuration Mode

Prompt: (config-sbc)

Enter the configuration mode for a session border controller (SBC) service by using the **sbc** command in global configuration mode. If the specified SBC service does not exist, the first-time use of the **sbc** command with the new name creates the instance of that SBC service.

For example, create the SBC instance named mySBC:

```
RP/0/RP0/CPU0:router(config)# sbc mySBC
RP/0/RP0/CPU0:router (config-sbc)#
```

SBC DBE Configuration Mode

Prompt: (config-sbc-dbe)

Enter the configuration mode for a particular instance of a data border element (DBE) by using the **dbe** command in SBC configuration mode. The DBE mode and applicable commands pertain to the media gateway tasks of SBC.

If the specified DBE does not exist, the first-time use of the **dbe** command with the new name creates the new DBE. If you plan to create both a DBE and an SBE on a card, you must create the DBE first.

For example, enter the DBE configuration mode for an SBC service instance named mySBC:

```
RP/0/RP0/CPU0:router(config)# sbc mySBC
RP/0/RP0/CPU0:router(config-sbc)# dbe
RP/0/RP0/CPU0:router (config-sbc-dbe)#
```

SBC DBE Media Address Configuration Mode

Prompt: (config-sbc-dbe-media-address)

Enter the mode to configure a data border element (DBE) media address pool and create an address pool for use with VPN routing and forwarding (VRF) by using the **media-address vrf** command in DBE configuration mode.

For example, configure an address pool for use in a VRF instance named vpn3. In this case, the DBE configuration mode for the SBC service instance called mySBC is entered from global configuration mode.

```
RP/0/RP0/CPU0:router(config)# sbc mySBC dbe
RP/0/RP0/CPU0:router(config-sbc-dbe)# media-address vrf vpn3
RP/0/RP0/CPU0:router(config-sbc-dbe-media-address)#
```

SBC Virtual DBE Configuration Mode

Prompt: (config-sbc-dbe-vdbe)

Enter the mode for specifying virtual data border element (vDBE) parameters by using the **vdbe** command in the DBE configuration mode for a specific SBC service instance.

Note The current release supports only one (global) vDBE, so you cannot partition DBE resources and do not need to specify a vDBE name. The example reflects this global vDBE and absence of a vDBE name.

For example, enter vDBE configuration mode for an SBC service instance named mySBC:

```
RP/0/RP0/CPU0:router(config)# sbc mySBC dbe
RP/0/RP0/CPU0:router(config-sbc-dbe)# vdbe
RP/0/RP0/CPU0:router(config-sbc-dbe-vdbe)#
```

SBC Virtual DBE H248 Configuration Mode

Prompt: (config-sbc-dbe-vdbe-h248)

Enter the mode for specifying an H248 controller by using the **controller h248** command in virtual data border element (vDBE) configuration mode.

Note The current release supports only one (global) vDBE, so you cannot partition DBE resources and do not need to specify a vDBE name. The example reflects the global vDBE and absence of a vDBE name.

For example, configure two DBE H248 controllers within the SBC instance named mySBC. Identify the first controller by the unique index number 1. Identify the second controller by the number 2:

```
RP/0/RP0/CPU0:router(config)# sbc mySBC dbe vdbe
RP/0/RP0/CPU0:router(config-sbc-dbe-vdbe)# controller h248 1
RP/0/RP0/CPU0:router(config-sbc-dbe-vdbe-h248)# end
RP/0/RP0/CPU0:router(config-sbc-dbe-vdbe)# controller h248 2
RP/0/RP0/CPU0:router(config-sbc-dbe-vdbe-h248)#
```

Session Border Controller SBE Configuration Mode

Prompt: (config-sbc-sbe)

Enter the signaling border element (SBE) configuration mode for an SBC instance by using the **sbe** command in SBC configuration mode. The SBE mode and applicable commands pertain to the signaling aspects of a particular SBC instance.

In the current release, you can configure:

- A DBE and an SBE on the same card. If you create both a DBE and an SBE, you must first configure the DBE.
- A standalone SBE on a card. If you want to add a DBE after adding a standalone SBE, you must first delete the SBE and then add the DBE, followed by the SBE.

For example, enter SBE configuration mode for the SBC service instance named mySBC:

```
RP/0/RP0/CPU0:router(config)# sbc mySBC
RP/0/RP0/CPU0:router(config-sbc)# sbe
RP/0/RP0/CPU0:router(config-sbc-sbe)#
```

SBC SBE Routing Policy Configuration Mode

Prompt: (config-sbc-sbe-rtgpolicy)

Enter the mode for configuring a routing policy within a signaling border element (SBE) entity by using the **routing-policy-set** command in SBE configuration mode. If the policy does not exist, using this command creates it. A policy set cannot be destroyed or modified if that policy set is marked as complete.

For example, create an empty policy set identified by the number 1 for the SBC instance named mySBC:

```
RP/0/RP0/CPU0:router(config)# sbc mySBC sbe
RP/0/RP0/CPU0:router(config-sbc-sbe)# routing-policy-set 1
RP/0/RP0/CPU0:router(config-sbc-sbe-rtgpolicy)#
```

SBC RADIUS Account Configuration Mode

Prompt: (config-sbc-sbe-acc)

Enter the mode for creating and configuring a RADIUS accounting client by using the **radius-account** command in signaling border element (SBE) configuration mode. Each client maintains a list of servers consisting of one active server and a set of standby servers. The list is traversed by the client in the order of user-configured priorities. If the named client does not exist, using the **radius-account** command creates it.

If call detail reports (CDRs) must be sent to multiple RADIUS servers simultaneously, you can configure an SBC instance to have multiple clients (each with its own ordered set of servers).

An accounting client sends a CDR to the active server. If the active server cannot be contacted, a standby server is used.

For example, create a RADIUS accounting client named radius1. The radius1 client belongs to the SBC service instance named mySBC:

```
RP/0/RP0/CPU0:router(config)# sbc mySBC sbe
RP/0/RP0/CPU0:router(config-sbc-sbe)# radius-account radius1
RP/0/RP0/CPU0:router(config-sbc-sbe-acc)#
```

SBC H.323 Adjacency Configuration Mode

Prompt: (config-sbc-sbe-adj-h323)

Enter the mode for configuring a signaling border element (SBE) H.323 adjacency within an SBC service instance by using the **adjacency h323** command in SBE configuration mode. If a particular adjacency does not exist, the first-time identification of the adjacency to this command creates it.

For example, create an H.323 adjacency called h323ToIsp42 for the SBC service instance called mySBC:

```
RP/0/RP0/CPU0:router(config)# sbc mySBC sbe
RP/0/RP0/CPU0:router(config-sbc-sbe)# adjacency h323 h323ToIsp42
RP/0/RP0/CPU0:router(config-sbc-sbe-adj-h323)#
```

SBC SIP Adjacency Configuration Mode

Prompt: (config-sbc-sbe-adj-sip)

Enter the configuration mode for Session Initiation Protocol (SIP) by using the **adjacency sip** command in signaling border element (SBE) configuration mode. If this SIP adjacency does not exist, using this command creates it.

For example, create an SIP adjacency called SipToIsp42 for the SBC service instance named mySBC:

```
RP/0/RP0/CPU0:router(config)# sbc mySBC sbe
RP/0/RP0/CPU0:router(config-sbc-sbe)# adjacency sip SipToIsp42
RP/0/RP0/CPU0:router(config-sbc-sbe-adj-sip)#
```

SBC CAC Policy Configuration Mode

Prompt: (config-sbc-sbe-cacpolicy)

Enter the mode for configuring call admission control (CAC) policy set by using the **cac-policy-set** command in signaling border element (SBE) configuration mode. If the CAC policy does not exist, this command creates it. If a policy is marked as complete, you cannot change it. Further, a policy set cannot be destroyed if it is marked as complete.

For example, create an empty (new) policy set with an ID of 1 for the SBC service instance named mySBC:

```
RP/0/RP0/CPU0:router(config)# sbc mySBC sbe
RP/0/RP0/CPU0:router(config-sbc-sbe)# cac-policy-set 1
RP/0/RP0/CPU0:router(config-sbc-sbe-cacpolicy)#
```

SBC CAC Table Configuration Mode

Prompt: (config-sbc-sbe-cacpolicy-cactable)

Enter the mode for configuring a call admission control (CAC) table by using the **cac-policy-table** command in CAC policy configuration mode. A CAC table exists within the context of a CAC policy set. The CAC policy set exists within a signaling border element (SBE). If the named CAC table does not exist, this command creates it.

If a policy set to which a table belongs is marked as being complete, you cannot modify the CAC table. Also, a CAC table cannot be destroyed if its context is that of a complete policy.

For example, create the CAC table named MyCacTable for the CAC policy set whose ID is 1. The SBC service instance is named mySBC:

```
RP/0/RP0/CPU0:router(config)# sbc mySBC sbe
RP/0/RP0/CPU0:router(config-sbc-sbe)# cac-policy-set 1
RP/0/RP0/CPU0:router(config-sbc-sbe-cacpolicy)# cac-table MyCacTable
RP/0/RP0/CPU0:router(config-sbc-sbe-cacpolicy-cactable)#
```

SBC CAC Table Entry Configuration Mode

Prompt: (config-sbc-sbe-cacpolicy-cactable-entry)

Enter the mode for specifying entries in an SBC SBE CAC table for an CAC policy by using the **entry** command in CAC table configuration mode. For a description of the commands that let you specify the entries in the mode, see the *CAC Policy Table Entry Commands* module in *Cisco IS XR Session Border Controller Command Reference*.

For example, configure the next table to process in a new CAC table called MyCacTable, and identify that table as MyCacTable2:

```
RP/0/RP0/CPU0:router(config)# sbc mySBC sbe
RP/0/RP0/CPU0:router(config-sbc-sbe)# cac-policy-set 1
RP/0/RP0/CPU0:router(config-sbc-sbe-cacpolicy)# cac-table MyCacTable
RP/0/RP0/CPU0:router(config-sbc-sbe-cacpolicy-cactable)# entry 1
RP/0/RP0/CPU0:router(config-sbc-sbe-cacpolicy-cactable-entry)# action next-table
MyCacTable2
```

SBC Local Billing Configuration Mode

Prompt: (config-sbc-sbe-lclbill)

Enter the configuration mode for a local billing policy by using the **billing-local** command in SBE configuration mode.

For example, enter the local billing mode for the SBC service instance named mySBC but do so from the global configuration mode:

```
RP/0/RP0/CPU0:router(config)# sbc mySBC sbe
RP/0/RP0/CPU0:router(config-sbc-sbe)# billing-local
RP/0/RP0/CPU0:router(config-sbc-sbe-lclbill)
```

SBC Media Gateway Configuration Mode

Prompts:

- (config-sbc-sbe-mg) for **media-gateway ipv4** command
- (config-sbc-sbe-media-gateway) for **codecs** and **transcoder** commands

Enter media gateway configuration mode for a signaling border element (SBE) by using the **media-gateway** command in SBE configuration mode. This command takes an IPv4 H.248 control IP address as an argument.

For example, enter media gateway configuration mode for the media gateway with IP address 10.0.0.1:

```
RP/0/RP0/CPU0:router(config)# sbc mySBC sbe
RP/0/RP0/CPU0:router(config-sbc-sbe)# media-gateway ipv4 10.0.0.1
RP/0/RP0/CPU0:router(config-sbc-sbe-mg)#
```

For example, enter media gateway configuration mode for the media gateway with IP address 10.0.0.1, and then specify the following codecs for the media gateway:

```
RP/0/RP0/CPU0:router(config)# sbc mySBC sbe
RP/0/RP0/CPU0:router(config-sbc-sbe)# media-gateway ipv4 10.0.0.1
RP/0/RP0/CPU0:router(config-sbc-sbe-media-gateway)# codecs "m=audio 6000 RTP/AVP
4,a=rtpmap:0 PCMU/8000"
```

SBC Remote Billing Configuration Mode

Prompt: (config-sbc-sbe-rmtbill)

Enter the configuration mode for a remote billing policy by using the **billing-remote** command in signaling border element (SBE) configuration mode.

For example, enter the remote billing mode for the SBC service instance named mySBC:

```
RP/0/RP0/CPU0:router(config)# sbc mySBC sbe
RP/0/RP0/CPU0:router(config-sbc-sbe)# billing-remote
RP/0/RP0/CPU0:router(config-sbc-sbe-rmtbill)
```

SBC RADIUS Accounting Server Configuration Mode

Prompt: (config-sbc-sbe-acc-ser)

Enter the mode for configuring ordered lists of RADIUS accounting servers by using the **accounting-server** command in RADIUS accounting configuration mode. You can specify any number of accounting servers. When a call is terminated, a call detail report (CDR) is sent to the server that has the highest priority.

For example, create an instance of the accounting servers named castor and pollux for the RADIUS accounting client named radius1. The name of the SBC service instance is mySBC.

```
RP/0/RP0/CPU0:router(config)# sbc mySBC sbe
RP/0/RP0/CPU0:router(config-sbc-sbe)# radius-account radius1
RP/0/RP0/CPU0:router(config-sbc-sbe-acc)# accounting-server castor
RP/0/RP0/CPU0:router(config-sbc-sbe-acc-ser)# end
RP/0/RP0/CPU0:router(config-sbc-sbe-acc)# accounting-server pollux
RP/0/RP0/CPU0:router(config-sbc-sbe-acc-ser)#
```

SBC RADIUS Authentication Configuration Mode

Prompt: (config-sbc-sbe-auth)

Enter the SBC RADIUS authentication configuration mode by using the **radius authentication** command in SBC SBE configuration mode.

For example, configure an authentication server named bengal. The name of the SBC service instance is mySBC.

```
RP/0/RP0/CPU0:router(config)# sbc mySBC sbe
RP/0/RP0/CPU0:router(config-sbc-sbe)# radius authentication
RP/0/RP0/CPU0:router(config-sbc-sbe-auth)# server bengal
RP/0/RP0/CPU0:router(config-sbc-sbe-auth-ser)#
```

SBC RADIUS Authentication Server Configuration Mode

Prompt: (config-sbc-sbe-auth-ser)

Enter the SBC RADIUS authentication server configuration mode by using the **server** command in RADIUS authentication configuration mode.

For example, configure authentication servers named castor and pollux for RADIUS authorization. Identify the server by IP address 10.0.0.1. The name of the SBC service instance is mySBC.

```
RP/0/RP0/CPU0:router(config)# sbc mySBC sbe
RP/0/RP0/CPU0:router(config-sbc-sbe)# radius authentication
RP/0/RP0/CPU0:router(config-sbc-sbe-auth)# server castor
RP/0/RP0/CPU0:router(config-sbc-sbe-auth-ser)# address ipv4 10.0.0.1
RP/0/RP0/CPU0:router(config-sbc-sbe-auth-ser)# end
RP/0/RP0/CPU0:router(config-sbc-sbe-auth)# server pollux
RP/0/RP0/CPU0:router(config-sbc-sbe-auth-ser)# address pollux
```

SBC Routing Policy Number Analysis Configuration Mode

Prompt: (config-sbc-sbe-rtgpolicy-natable)

Enter the configuration mode of a number analysis table within the context of a signaling border element (SBE) routing policy set. In this mode, you can create or configure a table that consists of all of the following types of content:

- Destination number—the whole called number (by using the **na-dst-number-table** command)
- Destination prefix—the prefix of the called number (by using the **na-dst-prefix-table** command)
- Source adjacency—by using the **na-src-adjacency-table** command
- Source account—by using the **na-src-account-table** command

If the identified number analysis table does not exist, this command creates it. Within a policy set, a table name must be unique across all tables.

For example, create a number analysis table named MyNaTable with entries that are to be matched against the entire dialed number. In this case, the number of the routing policy is 1, and the SBC service instance is named mySBC:

```
RP/0/RP0/CPU0:router(config)# sbc mySbc sbe
RP/0/RP0/CPU0:router(config-sbc-sbe)# routing-policy-set 1
RP/0/RP0/CPU0:router(config-sbc-sbe-rtgpolicy)# na-dst-number-table MyNaTable
RP/0/RP0/CPU0:router(config-sbc-sbe-rtgpolicy-natable)#
```

SBC Routing Policy Number Analysis Entry Configuration Mode

Prompt: (config-sbc-sbe-rtgpolicy-natable-entry)

Enter the mode for configuring an entry to a number analysis table within the context of an SBE routing policy set by using the **entry** command. The mode in which you use the **entry** command is a number analysis table configuration mode.

To use the **entry** command, first specify a number analysis table that applies to a destination number, destination prefix, source adjacency, or source account. When you enter one of the commands from the preceding list, the prompt shows only that you are configuring for a number analysis table (not the type of number analysis table), and when you subsequently use the **entry** command for one of these types of number analysis constituents, the prompt changes to show only “entry.” The examples illustrate this progression.

Within a number analysis table, each entry must have a unique number.

For example, create the first entry (entry number = 1) in a new destination prefix number analysis table named MyNaTable. The MyNaTable table belongs to routing policy set 1.

```
RP/0/RP0/CPU0:router(config)# sbc mySbc sbe
RP/0/RP0/CPU0:router(config-sbc-sbe)# routing-policy-set 1
RP/0/RP0/CPU0:router(config-sbc-sbe-rtgpolicy)# na-dst-prefix-table MyNaTable
RP/0/RP0/CPU0:router(config-sbc-sbe-rtgpolicy-natable)# entry 1
RP/0/RP0/CPU0:router(config-sbc-sbe-rtgpolicy-natable-entry)#
```

Create an entry for a source adjacency number analysis table called MyOtherNaTable. The MyOtherNaTable table belongs to a routing policy set with an ID of 1.

```
RP/0/RP0/CPU0:router(config)# sbc mySbc sbe
RP/0/RP0/CPU0:router(config-sbc-sbe)# routing-policy-set 1
RP/0/RP0/CPU0:router(config-sbc-sbe-rtgpolicy)# na-src-adjacency-table MyOtherNaTable
RP/0/RP0/CPU0:router(config-sbc-sbe-rtgpolicy-natable)# entry 1
RP/0/RP0/CPU0:router(config-sbc-sbe-rtgpolicy-natable-entry)#
```

Secure Domain Router Configuration Mode

Prompt: (admin-config-sdr:*router*)

Enter secure domain router (SDR) configuration mode by entering the **sdr** command in administrative configuration mode. After you name a new or an existing SDR, the CLI enters SDR configuration mode. The prompt for this mode contains the name of the router.

For example, create an SDR named testbed:

```
RP/0/RP1/CPU0:router# admin
RP/0/RP1/CPU0:router(admin)# configure
RP/0/RP1/CPU0:router(admin-config)# sdr testbed
RP/0/RP1/CPU0:router(admin-config-sdr:testbed)#
```

SBC Routing Policy Routing Table Configuration Mode

Prompt: (config-sbc-sbe-rtgpolicy-rtgtable)

Enter the SBE routing policy routing table configuration mode by using any of the following commands in routing policy mode:

- **rtg-dst-address-table**
- **rtg-src-address-table**
- **rtg-src-adjacency-table**
- **rtg-src-account-table**
- **rtg-round-robin-table**

Any of these commands places the CLI in the routing table mode for specifying entries within a routing table. The command you can subsequently use for configuring a table entry is the **entry** command.

For example, create a source address table called MyRtgTable. The SBC service instance is called mySBC, and the routing policy set ID is 1:

```
RP/0/RP0/CPU0:router(config)# sbc mySbc sbe
RP/0/RP0/CPU0:router(config-sbc-sbe)# routing-policy-set 1
RP/0/RP0/CPU0:router(config-sbc-sbe-rtgpolicy)# rtg-src-address-table MyRtgTable
RP/0/RP0/CPU0:router(config-sbc-sbe-rtgpolicy-rtgtable)#
```

SBC Routing Policy Routing Table Entry Configuration Mode

Prompt: (config-sbc-sbe-rtgpolicy-rtgtable-entry)

Enter the mode for specifying entries in a routing policy routing table by using the **entry** command in the routing table mode for a particular routing policy. A particular routing table mode is entered by using one of the following commands in routing policy mode:

- **rtg-dst-address-table**
- **rtg-src-address-table**
- **rtg-src-adjacency-table**
- **rtg-src-account-table**
- **rtg-round-robin-table**

See also the description of SBC Routing Policy Routing Table Configuration Mode.

For example, create an entry with a value of 1 in a new round-robin routing table called MyRtgTable. The SBC service instance is called mySBC, and the routing policy set ID is 1:

```
RP/0/RP0/CPU0:router(config)# sbc mySBC sbe
RP/0/RP0/CPU0:router(config-sbc-sbe)# routing-policy-set 1
RP/0/RP0/CPU0:router(config-sbc-sbe-rtgpolicy)# rtg-round-robin-table MyRtgTable
RP/0/RP0/CPU0:router(config-sbc-sbe-rtgpolicy-rtgtable)# entry 1
RP/0/RP0/CPU0:router(config-sbc-sbe-rtgpolicy-rtgtable-enable)#
```

Session Group Configuration Mode

Prompt: (config-bgp-sngrp)

Enter the session group configuration mode by using the **session-group** command in router configuration mode. In session group configuration mode, you can configure values that are independent of address family configuration. In turn, neighbors can inherit these configured values.

The **session-group** command allows you to create a session group from which neighbors can inherit an address family-independent configuration. A neighbor inherits the configuration from a session group by way of the **use** command. If a neighbor is configured to use a session group, the neighbor (by default) inherits the session group's entire configuration. A neighbor does not inherit all the configuration from a session group if a configuration is done directly on that neighbor.

For example, define a session group named session1, and then configure neighbor 172.168.40.24 to use session1. Consequently, the session1 configuration also takes effect on the neighbor.

```
RP/0/RP0/CPU0:router(config)# router bgp 1
RP/0/RP0/CPU0:router(config-bgp)# session-group session1
RP/0/RP0/CPU0:router(config-bgp-sngrp)# advertisement-interval 40
RP/0/RP0/CPU0:router(config-bgp-sngrp)# timers 30 90
RP/0/RP0/CPU0:router(config-bgp-sngrp)# exit
RP/0/RP0/CPU0:router(config-bgp)# neighbor 172.168.40.24
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 2
RP/0/RP0/CPU0:router(config-bgp-nbr)# use session-group session1
RP/0/RP0/CPU0:router(config-bgp-nbr)# exit
```

SONET/SDH Configuration Mode

Prompt: (config-sonet)

Enter SONET/SDH configuration mode from global configuration mode by using the **controller sonet** command and providing it with the interface identifier.

For example, all packets are looped back to the SONET/SDH controller:

```
RP/0/RP0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/RP0/CPU0:router(config-sonet)# loopback internal
```

To set the SONET/SDH overhead bytes in the frame header to a specific standards requirement or to ensure interoperability with equipment from another vendor, use the **overhead** command.

For example, set the **s1s0** keyword to 2 for SDH. (The **s1s0** keyword defines the S1 and S0 bits for the SONET/SDH transmission equipment. 0=SONET, and 2=SDH.)

```
RP/0/RP0/CPU0:router(config)# controller sonet 0/1/0/1
RP/0/RP0/CPU0:router(config-sonet)# overhead sls0 2
```

SONET/SDH Path Configuration Mode

Prompt: (config-sonet-path)

Enter SONET/SDH path configuration mode from SONET/SDH configuration mode by using the **path** command. After the CLI enters SONET/SDH path configuration mode, you can run the following SONET/SDH-specific commands: **ais-shut**, **overhead**, **report**, **scrambling**, **threshold**, and **uneq-shut**. The SONET/SDH standards permit or require user access for configuration of some bytes or bits in the SONET/SDH path overhead. Use the **overhead** command to set the SONET/SDH path overhead bytes in the frame header to a specific standards requirement.

For example, use the **overhead** command to set the SONET/SDH path overhead bytes in the frame header. In this case, set the c2 value to 0x13t:

```
RP/0/RP0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/RP0/CPU0:router(config-sonet)# path
RP/0/RP0/CPU0:router(config-sonet-path)# overhead c2 0x13
```

Subinterface Configuration Mode

Prompt: (config-subif)

Enter the interface submode from global configuration mode to configure a variety of technologies, such as virtual local area network (VLAN).

For example, first create of a Ten Gigabit Ethernet subinterface with ID 0/2/0/4.1, and then specify a VLAN of 10. Lastly, configure an interface IP address of 10.0.0.1/24:

```
RP/0/RP0/CPU0:router# configure terminal
RP/0/RP0/CPU0:router(config)# interface TenGigE 0/2/0/4.1
RP/0/RP0/CPU0:router(config-subif)# dot1q vlan 10
RP/0/RP0/CPU0:router(config-subif)# ip addr 10.0.0.1/24
```

TACACS+ Server Group Configuration Mode

Prompt: (config-sg-tacacs+)

Enter TACACS+ server group configuration mode from global configuration mode by using the **aaa group server tacacs+** command. This command lets you group different server hosts into distinct lists.

For example, enter TACACS+ server group configuration mode, and then specify the IP address of an external TACACS+ server to be 192.168.60.15:

```
RP/0/RP0/CPU0:router(config)# aaa group server tacacs+
RP/0/RP0/CPU0:router(config-sg-tacacs+)# server 192.168.60.15
```

Task Group Configuration Mode

Prompt: (config-tg)

Enter task group configuration mode from global configuration mode. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

For example, create the following description of a task group named alpha: “this is a sample user group.”

```
RP/0/RP0/CPU0:router(config)# taskgroup alpha
RP/0/RP0/CPU0:router(config-tg)# description this is a sample taskgroup
```

Template Configuration Mode

Prompt: (config-TPL)

Enter template configuration mode by using the **template** command with the name of a new or existing template in global configuration mode. In template configuration mode, you can specify the details of a template. Subsequently, the template can be applied to a router or to a particular interface.

For example, enter template configuration mode by creating a template named pre-pos (for preconfiguring a POS interface). The configuration consists of the preconfigured Packet-over-SONET interface 0/1/0/1:

```
RP/0/RP0/CPU0:router(config)# template pre-pos
RP/0/RP0/CPU0:router(config-TPL)# interface preconfigure pos0/1/0/0
RP/0/RP1/CPU0:router(config-if-pre)# ipv4 address 10.3.32.154 255.0.0.0
```

Transport Configuration Mode

Prompt: (config-transport)

Enter transport configuration mode from global configuration mode by using the **crypto ipsec transport** command. In transport configuration mode, you can specify the crypto profile to use in IPSec processing and then determine which traffic is protected and how that traffic is protected.

For example, configure the crypto profile as shown:

```
RP/0/RP0/CPU0:router(config)# crypto ipsec transport
RP/0/RP0/CPU0:router(config-transport)# profile pn1
RP/0/RP0/CPU0:router(config)# interface tunnel-ipsec0
RP/0/RP0/CPU0:router(config-if)# profile pn1
```

Trustpoint Configuration Mode

Prompt: (config-trustp)

Enter the trustpoint configuration mode from global configuration mode. Use the **crypto ca trustpoint** command to create a new trustpoint or identify an existing trustpoint for you to modify. After you use this command, the CLI enters trustpoint configuration mode. In this mode, the available commands are **enrollment retry count**, **enrollment retry period**, **enrollment url**, **query url**, and **rsakeypair**.

For example, use the **crypto ca trustpoint** command to create a trustpoint called myca:

```
RP/0/RP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RP0/CPU0:router(config-trustp)# enrollment url http://myca.mydomain.com
```

For example, declare a certification authority (CA); change the retry period to 10 minutes; and change the retry count to 60 retries.

```
RP/0/RP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RP0/CPU0:router(config-trustp)# enrollment url http://ca_server
RP/0/RP0/CPU0:router(config-trustp)# enrollment retry period 10
RP/0/RP0/CPU0:router(config-trustp)# enrollment retry count 60
```

Tunnel Configuration Mode

Prompt: (config-if)

Enter tunnel configuration mode for MPLS traffic engineering by using the **interface tunnel-te** command in global configuration mode.

For example, enable fast reroute on an MPLS traffic engineering tunnel:

```
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# fast-reroute
```

User Group Configuration Mode

Prompt: (config-ug)

Enter usergroup configuration mode by executing the **usergroup** command global configuration mode. In this mode, you can create or configure a user group.

For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

For example, create a description of a user group named alpha: “this is a sample user group.”

```
RP/0/RP0/CPU0:router(config)# usergroup alpha
RP/0/RP0/CPU0:router(config-ug)# description this is a sample user group
```

For example, add permissions from the user group beta to the user group alpha:

```
RP/0/RP0/CPU0:router(config)# usergroup alpha
RP/0/RP0/CPU0:router(config-ug)# inherit usergroup beta
```

Username Configuration Mode

Prompt: (config-un)

Enter username configuration mode by executing the **username** command in global configuration mode. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

For example, create a login password for the user named user1 by running the **password** command. For user1, create an unencrypted password to be pwd1:

```
RP/0/RP0/CPU0:router(config)# username user1
RP/0/RP0/CPU0:router(config-un)# password 0 pwd1
```

For example, enter username configuration mode by specifying a user named enzo, and then create a group named ferrari. (Groups are created in username configuration mode.)

```
RP/0/RP1/CPU0:router(config)# username enzo
RP/0/RP1/CPU0:router(config-un)# group ferrari
```

Virtual-link Configuration Mode

Prompt: (config-router-ar-vl)

Enter virtual link configuration mode from the area command mode for OSPF or OSPFv3. Provide the router ID of the virtual link neighbor as input to the **virtual-link** command. For OSPF, you can set the estimated time required to send a link-state update packet on the interface.

For OSPFv3, you can:

- Specify the time from the start of one link-state advertisement (LSA) transmissions to the next transmission for adjacencies on an interface
- Specify the interval between hello packets that OSPFv3 sends on an interface
- Set the interval after which a neighbor is declared dead when no hello packets are observed
- Set the estimated time required to send a link-state update packet on the interface

For example, after you specify area 0, enter virtual-link mode by specifying the router ID 10.1.0.1. Configure a transmit delay of 50 seconds:

```
RP/0/RP1/CPU0:router(config)# router ospf 10
RP/0/RP1/CPU0:router(config-ospf)# area 0
RP/0/RP1/CPU0:router(config-ospf-ar)# virtual-link 10.0.0.1
RP/0/RP1/CPU0:router(config-ospf-ar-vl)# transmit-delay 50
```

Virtual Private Network Routing and Forwarding Mode

Prompt: (config-*protocol*-vrf)

Enter VPN routing and forwarding (VRF) configuration mode by using the **vrf** command in the router configuration mode for the chosen protocol.

For example, in router BGP configuration mode, enter VRF mode for the instance named new1:

```
RP/0/RP0/CPU0:router (config-bgp)# vrf new1
RP/0/RP0/CPU0:router (config-bgp-vrf)#
```

Virtual Private Network Routing and Forwarding Neighbor Mode

Prompt: (config-*protocol*-vrf-nbr)

Enter the neighbor submode for VPN routing and forwarding (VRF) by using the **neighbor** command in VRF configuration mode. The *protocol* is whatever is specified for the router configuration mode.

For example, enter the configuration submode for a BGP VRF instance named new1 for the neighbor at 10.1.1.1:

```
RP/0/RP0/CPU0:router(config-bgp)# vrf newb1
RP/0/RP0/CPU0:router(config-bgp-vrf)# neighbor 10.1.1.1
RP/0/RP0/CPU0:router(config-bgp-vrf-nbr)#
```

VPNv4 Address Family Group Command Mode

Prompt: (config-*protocol*-af)

Enter VPNv4 address family group configuration mode by using the **address-family vpnv4 unicast** command in router configuration mode for the selected protocol.

For example, enter address family VPNv4 unicast mode:

```
RP/0/RP0/CPU0:router(config-bgp)# address-family vpnv4 unicast
RP/0/RP0/CPU0:router(config-bgp-af)#
```

VPNv4 Neighbor Group Address Family Command Mode

Prompt: (config-*protocol*-nbr-af)

Enter the neighbor group address family configuration mode for VPNv4 unicast by using the **neighbor group** command in router configuration mode for the chosen protocol. (See the example.)

For example, from BGP router configuration mode, enter neighbor configuration mode for 10.1.1.1. Enter the neighbor group address family configuration mode for VPNv4 unicast.

```
RP/0/RP0/CPU0:router(config-bgp)# neighbor 10.1.1.1
RP/0/RP0/CPU0:router(config-bgp-nbr)# address-family vpnv4 unicast
RP/0/RP0/CPU0:router(config-bgp-nbr-af)#
```

VRRP Interface Configuration Mode

Prompt: (config-vrrp-if)

Enter Virtual Router Redundancy Protocol (VRRP) interface configuration mode by using the **interface** command in router VRRP configuration mode.

For example, enable VRRP on Ten Gigabit Ethernet interface 0/3/0/0. The VRRP virtual router identifier is 1, and 10.0.1.20 is the IP address of the virtual router.

```
RP/0/RP0/1:router(config)# router vrrp
RP/0/RP0/1:router(config-vrrp)# interface TenGigE 0/3/0/0
RP/0/RP0/1:router(config-vrrp-if)# vrrp 1 ipv4 10.0.1.20
```

Cisco IOS XR Command Prompts

This chapter helps you determine the current CLI mode by the information that appears in the prompt. The chapter primarily consists of a table with all the standard user-prompts. The prompts are listed in alphabetical order as the method for navigating the table.

The first column in Table 2-1 contains the prompts arranged in alphabetical order. For each prompt, the following information is provided:

- The section in the "Cisco IOS XR Command Mode Descriptions" chapter that describes the mode
- The method of accessing the mode
- An example of entry to the mode

The availability of a command mode depends on the feature set in the software image and on the router.

Table 2-1 CLI Prompts and Modes

Prompt	Mode Section	Access Method	Example
(admin)	Administration EXEC Mode	Enter from executive mode: use the **admin** command.	`router# admin` `router(admin)#`
(admin-config)	Administration Configuration Mode	In admin mode, enter the **configuration** command.	`(admin)# configure` `(admin-config)#`

(admin-config-pairing:drp_name)	Distributed Route Processor Pairing Mode	In the administration configuration mode, use the **pairing** command with the name of a pair.	`router# admin`
			`router(admin)# config`
			`router(admin-config)# pairing drp1`
			`router(admin-config-pairing:drp1)# location 0/3/* 0/4/*`

(admin-config-sdr:)	Secure Domain Router Configuration Mode	In administration configuration mode, use the **sdr** command.	`router# admin`
			`(admin)#config`
			`(admin-config)#sdr test`
			`(admin-config-sdr:test)#`

(config-aps)	Administration EXEC Mode	Use the **aps group** command in global configuration mode.	`(config)# aps group 1` `(config-aps)#`

Table 2-1 CLI Prompts and Modes (continued)

Prompt	Mode Section	Access Method	Example
(config-bgp)	Router Configuration Mode	In global configuration mode, use the **router** command.	`(config)# router bgp 140` `(config-bgp)#`
(config-bgp-afgrp)	Address Family Group Configuration Mode	Use the **af-grp** command in router configuration mode for BGP	`(config-bgp)# af-group newgroup1 address-family ipv4 unicast` `(config-bgp-afgrp)#`
(config-bgp-confed-peers)	BGP Confederation Peers Configuration Mode	Use the **config-bgp-confed-peers** command in BGP router configuration mode.	`(config)# router bgp 1095` `(config-bgp)# bgp confederation peers`
(config-bgp-nbr)	Neighbor Configuration Mode	In router config mode for BGP, use the **neighbor** command.	`(config-bgp)# neighbor 10.0.0.1` `(config-bgp-nbr)#`
(config-bgp-nbrgrp)	Neighbor Group Configuration Mode	Use the **neighbor-group** command in neighbor configuration mode.	`(config-bgp)# neighbor-group` `(config-bgp-nbrgrp)`

(config-bgp-nbrgrp-af)	Neighbor Group Address Family Configuration Mode	Use the **address-family** command in neighbor group configuration mode.	`(config-bgp)# neighbor-group rrclients`
			`(config-bgp-nbrgrp)# remote-as 65534`
			`router(config-bgp-nbrgrp)# address-family ipv4 unicast`
			`router(config-bgp-nbrgrp-af)`

(config-client-keys)	Key Chain Mode	In global configuration mode, use the **key chain** command.	`(config)# key chain isis-keys` `(config-isis-keys)#`

(config-client-keys-key-id)	Keychain-Key Mode	In keychain-key configuration mode use the **key** command.	`(config)# key chain isis-keys`
			`(config-isis-keys)# key 8`
			`(config-isis-keys-0x8)#`

(config-cmap)	Class Map Configuration Mode	Use the **class-map** command in global configuration mode.	`(config)# class-map class1` `(config-cmap)#`
(config-dwdm)	DWDM Controller Mode	Use the **controller dwdm** command in global configuration mode.	`(config)# controller dwdm 0/6/0/0` `(config-dwdm)#`
(config-eigrp)	Router Configuration Mode	Use the **router eigrp** command in global configuration mode.	`(config)# router eigrp 1` `(config-eigrp)#`

Table 2-1 CLI Prompts and Modes (continued)

Prompt	Mode Section	Access Method	Example
(config-eigrp-af)	Address Family Configuration Mode	Use the **address family** command in EIGRP router configuration mode.	`(config-eigrp)# address-family ipv6 unicast` `(config-eigrp-af)#`
(config-eigrp-af-if)	Interface Configuration Mode (Protocol Areas)	Use the **interface** command in EIGRP address family configuration mode.	`(config-eigrp-af)# interface POS 0/1/0/0` `(config-eigrp-af-if)#`
(config-expl-path)	Explicit Path Configuration Mode	Use the **explicit-path** command in global configuration mode.	`(config)# explicit-path identifier 200` `(config-expl-path)# exclude-address 192.168.3.2`

(config-if-pos)	POS Interface Configuration Mode	Use the **pos** command in interface configuration mode.	`(config)# interface POS 0/1/0/2`
			`(config-if)# pos`
			`(config-if-pos)# crc 32`

(config-if-pre)	Interface Preconfiguration Mode	Use the **interface preconfigure** command in template configuration mode.	`(config-TPL)# interface preconfigure pos0/1/0/0` `(config-if-pre)#`
(config-if-sbc)	Interface Session Border Controller Configuration Mode	Use the **interface sbc** command in global configuration mode.	`(config)# interface sbc sbcControlIf` `(config-if-sbc)#`
(config-igmp)	Router IGMP Configuration Mode	Use the **router igmp** command in global configuration mode.	`(config)# router igmp` `(config-igmp)# interface pos 0/1/0/1`

(config-igmp-if)	Interface IGMP Configuration Mode	In router IGMP configuration mode, use the **interface** command.	`(config)# router igmp`
			`(config-igmp)# interface pos 0/1/0/1`
			`(config-igmp-if)#`

(config-ipsla-icmp-echo)	IP SLA ICMP Echo Configuration Mode	Use the **type icmp echo** command in IP SLA operation configuration mode.	`(config-ipsla-op)# type icmp echo` `(config-ipsla-icmp-echo)#`
(config-ipsla-icmp-path-echo)	IP SLA ICMP Path-Echo Configuration Mode	Use the **type icmp path-echo** command in IP SLA operation configuration mode.	`(config-ipsla-op)# type icmp path-echo` `(config-ipsla-icmp-path-echo)#`
(config-ipsla-icmp-path-jitter)	IP SLA ICMP Path-Jitter Configuration Mode	Use the **type udp jitter** command in IP SLA operation configuration mode.	`(config-ipsla-op)# type udp jitter` `(config-ipsla-udp-jitter#`

Table 2-1 CLI Prompts and Modes (continued)

Prompt	Mode Section	Access Method	Example
(config-ipsla-op)	IP SLA Operation Configuration Mode	Enter the **ipsla operation** command in global configuration mode.	`(config)# ipsla operation 1` `(config-ipsla-op)# type udp echo statistics interval 0 buckets 1`

(config-ipsla-op-hist)	IP SLA Operation History Configuration Mode	Use the **history** command in UDP echo configuration mode.	`(config-ipsla-op)# type udp echo`
			`(config-ipsla-udp-echo)# history`
			`(config-ipsla-op-hist)#`

(config-ipsla-op-stats)	IP SLA Operation Statistics Configuration Mode	Use the **statistics** command in IP SLA UDP jitter mode or IP SLA UDP path echo mode.	`(config-ipsla-op)# type icmp path-echo`
			`(config-ipsla-icmp-path-echo)# statistics hourly`
			`(config-ipsla-op-stats)#`

(config-ipsla-react)	IP SLA Reaction Configuration Mode	Use the **ipsla reaction operation** command in global configuration mode.	`(config)# ipsla reaction operation 432` `(config-ipsla-react)#`

(config-ipsla-react-cond)	IP SLA Reaction Condition Configuration Mode	Use the **react connection-loss** command in IP SLA reaction configuration mode.	`(config)# ipsla reaction operation 432`
			`(config-ipsla-react)# react connection-loss`
			`(config-ipsla-react-cond# action logging`

(config-ipsla-resp)	IP SLA Responder Configuration Mode	Use the **ipsla responder** command in global configuration mode.	`(config)# ipsla responder` `(config-ipsla-resp)#`
(config-ipsla-sched)	IP SLA Schedule Configuration Mode	Use the **ipsla schedule operation** command in global configuration mode.	`(config)# ipsla schedule operation 1` `(config-ipsla-sched)# recurring`
(config-ipsla-udp-echo)	IP SLA UDP Echo Configuration Mode	Use the **type udp echo** command in IP SLA operation mode.	`(config-ipsla-op)# type udp echo` `(config-ipsla-udp-echo)#`
(config-ipsla-udp-jitter)	IP SLA UDP Jitter Configuration Mode	Use the **type udp jitter** command in IP SLA operation mode.	`(config-ipsla-op)# type udp jitter` `(config-ipsla-udp-jitter#`
(config-ipv4-acl)	IPv4 Access List Configuration Mode	Use the **ipv4 access-list** command in the global configuration mode.	`(config)# ipv4 access-list Internetfilter` `(config-ipv4-acl)# 10 deny 192.168.34.0 0.0.0.255`

Table 2-1 CLI Prompts and Modes (continued)

Prompt	Mode Section	Access Method	Example
(config-ipv4-pfx)	IPv4 Prefix List Configuration Mode	Use the **ipv4 prefix-list** command in the global configuration mode.	`(config)# ipv4 prefix-list list1` `(config-ipv4-pfx)# permit 172.20.10.171/16 le 24`
(config-ipv6-acl)	IPv6 Access List Configuration Mode	Use the **ipv6 access-list** command in the global configuration mode.	`(config)# ipv6 access-list Internetfilter` `(config-ipv6-acl)#`
(config-ipv6-pfx)	IPv6 Prefix List Configuration Mode	Use the **ipv6 prefix-list** command in the global configuration mode.	`(config)# ipv6 prefix-list list1` `(config-ipv6-pfx)# permit 172.20.10.171/16 le 24`
(config-isakmp)	ISAKMP Policy Configuration Mode	In the global configuration, use the **crypto isakmp** command.	`(config)# crypto isakmp policy 15` `(config-isakmp)# hash md5`
(config-isis)	Router Configuration Mode	In global configuration mode, use the **router** command.	`(config)# router isis 140` `(config-isis)#`

(config-isis-if-af)	Interface Address Family Configuration Mode	In the IS-IS interface submode, use the **address-family ipv4** command.	`config)# router isis isp`
			`(config-isis)# interface POS0/1/0/1`
			`(config-isis-if)# address-family ipv4 unicast`
			`(config-isis-if-af)#`

(config-ldp)	MPLS LDP Configuration Mode	Use the **mpls ldp** command in global configuration mode.	`(config)# mpls ldp` `(config-ldp)#`
(config-ldp-if)	MPLS LDP Interface Configuration Mode	Use the **mpls ldp interface** command in global configuration mode.	`(config)# mpls ldp interface POS 0/1/0/0` `(config-ldp-if)`

(config-ldp-lbl-acpt)	MPLS LDP Label Accept Configuration Mode	Use the **label accept** command in MPLS LDP configuration mode.	`(config)# mpls ldp`
			`(config-ldp)# label accept`
			`(config-ldp-lbl-acpt)#`

(config-ldp-lbl-advt)	MPLS LDP Label Advertise Configuration Mode	Use the **label advertise** command in MPLS LDP configuration mode.	`(config)# mpls ldp`
			`(config-ldp)# label advertise`
			`(config-ldp-lbl-advt)#`

(config-ldp-log)	MPLS LDP Log Configuration Mode	Use the **mpls ldp log** command in global configuration mode.	`(config)# mpls ldp log` `(config-ldp-log)#`

Table 2-1 CLI Prompts and Modes (continued)

Prompt	Mode Section	Access Method	Example
(config-line)	Line (Template) Configuration Mode	Use the **line default** command in global configuration mode.	`(config)# line default` `(config-line)#`

(config-mcast-ipv4)	Multicast Routing Configuration Mode	Enter the multicast routing configuration mode by using the **multicast-routing** command in global configuration mode or in EXEC mode.	EXEC mode:
			`router# multicast-routing`
			`router(config-mcast-ipv4)`
			Global configuration mode:
			`(config)# multicast-routing`
			`(config-mcast-ipv4)#`

(config-mcast-ipv4-if)	Interface Mulitcasting Mode	Use the **interface** command or other commands in multicast routing configuration mode.	`(config-mcast-ipv4)# interface pos 0/1/0/0` `(config-mcast-ipv4-if)#`

(config-mld)	Router MLD Configuration Mode	Enter the **router mld** command in global configuration mode.	`(config)# router mld`
			`(config-mld)# interface pos 0/1/0/1`
			`(config-mld-if)# access-group anygroup`

(config-mpls-ouni)	MPLS O-UNI Configuration Mode	Use the **mpls optical-uni** command in global configuration mode.	`(config)# mpls optical-uni` `(config-mpls-ouni)`

(config-mpls-ouni-if)	MPLS O-UNI Interface Configuration Mode	In MPLS O-UNI configuration mode, use the **interface** POS command.	`(config)# mpls optical-uni`
			`(config-mpls-ouni)# interface POS0/1/0/1`
			`(config-mpls-ouni-if)#`

(config-mpls-ouni-if-adj)	O-UNI LMP Datalink Adjacency Configuration Mode	In the interface submode for MPLS O-UNI, run the **lmp data-link adjacency** command.	`(config)# mpls optical-uni`
			`(config-mpls-ouni)# interface POS 0/1/0/1`
			`(config-mpls-ouni-if)# lmp data-link adjacency`
			`(config-mpls-ouni-if-adj)# neighbor router1`

(config-mpls-ouni-if-adj)	O-UNI LMP Neighbor Adjacency Configuration Mode	In the interface submode for MPLS O-UNI, run the **lmp data-link adjacency** command.	`(config)# mpls optical-uni`
			`(config-mpls-ouni)# interface pos 0/2/0/0`
			`(config-mpls-ouni-if)# lmp data-link adjacency`
			`(config-mpls-ouni-if-adj)# remote interface-id 2`

(config-mpls-te)	MPLS TE Configuration Mode	Enter the **mpls traffic-eng** command in the global configuration mode.	`(config)# mpls traffic-eng` `(config-mpls-te)#`

Table 2-1 CLI Prompts and Modes (continued)

Prompt	Mode Section	Access Method	Example

(config-mpls-te-if)	MPLS TE Interface Configuration Mode	In the MPLS traffic engineering mode, use the **interface** command.	`(config)# mpls traffic-eng`
			`(config-mpls-te)# interface pos 0/7/0/0`
			`(config-mpls-te-if)# admin-weight 20`

(config-msdp)	Router MSDP Configuration Mode	Use the **router msdp** command in global configuration mode.	`(config)# router msdp` `(config-msdp)#`

(config-msdp-peer)	Peer Configuration Mode	In router MSDP mode, enter an IP address for the **peer** command.	`(config)# router msdp`
			`(config-msdp)# peer 152.61.2.3`
			`(config-msdp-peer)#`

(config-ntp)	NTP Configuration Mode	Enter the **ntp** command in global configuration mode.	`(config)# ntp` `(config-ntp)#`

(config-ntp-int)	NTP Interface Configuration Mode	Use the **interface** command in NTP configuration mode or the **ntp interface** command in global configuration mode.	`(config)# ntp interface POS 0/0/0/1`
			`(config-ntp-int)#`
			
			or
			
			`(config-ntp)# interface POS 0/0/0/1`
			`(config-ntp-int)#`

(config-oam)	MPLS OAM Configuration Mode	Use the **mpls oam** command in EXEC mode.	`router# configure`
			`(configure)# mpls oam`
			`router(config-oam)#`

(config-ouni-nbr-router)	O-UNI LMP Neighbor Configuration Mode	In MPLS O-UNI configuration mode, use the **lmp neighbor** name command.	`(config-mpls-ouni)# lmp neighbor router1` `(config-ouni-nbr-router1)#`
(config-pim-ipv4)	Router PIM Configuration Mode	Use the **router pim** command in global configuration mode.	`(config)# router pim` `(config-pim-ipv4)#`
(config-pim-ipv4-if)	Interface PIM Configuration Mode	Use the **interface** command in router PIM configuration mode.	`(config-pim-ipv4)# interface pos 0/1/0/0` `(config-pim-ipv4-if)# dr-priority 4`
(config-place)	Placement Program Mode	Use the **placement program** command in global configuration mode.	`router(config)# placement program pim default` `router(config-place)# affinity location-set current attract 100`
(config-pmap)	Policy Map Configuration Mode	Use the **policy-map** command to enter map configuration.	`(config)# policy-map policy1` `(config-pmap)#`

Table 2-1 CLI Prompts and Modes (continued)

Prompt	Mode Section	Access Method	Example
(config-pmap-c)	Policy Map Class Configuration Mode	In policy map configuration mode, use the command.	`(config-pmap)# class class1` `(config-pmap-c)#`

(config-profilename)	Profile Configuration Mode	Use the **crypto ipsec profile** command in global configuration mode.	Prompt shows the profile name.
			`(config)# crypto ipsec profile sampleX`
			`router(config-sampleX)#`

(config-protocol-vrf-nbr)	Virtual Private Network Routing and Forwarding Neighbor Mode	In neighbor configuration mode, use **address-family vpnv4** command	`(config-bgp-nbr)#address-family vpnv4 unicast` `(config-bgp-nbr-af)#`
(config-pubkey-chain)	Public Key Chain Configuration Mode	Use the **crypto key pubkey-chain rsa** command in global configuration mode.	`(config)# crypto key pubkey-chain rsa` `(config-pubkey-chain)#`

(config-pubkey-key)	Public Key Configuration Mode	Use either the **named-key** or the **addressed-key** command in global configuration mode.	`(config)# crypto key pubkey-chain rsa`
			`(config-pubkey-chain)# addressed-key 10.5.5.1`
			`(config-pubkey-key)#`

(config-rd)	Route Distinguisher Configuration Mode	Use the **rd-set** command in global configuration mode.	`(config)# rd-set vpn-1` `(config-rd)# 10.0.0.2:777`

(config-router-ar-vl)	Virtual-link Configuration Mode	In the area command mode for OSPF or OSPFv3, use the **virtual-link** command; include the router ID of the virtual link neighbor.	`(config-ospf)# area 0`
			`(config-ospf-ar)# virtual-link 10.0.0.1`
			`(config-ospf-ar-vl)# transmit-delay 50`

(config-rpl)	Route-policy Configuration Mode	Enter route-policy configuration mode by using the **route-policy** command in global configuration mode.	`(config)# route-policy drop-everything` `(config-rpl)# drop`
(config-rsvp)	RSVP Configuration Mode	Use the **rsvp** command in global configuration mode.	`(config)# rsvp` `(config-rsvp)#`

Table 2-1 CLI Prompts and Modes (continued)

Prompt	Mode Section	Access Method	Example
(config-rsvp-if)	RSVP Interface Configuration Mode	Use the **rsvp interface pos** command in global configuration mode.	`(config)# rsvp interface pos 0/3/0/0` `(config-rsvp-if)#`
(config-sbc)	Session Border Controller Configuration Mode	Use the **sbc** command in global configuration mode.	`(config)# sbc mySBC` `(config-sbc)#`
(config-sbc-dbe)	SBC DBE Configuration Mode	Use the **dbe** command in SBC configuration mode.	`(config-sbc)# dbe` `(config-sbc-dbe)#`

(config-sbc-dbe-media-address)	SBC DBE Media Address Configuration Mode	Use the **media-address vrf** command in DBE configuration mode.	`(config)# sbc mySBC dbe`
			`(config-sbc-dbe)#`
			`media-address vrf vpn3`
			`(config-sbc-dbe-media-address)#`

(config-sbc-dbe-vdbe)	SBC Virtual DBE Configuration Mode	Use the **vdbe** command in the DBE configuration mode.	`(config)# sbc mySBC dbe`
			`(config-sbc-dbe)# vdbe`
			`(config-sbc-dbe-vdbe)#`

(config-sbc-dbe-vdbe-h248)	SBC Virtual DBE H248 Configuration Mode	Use the **controller h248** command in virtual data border element (vDBE) configuration mode.	`(config)# sbc mySBC dbe vdbe`
			`(config-sbc-dbe-vdbe)#`
			`controller h248 1`
			`(config-sbc-dbe-vdbe-h248)#`

(config-sbc-sbe)	Session Border Controller SBE Configuration Mode	Use the **sbe** command in SBC configuration mode.	`(config)# sbc mySBC`
			`(config-sbc)# sbe`
			`(config-sbc-sbe)#`

(config-sbc-sbe-acc)	SBC RADIUS Account Configuration Mode	Use the **radius-account** command in signaling border element (SBE) configuration mode.	`(config)# sbc mySBC sbe`
			`(config-sbc-sbe)#`
			`radius-account radius1`
			`(config-sbc-sbe-acc)#`

(config-sbc-sbe-acc-ser)	SBC RADIUS Accounting Server Configuration Mode	Use the **accounting-server** command in RADIUS accounting configuration mode.	`(config)# sbc mySBC sbe`
			`(config-sbc-sbe)#`
			`radius-account radius1`
			`(config-sbc-sbe-acc)#`
			`accounting-server castor`
			`(config-sbc-sbe-acc-ser)#`

(config-sbc-sbe-adj-h323)	SBC H.323 Adjacency Configuration Mode	Use the **adjacency h323** command in SBE configuration mode.	`(config)# sbc mySBC sbe`
			`(config-sbc-sbe)#`
			`adjacency h323 h323ToIsp42`
			`(config-sbc-sbe-adj-h323)`

Table 2-1 CLI Prompts and Modes (continued)

Prompt	Mode Section	Access Method	Example

(config-sbc-sbe-adj-sip)	SBC SIP Adjacency Configuration Mode	Use the **adjacency sip** command in signaling border element (SBE) configuration mode.	`(config)# sbc mySBC sbe`
			`(config-sbc-sbe)#`
			`adjacency sip SipToIsp42`
			`(config-sbc-sbe-adj-sip)#`

(config-sbc-sbe-auth)	SBC RADIUS Authentication Configuration Mode	Use the **radius authentication** command in signaling border element (SBE) configuration mode.	`(config-sbc-sbe)# radius authentication` `(config-sbc-sbe-auth)#`

(config-sbc-sbe-auth-ser)	SBC RADIUS Accounting Server Configuration Mode	Use the **server** command in RADIUS authentication configuration mode.	`(config-sbc-sbe-auth)#`
			`server castor`
			`(config-sbc-sbe-auth-ser)`
			`#`

(config-sbc-sbe-cacpolicy)	SBC CAC Policy Configuration Mode	Use the **cac-policy-set** command in SBE configuration mode.	`(config)# sbc mySBC sbe`
			`(config-sbc-sbe)#`
			`cac-policy-set 1`
			`(config-sbc-sbe-cacpolicy`
			`)#`

(config-sbc-sbe-cacpolicy-cactable)	SBC CAC Table Configuration Mode	Use the **cac-policy-table** command in CAC policy configuration mode.	`(config)# sbc mySBC sbe`
			`(config-sbc-sbe)#`
			`cac-policy-set 1`
			`(config-sbc-sbe-cacpolicy`
			`)# cac-table MyCacTable`
			`(config-sbc-sbe-cacpolicy`
			`-cactable)#`

(config-sbc-sbe-cacpolicy-cactable-entry)	SBC CAC Table Entry Configuration Mode	Use the **entry** command in CAC table configuration mode.	`(config-sbc-sbe)#`
			`cac-policy-set 1`
			
			`(config-sbc-sbe-cacpolicy`
			`) # cac-table MyCacTable`
			
			`(config-sbc-sbe-cacpolicy`
			`-cactable)# entry 1`
			
			`(config-sbc-sbe-cacpolicy`
			`-cactable-entry)#`

(config-sbc-sbe-lclbill)	SBC Local Billing Configuration Mode	Use the **billing-local** command in SBE configuration mode.	`(config)# sbc mySBC sbe`
			`(config-sbc-sbe)#`
			`billing-local`
			`(config-sbc-sbe-lclbill)`

(config-sbc-sbe-mg)
or
(config-sbc-sbe-media-gateway)
	SBC Media Gateway Configuration Mode	Use the **media-gateway** command in SBE configuration mode.	`(config)# sbc mySBC sbe`
			`(config-sbc-sbe)#`
			`media-gateway ipv4`
			`10.0.0.1`
			`(config-sbc-sbe-mg)#`
			`or`
			`(config-sbc-sbe-media-gat`
			`eway)`

Table 2-1 CLI Prompts and Modes (continued)

Prompt	Mode Section	Access Method	Example

(config-sbc-sbe-qos-fax)	QoS FAX Configuration Mode	Use the **qos fax residential** command in SBC SBE mode.	`(config)# sbc MySbc sbe`
			`(config-sbc-sbe)# qos fax residential`
			`config-sbc-sbe-qos-fax)# marking dscp`

(config-sbc-sbe-qos-video)	QoS Video Configuration Mode	Use the **qos video residential** command in SBC SBE mode.	`(config)# sbc MySbc sbe`
			`(config-sbc-sbe)# qos video residential`
			`config-sbc-sbe-qos-video)# marking dscp`

(config-sbc-sbe-qos-voice)	QoS Voice Configuration Mode	Use the **qos voice residential** command in SBC SBE mode.	`(config)# sbc MySbc sbe`
			`(config-sbc-sbe)# qos voice residential`
			`config-sbc-sbe-qos-voice)# marking dscp`

(config-sbc-sbe-rmtbill)	SBC Remote Billing Configuration Mode	Use the **billing-remote** command in signaling border element (SBE) configuration mode.	`(config)# sbc mySBC sbe`
			`RP/0/RP0/CPU0:router(config-sbc-sbe)#`
			`billing-remote`
			`(config-sbc-sbe-rmtbill)`

(config-sbc-sbe-rtgpolicy)	SBC SBE Routing Policy Configuration Mode	Use the **routing-policy-set** command in SBE configuration mode.	`(config)# sbc mySBC sbe`
			`(config-sbc-sbe)#`
			`routing-policy-set 1`
			`(config-sbc-sbe-rtgpolicy)#`

(config-sbc-sbe-rtgpolicy-natable)	SBC Routing Policy Number Analysis Configuration Mode	Use any of the following in SBE routing policy configuration mode: **na-dst-number-table** **na-dst-prefix-table** **na-src-adjacency-table** **na-src-account-table**	`(config)# sbc mySbc sbe`
			`(config-sbc-sbe)#`
			`routing-policy-set 1`
			`(config-sbc-sbe-rtgpolicy)# na-dst-number-table MyNaTable`
			`(config-sbc-sbe-rtgpolicy-natable)#`

(config-sbc-sbe-rtgpolicy-natable-entry)	SBC Routing Policy Number Analysis Entry Configuration Mode	Use the **entry** command in a number analysis table configuration mode. For details, see the SBC Routing Policy Number Analysis Entry Configuration Mode section	`(config)# sbc mySbc sbe`
			`(config-sbc-sbe)#`
			`routing-policy-set 1`
			`(config-sbc-sbe-rtgpolicy)# na-dst-prefix-table MyNaTable`
			`(config-sbc-sbe-rtgpolicy-natable)# entry 1`
			`(config-sbc-sbe-rtgpolicy-natable-entry)#`

Table 2-1 CLI Prompts and Modes (continued)

Prompt	Mode Section	Access Method	Example

(config-sbc-sbe-rtgpolicy-rtgtable)	SBC Routing Policy Routing Table Configuration Mode	In the routing policy configuration mode, use any of the following commands:
		• **rtg-dst-address-table**
		• **rtg-src-address-table**
		• **rtg-src-adjacency-table**
		• **rtg-src-account-table**
		• **rtg-round-robin-table**
			`(config)# sbc mySbc sbe`
			`(config-sbc-sbe)# routing-policy-set 1`
			`(config-sbc-sbe-rtgpolicy)# rtg-src-address-table MyRtgTable`
			
			`(config-sbc-sbe-rtgpolicy-rtgtable)#`

(config-sbc-sbe-rtgpolicy-rtgtable-entry)	SBC Routing Policy Routing Table Entry Configuration Mode	Use any of the following commands in routing table configuration mode:
		• **rtg-dst-address-table**
		• **rtg-src-address-table**
		• **rtg-src-adjacency-table**
		• **rtg-src-account-table**
		• **rtg-round-robin-table**
			`(config)# sbc mySBC sbe`
			
			`(config-sbc-sbe)# routing-policy-set 1`
			
			`(config-sbc-sbe-rtgpolicy)# rtg-round-robin-table MyRtgTable`
			
			`(config-sbc-sbe-rtgpolicy-rtgtable)# entry 1`
			
			`(config-sbc-sbe-rtgpolicy-rtgtable-enable)#`

(config-sg-radius)	RADIUS Server Group Configuration Mode	Use the **aaa group server tacacs+** command in global configuration mode.	`(config)# aaa group server tacacs+`
(config-sg-tacacs+)	TACACS+ Server Group Configuration Mode	Use the **aaa group server radius** command in global configuration mode.	`(config)# aaa group server radius`
(config-sonet)	SONET/SDH Configuration Mode	Use the **controller sonet** command in global configuration mode.	`(config)# controller sonet 0/2/0/2` `(config-sonet)#`

Table 2-1 CLI Prompts and Modes (continued)

Prompt	Mode Section	Access Method	Example
(config-sonet-path)	SONET/SDH Path Configuration Mode	Use the **path** command in SONET/SDH configuration mode.	`(config-sonet)# path` `(config-sonet-path)#`
(config-static)	Router Configuration Mode	Use the **static** command in global configuration mode.	`(config)# router static` `(config-static)# vrf new1`

(config-static-vrf-af)	VPNv4 Address Family Group Command Mode	Use the **static** command in global configuration mode, and then use the **vrf** and **address family** commands.	`(config)# router static`
			`(config-static)# vrf new1`
			`(config-static-vrf)# address-family ipv4 unicast`
			`(config-static-vrf-afi)#`

(config-subif)	Subinterface Configuration Mode	In EXEC mode, use the **configure terminal** command to enter global configuration mode, and then use the **interface TenGig** command.	`# configure terminal`
			`router(config)# interface TenGigE 0/2/0/4.1`
			`(config-subif)#`

(config-tg)	Task Group Configuration Mode	Use the **taskgroup** command in global configuration mode.	`(config)# taskgroup alpha` `(config-tg)#`
(config-TPL)	Template Configuration Mode	Use the **template** command in global configuration mode.	`(config)# template pre-pos` `(config-TPL)#`
(config-transport)	Transport Configuration Mode	Use the **crypto ipsec transport** command in global configuration mode.	`(config)# crypto ipsec transport` `(config-transport)#`
(config-trustpt)	Trustpoint Configuration Mode	Run the **crypto ca trustpoint myca** command in global configuration mode.	`(config)# crypto ca trustpoint myca` `(config-trustp)#`
(config-ug)	User Group Configuration Mode	Use the **usergroup** command in global configuration mode.	`(config)# usergroup alpha` `(config-ug)# inherit`
(config-un)	Username Configuration Mode	Use the **username** command in global configuration mode.	`(config)# username enzo` `(config-un)# group ferrari`
(config-vrrp)	Router VRRP Configuration Mode	Use the **router vrrp** command in global configuration mode.	`(config)# router vrrp` `(config-vrrp)#`

Table 2-1 CLI Prompts and Modes (continued)

Prompt	Mode Section	Access Method	Example

(config-vrrp-if)	VRRP Interface Configuration Mode	In router VRRP configuration mode, use the **interface TenGigE** command.	`(config)# router vrrp`
			`(config-vrrp)# (config)#`
			`interface TenGigE 0/3/0/0`
			`(config-vrrp-if)#`

(isakmp-group)	ISAKMP Group Configuration Mode	In the global configuration mode, use **crypto isakmp client**.	`(config)# crypto isakmp client configuration group cisco` `(isakmp-group)# key cisco`