Cisco IOS XE IP Routing: RIP Configuration Guide

Release 2

Americas 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: 408 527-0883

Cisco IOS XE IP Routing: RIP Configuration Guide

About Cisco IOS XE Software Documentation

Last Updated: December 1, 2009

This document describes the objectives, audience, conventions, and organization used in Cisco IOS XE software documentation. Also included are resources for obtaining technical assistance, additional documentation, and other information from Cisco. This document is organized into the following sections:

Documentation Objectives

Cisco IOS XE documentation describe the tasks and commands available to configure and maintain Cisco networking devices.

Audience

The Cisco IOS XE documentation set is intended for users who configure and maintain Cisco networking devices (such as routers and switches) but who may not be familiar with the configuration and maintenance tasks, the relationship among tasks, or the Cisco IOS commands necessary to perform particular tasks. The Cisco IOS XE documentation set is also intended for those users experienced with Cisco IOS XE software who need to know about new features, new configuration options, and new software characteristics in the current Cisco IOS XE release.

Documentation Conventions

In Cisco IOS XE documentation, the term *router* may be used to refer to various Cisco products; for example, routers, access servers, and switches. These and other networking devices that support Cisco IOS XE software are shown interchangeably in examples and are used only for illustrative purposes. An example that shows one product does not necessarily mean that other products are not supported.

This section contains the following topics:

Typographic Conventions

Cisco IOS XE documentation uses the following typographic conventions:

Convention	Description
^ or Ctrl	Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination **^D** or **Ctrl-D** means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)
string	A string is a nonquoted set of characters shown in italics. For example, when setting a Simple Network Management Protocol (SNMP) community string to *public*, do not use quotation marks around the string; otherwise, the string will include the quotation marks.

Command Syntax Conventions

Cisco IOS XE documentation uses the following command syntax conventions:

Convention	Description
bold	Bold text indicates commands and keywords that you enter as shown.
italic	Italic text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional keyword or argument.
...	An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.
|	A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.
[x | y]	Square brackets enclosing keywords or arguments separated by a pipe indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a pipe indicate a required choice.
[x {y | z}]	Braces and a pipe within square brackets indicate a required choice within an optional element.

Software Conventions

Cisco IOS XE software uses the following conventions:

Convention	Description
`Courier font`	Courier font is used for information that is displayed on a PC or terminal screen.
`Bold Courier font`	Bold Courier font indicates text that the user must enter.
< >	Angle brackets enclose text that is not displayed, such as a password. Angle brackets also are used in contexts in which the italic font style is not supported; for example, ASCII text.
!	An exclamation point at the beginning of a line indicates that the text that follows is a comment, not a line of code. An exclamation point is also displayed by the Cisco IOS XE software for certain processes.
[ ]	Square brackets enclose default responses to system prompts.

Reader Alert Conventions

Cisco IOS XE documentation uses the following conventions for reader alerts:

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

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

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Documentation Organization

This section describes the Cisco IOS XE documentation set, how it is organized, and how to access it on Cisco.com. Listed are configuration guides, command references, and supplementary references and resources that comprise the documentation set.

Cisco IOS XE Documentation Set

The Cisco IOS XE documentation set consists of the following:

- Release notes and caveats provide information about platform, technology, and feature support for a release and describe severity 1 (catastrophic), severity 2 (severe), and severity 3 (moderate) defects in released Cisco IOS XE software. Review release notes before other documents to learn whether updates have been made to a feature.
- Sets of configuration guides and command references organized by technology and published for each standard Cisco IOS XE release.
  - Configuration guides—Compilations of documents that provide conceptual and task-oriented descriptions of Cisco IOS XE features.
  - Command references—Alphabetical compilations of command pages that provide detailed information about the commands used in the Cisco IOS XE features and the processes that comprise the related configuration guides. For each technology, there is a single command reference that covers all Cisco IOS XE releases and that is updated at each standard release.
- Command reference book for **debug** commands.
- Lists of all the commands in a specific release and all commands that are new, modified, removed, or replaced in the release.
- Reference book for system messages for all Cisco IOS XE releases.

Cisco IOS XE Documentation on Cisco.com

The following sections describe the documentation organization and how to access various document types.

Use Cisco Feature Navigator to find information about Cisco IOS XE software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

New Features List

The New Features List for each release provides a list of all features in the release with hyperlinks to the feature guides in which they are documented.

Configuration Guides

Configuration guides are provided by technology and release and comprise a set of individual feature guides relevant to the release and technology.

Command References

Command reference books describe Cisco IOS XE commands that are supported in many different software releases and on many different platforms. The books are organized by technology. For information about all Cisco IOS XE commands, use the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or the *Cisco IOS Master Command List, All Releases*, at http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html.

Cisco IOS XE Supplementary Documents and Resources

Supplementary documents and resources are listed in Table 2 on page x.

Configuration Guides, Command References, and Supplementary Resources

Table 1 lists, in alphabetical order, Cisco IOS XE software configuration guides and command references, including brief descriptions of the contents of the documents. The command references contain commands for both Cisco IOS software and Cisco IOS XE software, for all releases. The command references support many different software releases and platforms. Your Cisco IOS XE software release or platform may not support all these technologies.

Table 2 lists documents and resources that supplement the Cisco IOS XE software configuration guides and command references. These supplementary resources include release notes and caveats; master command lists; new, modified, removed, and replaced command lists; system messages; and the debug command reference.

For additional information about configuring and operating specific networking devices, and to access Cisco IOS documentation, go to the Product/Technologies Support area of Cisco.com at the following location:

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

Table 1 Cisco IOS XE Configuration Guides and Command References

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Software Configuration Guide*	Configuration and troubleshooting of SPA interface processors (SIPs) and shared port adapters (SPAs) that are supported on the Cisco ASR 1000 Series Router.
• *Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide*	Overview of software functionality that is specific to the Cisco ASR 1000 Series Aggregation Services Routers.
• *Cisco IOS XE Access Node Control Protocol Configuration Guide* • *Cisco IOS Access Node Control Protocol Command Reference*	Communication protocol between digital subscriber line access multiplexers (DSLAMs) and a broadband remote access server (BRAS).
• *Cisco IOS XE Asynchronous Transfer Mode Configuration Guide* • *Cisco IOS Asynchronous Transfer Mode Command Reference*	LAN ATM, multiprotocol over ATM (MPoA), and WAN ATM.
• *Cisco IOS XE Broadband Access Aggregation and DSL Configuration Guide* • *Cisco IOS Broadband Access Aggregation and DSL Command Reference*	PPP over Ethernet (PPPoE).
• *Cisco IOS XE Carrier Ethernet Configuration Guide* • *Cisco IOS Carrier Ethernet Command Reference*	IEEE 802.3ad Link Bundling; Link Aggregation Control Protocol (LACP) support for Ethernet and Gigabit Ethernet links and EtherChannel bundles; LACP support for stateful switchover (SSO), in service software upgrade (ISSU), Cisco nonstop forwarding (NSF), and nonstop routing (NSR) on Gigabit EtherChannel bundles; and IEEE 802.3ad Link Aggregation MIB.
• *Cisco IOS XE Configuration Fundamentals Configuration Guide* • *Cisco IOS Configuration Fundamentals Command Reference*	Autoinstall, Setup, Cisco IOS command-line interface (CLI), Cisco IOS file system (IFS), Cisco IOS web browser user interface (UI), basic file transfer services, and file management.

Table 1 Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *Cisco IOS XE DECnet Configuration Guide* • *Cisco IOS DECnet Command Reference*	DECnet protocol.
• *Cisco IOS XE Dial Technologies Configuration Guide* • *Cisco IOS Dial Technologies Command Reference*	Asynchronous communications, dial backup, dialer technology, Multilink PPP (MLP), PPP, and virtual private dialup network (VPDN).
• *Cisco IOS XE High Availability Configuration Guide* • *Cisco IOS High Availability Command Reference*	A variety of high availability (HA) features and technologies that are available for different network segments (from enterprise access to service provider core) to facilitate creation of end-to-end highly available networks. Cisco IOS HA features and technologies can be categorized in three key areas: system-level resiliency, network-level resiliency, and embedded management for resiliency.
• *Cisco IOS XE Intelligent Services Gateway Configuration Guide* • *Cisco IOS Intelligent Services Gateway Command Reference*	Subscriber identification, service and policy determination, session creation, session policy enforcement, session life-cycle management, accounting for access and service usage, and session state monitoring.
• *Cisco IOS XE Interface and Hardware Component Configuration Guide* • *Cisco IOS Interface and Hardware Component Command Reference*	LAN interfaces, logical interfaces, serial interfaces, virtual interfaces, and interface configuration.
• *Cisco IOS XE IP Addressing Services Configuration Guide* • *Cisco IOS IP Addressing Services Command Reference*	IP addressing, Address Resolution Protocol (ARP), Network Address Translation (NAT), Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and Next Hop Address Resolution Protocol (NHRP).
• *Cisco IOS XE IP Application Services Configuration Guide* • *Cisco IOS IP Application Services Command Reference*	Enhanced Object Tracking (EOT), Gateway Load Balancing Protocol (GLBP), Hot Standby Router Protocol (HSRP), IP Services, TCP, Web Cache Communication Protocol (WCCP), User Datagram Protocol (UDP), and Virtual Router Redundancy Protocol (VRRP).
• *Cisco IOS XE IP Multicast Configuration Guide* • *Cisco IOS IP Multicast Command Reference*	Protocol Independent Multicast (PIM) sparse mode (PIM-SM), bidirectional PIM (bidir-PIM), Source Specific Multicast (SSM), Multicast Source Discovery Protocol (MSDP), Internet Group Management Protocol (IGMP), and Multicast VPN (MVPN).
• *Cisco IOS XE IP Routing: BFD Configuration Guide*	Bidirectional forwarding detection (BFD).
• *Cisco IOS XE IP Routing: BGP Configuration Guide* • *Cisco IOS IP Routing: BGP Command Reference*	Border Gateway Protocol (BGP), multiprotocol BGP, multiprotocol BGP extensions for IP multicast.
• *Cisco IOS XE IP Routing: EIGRP Configuration Guide* • *Cisco IOS IP Routing: EIGRP Command Reference*	Enhanced Interior Gateway Routing Protocol (EIGRP).
• *Cisco IOS XE IP Routing: ISIS Configuration Guide* • *Cisco IOS IP Routing: ISIS Command Reference*	Intermediate System-to-Intermediate System (IS-IS).

Table 1 Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *Cisco IOS XE IP Routing: ODR Configuration Guide* • *Cisco IOS IP Routing: ODR Command Reference*	On-Demand Routing (ODR).
• *Cisco IOS XE IP Routing: OSPF Configuration Guide* • *Cisco IOS IP Routing: OSPF Command Reference*	Open Shortest Path First (OSPF).
• *Cisco IOS XE IP Routing: Protocol-Independent Configuration Guide* • *Cisco IOS IP Routing: Protocol-Independent Command Reference*	IP routing protocol-independent features and commands. Generic policy-based routing (PBR) features and commands are included.
• *Cisco IOS XE IP Routing: RIP Configuration Guide* • *Cisco IOS IP Routing: RIP Command Reference*	Routing Information Protocol (RIP).
• *Cisco IOS XE IP SLAs Configuration Guide* • *Cisco IOS IP SLAs Command Reference*	Cisco IOS IP Service Level Agreements (IP SLAs).
• *Cisco IOS XE IP Switching Configuration Guide* • *Cisco IOS IP Switching Command Reference*	Cisco Express Forwarding.
• *Cisco IOS XE IPv6 Configuration Guide* • *Cisco IOS IPv6 Command Reference*	For a list of IPv6 features, protocols, and technologies, go to the IPv6 “Start Here” document at the following URL: http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-roadmap_xe.html
• *Cisco IOS XE ISO CLNS Configuration Guide* • *Cisco IOS ISO CLNS Command Reference*	ISO Connectionless Network Service (CLNS).
• *Cisco IOS XE LAN Switching Configuration Guide* • *Cisco IOS LAN Switching Command Reference*	VLANs and multilayer switching (MLS).
• *Cisco IOS XE Multiprotocol Label Switching Configuration Guide* • *Cisco IOS Multiprotocol Label Switching Command Reference*	MPLS Label Distribution Protocol (LDP), MPLS Layer 2 VPNs, MPLS Layer 3 VPNs, MPLS Traffic Engineering (TE), and MPLS Embedded Management (EM) and MIBs.
• *Cisco IOS XE NetFlow Configuration Guide* • *Cisco IOS NetFlow Command Reference*	Network traffic data analysis, aggregation caches, and export features.
• *Cisco IOS XE Network Management Configuration Guide* • *Cisco IOS Network Management Command Reference*	Basic system management, system monitoring and logging, Cisco IOS Scripting with Tool Control Language (Tcl), Cisco networking services (CNS), Embedded Event Manager (EEM), Embedded Syslog Manager (ESM), HTTP, Remote Monitoring (RMON), and SNMP.
• *Cisco IOS XE Novell IPX Configuration Guide* • *Cisco IOS Novell IPX Command Reference*	Novell Internetwork Packet Exchange (IPX) protocol.

Table 1 Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *Cisco IOS XE Quality of Service Solutions Configuration Guide* • *Cisco IOS Quality of Service Solutions Command Reference*	Class-based weighted fair queueing (CBWFQ), low latency queueing (LLQ), Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC), Network-Based Application Recognition (NBAR), priority queueing, Multilink PPP (MLP) for QoS, header compression, Resource Reservation Protocol (RSVP), weighted fair queueing (WFQ), and weighted random early detection (WRED).
• *Cisco IOS Security Command Reference*	Access control lists (ACLs); authentication, authorization, and accounting (AAA); firewalls; IP security and encryption; neighbor router authentication; network access security; public key infrastructure (PKI); RADIUS; and TACACS+.
• *Cisco IOS XE Security Configuration Guide: Secure Connectivity*	Internet Key Exchange (IKE) for IPsec VPNs; security for VPNs with IPsec; VPN availability features (reverse route injection, IPsec preferred peer, and real-time resolution for the IPsec tunnel peer); IPsec data plane features; IPsec management plane features; Public Key Infrastructure (PKI); Dynamic Multipoint VPN (DMVPN); Easy VPN; and Cisco Group Encrypted Transport VPN (GET VPN).
• *Cisco IOS XE Security Configuration Guide: Securing the Data Plane*	Access Control Lists (ACLs); Firewalls: Context-Based Access Control (CBAC) and Zone-Based Firewall; Cisco IOS Intrusion Prevention System (IPS); Flexible Packet Matching; Unicast Reverse Path Forwarding (uRPF); Threat Information Distribution Protocol (TIDP) and TMS.
• *Cisco IOS XE Security Configuration Guide: Securing User Services*	AAA (includes Network Admission Control [NAC]); Security Server Protocols (RADIUS and TACACS+); Secure Shell (SSH); Secure Access for Networking Devices (includes Autosecure and Role-Based CLI access); Lawful Intercept.
• *Cisco IOS XE Service Advertisement Framework Configuration Guide* • *Cisco IOS Service Advertisement Framework Command Reference*	Cisco Service Advertisement Framework.
• *Cisco IOS XE VPDN Configuration Guide* • *Cisco IOS VPDN Command Reference*	Multihop by Dialed Number Identification Service (DNIS), timer and retry enhancements for L2TP and Layer 2 Forwarding (L2F), RADIUS Attribute 82 (tunnel assignment ID), shell-based authentication of VPDN users, and tunnel authentication via RADIUS on tunnel terminator.
• *Cisco IOS XE Wide-Area Networking Configuration Guide* • *Cisco IOS Wide-Area Networking Command Reference*	Frame Relay; L2VPN Pseudowire Redundancy; and Media-Independent PPP and Multilink PPP.

Table 1 Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *Cisco Unified Border Element (Enterprise) Configuration Guide* • *Cisco IOS Voice Command Reference*	The Cisco Unified Border Element (Enterprise) on the Cisco ASR 1000 brings a scalable option for enterprise customers. Running as a process on the Cisco ASR 1000 and utilizing the high-speed RTP packet processing path, the Cisco Unified Border Element (Enterprise) is used as an IP-to-IP gateway by enterprises and commercial customers to interconnect SIP and H.323 voice and video networks. The Cisco UBE (Enterprise) provides a network-to-network demarcation interface for signaling interworking, media interworking, address and port translations, billing, security, quality of service (QoS), and bandwidth management.
• *Cisco Unified Border Element (SP Edition) Configuration Guide: Distributed Model* • *Cisco Unified Border Element (SP Edition) Command Reference: Distributed Model*	The Cisco Unified Border Element (SP Edition) is a session border controller (SBC) that is VoIP-enabled and deployed at the edge of networks. For Cisco IOS XE Release 2.3 and earlier releases, Cisco Unified Border Element (SP Edition) is supported only in the distributed mode. Operating in the distributed mode, the SBC is a toolkit of functions that can be used to deploy and manage VoIP services, such as signaling interworking, network hiding, security, and quality of service.
• *Cisco Unified Border Element (SP Edition) Configuration Guide: Unified Model* • *Cisco Unified Border Element (SP Edition) Command Reference: Unified Model*	The Cisco Unified Border Element (SP Edition) is a highly scalable, carrier-grade session border controller (SBC) that is designed for service providers and that is generally deployed at the border of the enterprise or SP networks to enable the easy deployment and management of VoIP services. Cisco Unified Border Element (SP Edition) is integrated into Cisco routing platforms and can use a large number of router functions to provide a very feature-rich and intelligent SBC application. Formerly known as Integrated Session Border Controller, Cisco Unified Border Element (SP Edition) provides a network-to-network demarcation interface for signaling interworking, media interworking, address and port translations, billing, security, quality of service, call admission control, and bandwidth management. For Cisco IOS XE Release 2.4 and later releases, Cisco Unified Border Element (SP Edition) can operate in two modes or deployment models: unified and distributed. The configuration guide documents the features in the unified mode.

Table 2 lists documents and resources that supplement the Cisco IOS XE software configuration guides and command references.

Table 2 Cisco IOS XE Software Supplementary Documents and Resources

Document Title or Resource	Description
Cisco IOS Master Command List, All Releases	Alphabetical list of all the commands documented in all Cisco IOS XE software releases.
Cisco IOS Debug Command Reference	Alphabetical list of **debug** commands including brief descriptions of use, command syntax, and usage guidelines.
Cisco IOS XE system messages	List of Cisco IOS XE system messages and descriptions. System messages may indicate problems with your system, may be informational only, or may help diagnose problems with communications lines, internal hardware, or the system software.
Release notes and caveats	Information about new and changed features, system requirements, and other useful information about specific software releases; information about defects in specific Cisco IOS XE software releases.
MIBs	Files used for network monitoring. To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator at the following URL: http://www.cisco.com/go/mibs
RFCs	Standards documents maintained by the Internet Engineering Task Force (IETF) that Cisco IOS XE documentation references where applicable. The full text of referenced RFCs may be obtained at the following URL: http://www.rfc-editor.org/

Additional Resources and Documentation Feedback

What's New in Cisco Product Documentation is updated monthly and describes all new and revised Cisco technical documentation. The *What's New in Cisco Product Documentation* publication also provides information about obtaining the following resources:

- Technical documentation
- Cisco product security overview
- Product alerts and field notices
- Technical assistance

Cisco IOS XE software technical documentation includes embedded feedback forms where you can rate documents and provide suggestions for improvement. Your feedback helps us improve our documentation.

Using the Command-Line Interface in Cisco IOS XE Software

Last Updated: December 1, 2009

This document provides basic information about the command-line interface (CLI) in Cisco IOS XE software and how you can use some of the CLI features. This document contains the following sections:

For more information about using the CLI, see "Part 1: Using the Cisco IOS Command-Line Interface (CLI)" of the *Cisco IOS XE Configuration Fundamentals Configuration Guide*.

For information about the software documentation set, see the "About Cisco IOS XE Software Documentation" document.

Initially Configuring a Device

Initially configuring a device varies by platform. For information about performing an initial configuration, see the hardware installation documentation that is provided with the original packaging of the product or go to the Product Support area of Cisco.com at http://www.cisco.com/go/techdocs.

After you have performed the initial configuration and connected the device to your network, you can configure the device by using the console port or a remote access method, such as Telnet or Secure Shell (SSH), to access the CLI or by using the configuration method provided on the device, such as Security Device Manager.

Changing the Default Settings for a Console or AUX Port

There are only two settings that you can change on a console port or an AUX port:

- Change the port speed with the **config-register 0x** command. Changing the port speed is not recommended. The well-known default speed is 9600.
- Change the behavior of the port; for example, by adding a password or changing the timeout value.

Note The AUX port on the Route Processor (RP) installed in a Cisco ASR 1000 series router does not serve any useful customer purpose and should be accessed only under the advisement of a customer support representative.

Using the CLI

This section describes the following topics:

Understanding Command Modes

The CLI command mode structure is hierarchical, and each mode supports a set of specific commands. This section describes the most common of the many modes that exist.

Table 1 lists common command modes with associated CLI prompts, access and exit methods, and a brief description of how each mode is used.

Table 1 CLI Command Modes

Command Mode	Access Method	Prompt	Exit Method	Mode Usage
User EXEC	Log in.	`Router>`	Issue the **logout** or **exit** command.	• Change terminal settings. • Perform basic tests. • Display device status.
Privileged EXEC	From user EXEC mode, issue the **enable** command.	`Router#`	Issue the **disable** command or the **exit** command to return to user EXEC mode.	• Issue **show** and **debug** commands. • Copy images to the device. • Reload the device. • Manage device configuration files. • Manage device file systems.
Global configuration	From privileged EXEC mode, issue the **configure terminal** command.	`Router(config)#`	Issue the **exit** command or the **end** command to return to privileged EXEC mode.	Configure the device.
Interface configuration	From global configuration mode, issue the **interface** command.	`Router(config-if)#`	Issue the **exit** command to return to global configuration mode or the **end** command to return to privileged EXEC mode.	Configure individual interfaces.
Line configuration	From global configuration mode, issue the **line vty** or **line console** command.	`Router(config-line)#`	Issue the **exit** command to return to global configuration mode or the **end** command to return to privileged EXEC mode.	Configure individual terminal lines.

Table 1 CLI Command Modes (continued)

Command Mode	Access Method	Prompt	Exit Method	Mode Usage
ROM monitor	From privileged EXEC mode, issue the **reload** command. Press the **Break** key during the first 60 seconds while the system is booting.	`rommon # >` The # symbol represents the line number and increments at each prompt.	Issue the **continue** command.	• Run as the default operating mode when a valid image cannot be loaded. • Access the fall-back procedure for loading an image when the device lacks a valid image and cannot be booted. • Perform password recovery when a CTRL-Break sequence is issued within 60 seconds of a power-on or reload event.
Diagnostic	The router boots or enters diagnostic mode in the following scenarios. When a Cisco IOS XE process or processes fail, in most scenarios the router will reload. • A user-configured access policy was configured using the **transport-map** command, which directed the user into diagnostic mode. • The router was accessed using an RP auxiliary port. • A break signal (**Ctrl-C**, **Ctrl-Shift-6**, or the **send break** command) was entered, and the router was configured to enter diagnostic mode when the break signal was received.	`Router(diag)#`	If a Cisco IOS XE process failure is the reason for entering diagnostic mode, the failure must be resolved and the router must be rebooted to exit diagnostic mode. If the router is in diagnostic mode because of a transport-map configuration, access the router through another port or use a method that is configured to connect to the Cisco IOS XE CLI. If the RP auxiliary port was used to access the router, use another port for access. Accessing the router through the auxiliary port is not useful for customer purposes.	• Inspect various states on the router, including the Cisco IOS XE state. • Replace or roll back the configuration. • Provide methods of restarting the Cisco IOS XE software or other processes. • Reboot hardware, such as the entire router, an RP, an ESP, a SIP, a SPA, or other hardware components. • Transfer files into or off of the router using remote access methods such as FTP, TFTP, and SCP.

EXEC commands are not saved when the software reboots. Commands that you issue in a configuration mode can be saved to the startup configuration. If you save the running configuration to the startup configuration, these commands will execute when the software is rebooted. Global configuration mode is the highest level of configuration mode. From global configuration mode, you can enter a variety of other configuration modes, including protocol-specific modes.

ROM monitor mode is a separate mode that is used when the software cannot load properly. If a valid software image is not found when the software boots or if the configuration file is corrupted at startup, the software might enter ROM monitor mode. Use the question symbol (?) to view the commands that you can use while the device is in ROM monitor mode.

```
rommon 1 > ?
alias               set and display aliases command
boot                boot up an external process
confreg             configuration register utility
cont                continue executing a downloaded image
context             display the context of a loaded image
cookie              display contents of cookie PROM in hex
.
.
.
rommon 2 >
```

The following example shows how the command prompt changes to indicate a different command mode:

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet 1/1
Router(config-if)# ethernet
Router(config-line)# exit
Router(config)# end
Router#
```

Note A keyboard alternative to the **end** command is Ctrl-Z.

Using the Interactive Help Feature

The CLI includes an interactive Help feature. Table 2 describes how to use the Help feature.

Table 2 CLI Interactive Help Commands

Command	Purpose
help	Provides a brief description of the Help feature in any command mode.
?	Lists all commands available for a particular command mode.
*partial command***?**	Provides a list of commands that begin with the character string (no space between the command and the question mark).
partial command<**Tab**>	Completes a partial command name (no space between the command and <Tab>).
command **?**	Lists the keywords, arguments, or both associated with the command (space between the command and the question mark).
command keyword **?**	Lists the arguments that are associated with the keyword (space between the keyword and the question mark).

The following examples show how to use the help commands:

help

```
Router> help

Help may be requested at any point in a command by entering a question mark '?'. If nothing
matches, the help list will be empty and you must backup until entering a '?' shows the
available options.

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument (e.g. 'show ?')
and describes each possible argument.

2. Partial help is provided when an abbreviated argument is entered and you want to know
what arguments match the input (e.g. 'show pr?'.)
```

?

```
Router# ?
Exec commands:
  access-enable        Create a temporary access-List entry
  access-profile       Apply user-profile to interface
  access-template      Create a temporary access-List entry
  alps                 ALPS exec commands
  archive              manage archive files
<snip>
```

***partial command*?**

```
Router(config)# zo?
zone  zone-pair
```

***partial command*<Tab>**

```
Router(config)# we<Tab> webvpn
```

***command* ?**

```
Router(config-if)# pppoe ?
  enable        Enable pppoe
  max-sessions  Maximum PPPOE sessions
```

***command keyword* ?**

```
Router(config-if)# pppoe enable ?
  group  attach a BBA group
  <cr>
```

Understanding Command Syntax

Command syntax is the format in which a command should be entered in the CLI. Commands include the name of the command, keywords, and arguments. Keywords are alphanumeric strings that are used literally. Arguments are placeholders for values that a user must supply. Keywords and arguments may be required or optional.

Specific conventions convey information about syntax and command elements. Table 3 describes these conventions.

Table 3 CLI Syntax Conventions

Symbol/Text	Function	Notes
< > (angle brackets)	Indicate that the option is an argument.	Sometimes arguments are displayed without angle brackets.
A.B.C.D.	Indicates that you must enter a dotted decimal IP address.	Angle brackets (< >) are not always used to indicate that an IP address is an argument.
WORD (all capital letters)	Indicates that you must enter one word.	Angle brackets (< >) are not always used to indicate that a WORD is an argument.
LINE (all capital letters)	Indicates that you must enter more than one word.	Angle brackets (< >) are not always used to indicate that a LINE is an argument.
<cr> (carriage return)	Indicates the end of the list of available keywords and arguments, and also indicates when keywords and arguments are optional. When <cr> is the only option, you have reached the end of the branch or the end of the command if the command has only one branch.	—

The following examples show syntax conventions:

```
Router(config)# ethernet cfm domain ?
  WORD  domain name

Router(config)# ethernet cfm domain dname ?
  level

Router(config)# ethernet cfm domain dname level ?
  <0-7>  maintenance level number

Router(config)# ethernet cfm domain dname level 7 ?
  <cr>

Router(config)# snmp-server file-transfer access-group 10 ?
  protocol  protocol options
  <cr>

Router(config)# logging host ?
  Hostname or A.B.C.D  IP address of the syslog server
  ipv6                 Configure IPv6 syslog server
```

Understanding Enable and Enable Secret Passwords

Some privileged EXEC commands are used for actions that impact the system, and it is recommended that you set a password for these commands to prevent unauthorized use. Two types of passwords, enable (not encrypted) and enable secret (encrypted), can be set. The following commands set these passwords and are issued in global configuration mode:

- **enable** *password*
- **enable secret** *password*

Using an enable secret password is recommended because it is encrypted and more secure than the enable password. When you use an enable secret password, text is encrypted (unreadable) before it is written to the config.text file. When you use an enable password, the text is written as entered (readable) to the config.text file.

Each type of password is case sensitive, can contain from 1 to 25 uppercase and lowercase alphanumeric characters, and can start with a number. Spaces are also valid password characters; for example, "two words" is a valid password. Leading spaces are ignored, but trailing spaces are recognized.

Note Both password commands have numeric keywords that are single integer values. If you choose a number for the first character of your password followed by a space, the system will read the number as if it were the numeric keyword and not as part of your password.

When both passwords are set, the enable secret password takes precedence over the enable password.

To remove a password, use the **no** form of the commands: **no enable** *password* or **no enable secret** *password*.

For more information about password recovery procedures for Cisco products, see http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00801746e6.shtml.

Using the Command History Feature

The command history feature saves the commands that you enter during a session in a command history buffer. The default number of commands saved is 10, but the number is configurable within the range of 0 to 256. This command history feature is particularly useful for recalling long or complex commands.

To change the number of commands saved in the history buffer for a terminal session, issue the **terminal history size** command:

```
Router# terminal history size num
```

A command history buffer is also available in line configuration mode with the same default and configuration options. To set the command history buffer size for a terminal session in line configuration mode, issue the **history** command:

```
Router(config-line)# history [size num]
```

To recall commands from the history buffer, use the following methods:

- Press Ctrl-P or the Up Arrow key—Recalls commands beginning with the most recent command. Repeat the key sequence to recall successively older commands.
- Press Ctrl-N or the Down Arrow key—Recalls the most recent commands in the history buffer after they have been recalled using Ctrl-P or the Up Arrow key. Repeat the key sequence to recall successively more recent commands.

Note The arrow keys function only on ANSI-compatible terminals such as the VT100.

- Issue the **show history** command in user EXEC or privileged EXEC mode—Lists the most recent commands that you entered. The number of commands that are displayed is determined by the setting of the **terminal history size** and **history** commands.

  The command history feature is enabled by default. To disable this feature for a terminal session, issue the **terminal no history** command in user EXEC or privileged EXEC mode or the **no history** command in line configuration mode.

Abbreviating Commands

Typing a complete command name is not always required for the command to execute. The CLI recognizes an abbreviated command when the abbreviation contains enough characters to uniquely identify the command. For example, the **show version** command can be abbreviated as **sh ver**. It cannot be abbreviated as **s ver** because **s** could mean **show**, **set**, or **systat**. The **sh v** abbreviation also is not valid because the **show** command has **vrrp** as a keyword in addition to **version**.

Using Aliases for CLI Commands

To save time and the repetition of entering the same command multiple times, you can use a command alias. An alias can be configured to do anything that can be done at the command line, but an alias cannot move between modes, type in passwords, or perform any interactive functions.

Table 4 shows the default command aliases.

Table 4 Default Command Aliases

Command Alias	Original Command
h	help
lo	logout
p	ping
s	show
u or **un**	undebug
w	where

To create a command alias, issue the **alias** command in global configuration mode. The syntax of the command is **alias** *mode command-alias original-command*. Following are some examples:

- Router(config)# **alias exec prt partition**—privileged EXEC mode
- Router(config)# **alias configure sb source-bridge**—global configuration mode
- Router(config)# **alias interface rl rate-limit**—interface configuration mode

To view both default and user-created aliases, issue the **show alias** command.

For more information about the **alias** command, see http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_book.html.

Using the no and default Forms of Commands

Most configuration commands have a **no** form that is used to reset a command to its default value or disable a feature or function. For example, the **ip routing** command is enabled by default. To disable this command, you would issue the **no ip routing** command. To re-enable IP routing, you would issue the **ip routing** command.

Configuration commands may also have a **default** form, which returns the command settings to their default values. For commands that are disabled by default, using the **default** form has the same effect as using the **no** form of the command. For commands that are enabled by default and have default settings, the **default** form enables the command and returns the settings to their default values.

The **no** form is documented in the command pages of command references. The **default** form is generally documented in the command pages only when the **default** form performs a different function than the plain and **no** forms of the command. To see what **default** commands are available on your system, enter **default ?** in the appropriate command mode.

Using the debug Command

A **debug** command produces extensive output that helps you troubleshoot problems in your network. These commands are available for many features and functions within Cisco IOS XE software. Some **debug** commands are **debug all**, **debug aaa accounting**, and **debug mpls packets**. To use **debug** commands during a Telnet session with a device, you must first enter the **terminal monitor** command. To turn off debugging completely, you must enter the **undebug all** command.

For more information about **debug** commands, see the *Cisco IOS Debug Command Reference* at http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html.

Caution Debugging is a high priority and high CPU utilization process that can render your device unusable. Use **debug** commands only to troubleshoot specific problems. The best times to run debugging are during periods of low network traffic and when few users are interacting with the network. Debugging during these periods decreases the likelihood that the **debug** command processing overhead will affect network performance or user access or response times.

Filtering Output Using Output Modifiers

Many commands produce lengthy output that may use several screens to display. You can use output modifiers to filter this output to show only the information that you want to see.

The following three output modifiers are available:

- **begin** *regular-expression*—Displays the first line in which a match of the regular expression is found and all lines that follow.
- **include** *regular-expression*—Displays all lines in which a match of the regular expression is found.
- **exclude** *regular-expression*—Displays all lines except those in which a match of the regular expression is found.

To use one of these output modifiers, type the command followed by the pipe symbol (|), the modifier, and the regular expression that you want to search for or filter. A regular expression is a case-sensitive alphanumeric pattern. It can be a single character or number, a phrase, or a more complex string.

The following example illustrates how to filter output of the **show interface** command to display only lines that include the expression “protocol.”

```
Router# show interface | include protocol

FastEthernet0/0 is up, line protocol is up
Serial4/0 is up, line protocol is up
Serial4/1 is up, line protocol is up
Serial4/2 is administratively down, line protocol is down
Serial4/3 is administratively down, line protocol is down
```

Understanding CLI Error Messages

You may encounter some error messages while using the CLI. Table 5 shows the common CLI error messages.

Table 5 Common CLI Error Messages

Error Message	Meaning	How to Get Help
% Ambiguous command: “show con”	You did not enter enough characters for the command to be recognized.	Reenter the command followed by a space and a question mark (?). The keywords that you are allowed to enter for the command appear.
% Incomplete command.	You did not enter all the keywords or values required by the command.	Reenter the command followed by a space and a question mark (?). The keywords that you are allowed to enter for the command appear.
% Invalid input detected at “^” marker.	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (?) to display all the commands that are available in this command mode. The keywords that you are allowed to enter for the command appear.

For more system error messages, see the *System Messages for Cisco IOS XE* document.

Saving Changes to a Configuration

To save changes that you made to the configuration of a device, you must issue the **copy running-config startup-config** command or the **copy system:running-config nvram:startup-config** command. When you issue these commands, the configuration changes that you made are saved to the startup configuration and saved when the software reloads or power to the device is turned off or interrupted. The following example shows the syntax of the **copy running-config startup-config** command:

```
Router# copy running-config startup-config
Destination filename [startup-config]?
```

You press Enter to accept the startup-config filename (the default), or type a new filename and then press Enter to accept that name. The following output is displayed indicating that the configuration was saved:

```
Building configuration...
[OK]
Router#
```

On most platforms, the configuration is saved to NVRAM. On platforms with a Class A flash file system, the configuration is saved to the location specified by the CONFIG_FILE environment variable. The CONFIG_FILE variable defaults to NVRAM.

Additional Information

- "Part 1: Using the Cisco IOS Command-Line Interface (CLI)" of the *Cisco IOS XE Configuration Fundamentals Configuration Guide*

  http://www.cisco.com/en/US/docs/ios/ios_xe/fundamentals/configuration/guide/2_xe/cf_xe_book.html

  or

  "Using Cisco IOS XE Software" chapter of the *Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide*

  http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/chassis/Using_CLI.html
- Cisco Product Support Resources

  http://www.cisco.com/go/techdocs
- Support area on Cisco.com (also search for documentation by task or product)

  http://www.cisco.com/en/US/support/index.html
- Software Download Center (downloads; tools; licensing, registration, advisory, and general information) (requires Cisco.com user ID and password)

  http://www.cisco.com/kobayashi/sw-center/
- Error Message Decoder, a tool to help you research and resolve error messages for Cisco IOS XE software

  http://www.cisco.com/pcgi-bin/Support/Errordecoder/index.cgi

- Command Lookup Tool, a tool to help you find detailed descriptions of Cisco IOS XE commands (requires Cisco.com user ID and password)

  http://tools.cisco.com/Support/CLILookup

- Output Interpreter, a troubleshooting tool that analyzes command output of supported **show** commands

  https://www.cisco.com/pcgi-bin/Support/OutputInterpreter/home.pl\

Configuring Routing Information Protocol

Last Updated: May 4, 2009

This chapter describes how to configure Routing Information Protocol (RIP). For a complete description of the RIP commands that appear in this chapter, refer to the "RIP Commands" chapter of the *Cisco IOS IP Routing: RIP Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index, or search online.

RIP is a relatively old but still commonly used interior gateway protocol that was created for use in small, homogeneous networks. It is a classical distance-vector routing protocol. RIP is documented in RFC 1058.

RIP uses broadcast User Datagram Protocol (UDP) data packets to exchange routing information. Cisco IOS XE software sends routing information updates every 30 seconds, which is termed *advertising*. If a router does not receive an update from another router for 180 seconds or more, it marks the routes served by the nonupdating router as being unusable. If there is still no update after 240 seconds, the router removes all routing table entries for the nonupdating router.

The metric that RIP uses to rate the value of different routes is *hop count*. The hop count is the number of routers that can be traversed in a route. A directly connected network has a metric of zero; an unreachable network has a metric of 16. This small range of metrics makes RIP an unsuitable routing protocol for large networks.

A router that is running RIP can receive a default network via an update from another router that is running RIP, or the router can source (generate) the default network itself with RIP. In both cases, the default network is advertised through RIP to other RIP neighbors.

Cisco IOS XE software will source the default network with RIP if one of the following conditions is met:

- The **ip default-network** command is configured.
- The **default-information originate** command is configured.
- The default route is learned via another routing protocol or static route and is then redistributed into RIP.

RIP sends updates to the interfaces in the specified networks. If the network of an interface network is not specified, it will not be advertised in any RIP update.

The Cisco implementation of RIP Version 2 supports plain text and Message Digest 5 (MD5) authentication, route summarization, classless interdomain routing (CIDR), and variable-length subnet masks (VLSMs).

For protocol-independent features, which also apply to RIP, see the "Configuring IP Routing Protocol-Independent Features" module.

Finding Feature Information

For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "Feature Information for Configuring Routing Information Protocol" section on page 15.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS XE software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Contents

RIP Configuration Task List

To configure RIP, perform the tasks described in the following sections. The tasks in the first two sections are required; the tasks in the remaining sections are optional.

- Enabling RIP, page 3 (Required)
- Allowing Unicast Updates for RIP, page 3 (Required)
- Applying Offsets to Routing Metrics, page 3 (Optional)
- Adjusting Timers, page 4 (Optional)
- Specifying a RIP Version, page 4 (Optional)
- Enabling RIP Authentication, page 5 (Optional)
- Summarizing RIP Routes, page 6 (Optional)
- Disabling the Validation of Source IP Addresses, page 9 (Optional)
- Enabling or Disabling Split Horizon, page 9 (Optional)
- Configuring Interpacket Delay, page 10 (Optional)
- Connecting RIP to a WAN, page 10 (Optional)

For information about the following topics, see the "Configuring IP Routing Protocol-Independent Features" module:

- Filtering RIP information
- Key management (available in RIP Version 2)
- VLSM

Enabling RIP

To enable RIP, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# router rip`	Enables a RIP routing process, which places you in router configuration mode.
Step 2	`Router(config-router)# network ip-address`	Associates a network with a RIP routing process.

Allowing Unicast Updates for RIP

Because RIP is normally a broadcast protocol, in order for RIP routing updates to reach nonbroadcast networks, you must configure the Cisco IOS XE software to permit this exchange of routing information. To do so, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# neighbor ip-address`	Defines a neighboring router with which to exchange routing information.

To control the set of interfaces with which you want to exchange routing updates, you can disable the sending of routing updates on specified interfaces by configuring the **passive-interface** router configuration command. See the discussion on filtering in the "Filter Routing Information" section in the "Configuring IP Routing Protocol-Independent Features" module.

Applying Offsets to Routing Metrics

An offset list is the mechanism for increasing incoming and outgoing metrics to routes learned via RIP. Optionally, you can limit the offset list with either an access list or an interface. To increase the value of routing metrics, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# offset-list [access-list-number | access-list-name] {in | out} offset [interface-type interface-number]`	Applies an offset to routing metrics.

Adjusting Timers

Routing protocols use several timers that determine such variables as the frequency of routing updates, the length of time before a route becomes invalid, and other parameters. You can adjust these timers to tune routing protocol performance to better suit your internetwork needs. You can make the following timer adjustments:

- The rate (time in seconds between updates) at which routing updates are sent
- The interval of time (in seconds) after which a route is declared invalid
- The interval (in seconds) during which routing information regarding better paths is suppressed
- The amount of time (in seconds) that must pass before a route is removed from the routing table
- The amount of time for which routing updates will be postponed

It also is possible to tune the IP routing support in the software to enable faster convergence of the various IP routing algorithm and, hence, quicker fallback to redundant routers. The total effect is to minimize disruptions to end users of the network in situations where quick recovery is essential.

In addition, an address family can have explicitly specified timers that apply to that address-family (or VRF) only. The **timers basic** command must be specified for an address family or the system defaults for the **timers basic** command are used regardless of what is configured for RIP routing. The VRF does not inherit the timer values from the base RIP configuration. The VRF will always use the system default timers unless explicitly changed using the **timers basic** command.

To adjust the timers, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# timers basic update invalid holddown flush [sleeptime]`	Adjusts routing protocol timers.

See the "Address Family Timers Example" section at the end of this chapter for examples of adjusting timers for an address family (VRF).

Specifying a RIP Version

The Cisco implementation of RIP Version 2 supports authentication, key management, route summarization, CIDR, and VLSMs. Key management and VLSM are described in the "Configuring IP Routing Protocol-Independent Features" module.

By default, the software receives RIP Version 1 and Version 2 packets, but sends only Version 1 packets. You can configure the software to receive and send only Version 1 packets. Alternatively, you can configure the software to receive and send only Version 2 packets. To configure the software to send and receive packets from only one version, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# version {1 | 2}`	Configures the software to receive and send only RIP Version 1 or only RIP Version 2 packets.

The preceding task controls the default behavior of RIP. You can override that behavior by configuring a particular interface to behave differently. To control which RIP version an interface sends, use the following commands in interface configuration mode, as needed:

:

Command	Purpose
`Router(config-if)# ip rip send version 1`	Configures an interface to send only RIP Version 1 packets.
`Router(config-if)# ip rip send version 2`	Configures an interface to send only RIP Version 2 packets.
`Router(config-if)# ip rip send version 1 2`	Configures an interface to send RIP Version 1 and Version 2 packets.

Similarly, to control how packets received from an interface are processed, use the following commands in interface configuration mode, as needed:

Command	Purpose
`Router(config-if)# ip rip receive version 1`	Configures an interface to accept only RIP Version 1 packets.
`Router(config-if)# ip rip receive version 2`	Configures an interface to accept only RIP Version 2 packets.
`Router(config-if)# ip rip receive version 1 2`	Configures an interface to accept either RIP Version 1 or 2 packets.

Enabling RIP Authentication

RIP Version 1 does not support authentication. If you are sending and receiving RIP Version 2 packets, you can enable RIP authentication on an interface.

The key chain determines the set of keys that can be used on the interface. If a key chain is not configured, no authentication is performed on that interface, not even the default authentication. Therefore, you must also perform the tasks in the section “Managing Authentication Keys” in the “Configuring IP Routing Protocol-Independent Features” module.

We support two modes of authentication on an interface for which RIP authentication is enabled: plain text authentication and MD5 authentication. The default authentication in every RIP Version 2 packet is plain text authentication.

Note Do not use plain text authentication in RIP packets for security purposes, because the unencrypted authentication key is sent in every RIP Version 2 packet. Use plain text authentication when security is not an issue, for example, to ensure that misconfigured hosts do not participate in routing.

To configure RIP authentication, use the following commands in interface configuration mode:

	Command	Purpose
Step 1	`Router(config-if)# ip rip authentication key-chain` *`name-of-chain`*	Enables RIP authentication.
Step 2	`Router(config-if)# ip rip authentication mode {text | md5}`	Configures the interface to use MD5 digest authentication (or let it default to plain text authentication).

See the "Key Management Examples" section of the "Configuring IP Routing Protocol-Independent Features" module for key management information and examples.

Summarizing RIP Routes

Summarizing routes in RIP Version 2 improves scalability and efficiency in large networks. Summarizing IP addresses means that there is no entry for child routes (routes that are created for any combination of the individual IP addresses contained within a summary address) in the RIP routing table, reducing the size of the table and allowing the router to handle more routes.

Summary IP address functions more efficiently than multiple individually advertised IP routes for the following reasons:

- The summarized routes in the RIP database are processed first.
- Any associated child routes that are included in a summarized route are skipped as RIP looks through the routing database, reducing the processing time required.

Cisco routers can summarize routes in two ways:

- Automatically, by summarizing subprefixes to the classful network boundary when crossing classful network boundaries (automatic summary).

Note You need not configure anything for automatic summary to be enabled. To disable automatic summary, use the **no auto-summary** router configuration command.

- As specifically configured, advertising a summarized local IP address pool on the specified interface (on a network access server) so that the address pool can be provided to dialup clients.

Automatic summary addressing always summarizes to the classful address boundary, while the **ip summary-address** router configuration command summarizes addresses on a specified interface. If automatic summary addressing is enabled, automatic summarization is the default behavior for interfaces on the router not associated with dial-in clients (the "backbone"), with *or* without the **ip summary-address rip** interface command present.

For example, if a local IP address pool of 10.1.1.1 to 10.1.1.254 is configured on the network access server, you could configure the **ip summary-address rip 10.1.1.0 255.255.255.0** command on the network access server port that provides addresses to dialup clients to cause the router to advertise 10.1.1.0/24 routes to dialup clients. Because a summary route is advertised, advertisement of the /32 host routes (installed when the dialup client connects) is suppressed so that the router does not advertise these routes to the network access server interface.

Automatic summary will override the configured summary address feature on a given interface except when *both* of the following conditions are true:

- The configured interface summary address and the IP address of the configured interface share the same major network (the classful, nonsubnetted portion of the IP address).
- Split horizon is not enabled on the interface.

In the following example configuration, the major network is 10.0.0.0. The 10 in the address defines a Class A address space, allowing space for 0.*x*.*x*.*x* unique hosts where *x* defines unique bit positions in the addresses for these hosts. The summary of the major net defines the prefix as implied by the class (A, B, or C) of the address, without any network mask. The summary address 10.2.0.0 overrides the automatic summary address of 10.0.0.0, 10.2.0.0 is advertised out interface E1, and 10.0.0.0 is not advertised.

```
Router(config)# interface Ethernet1
```

```
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if)# ip summary-address rip 10.2.0.0 255.255.0.0
Router(config-if)# no ip split-horizon
Router(config-if)# exit
Router(config)# router rip
Router(config)# network 10.0.0.0
```

When RIP determines that a summary address is required in the RIP database, a summary entry is created in the RIP routing database. As long as there are child routes for a summary address, the address remains in the routing database. When the last child route is removed, the summary entry also is removed from the database. This method of handling database entries reduces the number of entries in the database because each child route is not listed in an entry, and the aggregate entry itself is removed when there are no longer any valid child routes for it.

RIP Version 2 route summarization requires that the lowest metric of the "best route" of an aggregated entry, or the lowest metric of all current child routes, be advertised. The best metric for aggregated summarized routes is calculated at route initialization or when there are metric modifications of specific routes at advertisement time, and not at the time the aggregated routes are advertised.

Restrictions to RIP Route Summarization

Supernet advertisement (advertising any network prefix less than its classful major network) is not allowed in RIP route summarization, other than advertising a supernet learned in the routing tables. Supernets learned on any interface that is subject to configuration are still learned.

For example, the following summarization is invalid: (invalid supernet summarization)

```
Router(config)# interface Ethernet 1
Router(config-if)# ip summary-address rip 10.0.0.0 252.0.0.0
.
.
.
```

Each route summarization on an interface must have a unique major net, even if the subnet mask is unique. For example, the following is not permitted:

```
Router(config)# interface Ethernet 1
Router(config)# ip summary-address rip 10.1.0.0 255.255.0.0
Router(config)# ip summary-address rip 10.2.2.0 255.255.255.0
.
.
.
```

Note The **ip summary-address eigrp** router configuration command uses other options that are not applicable to RIP. Do not confuse EIGRP summary address with the new RIP command, **ip summary-address rip**.

Configuring Route Summarization on an Interface

The **ip summary-address rip** router configuration command causes the router to summarize a given set of routes learned via RIP Version 2 or redistributed into RIP Version 2. Host routes are especially applicable for summarization. To configure IP summary addressing, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface type number`	Enters interface configuration mode.
Step 2	`Router(config-if)# ip summary-address rip ip-address network-mask`	Specifies the IP address and network mask that identify the routes to be summarized.

See the "Route Summarization Examples" section at the end of this chapter for examples of using split horizon.

Verifying IP Route Summarization

You can verify which routes are summarized for an interface using the **show ip protocols** EXEC command. The following example shows potential summarizations and the associated interface summary address and network mask for Ethernet interface 2:

```
Router# show ip protocols

 Routing Protocol is "rip"
   Sending updates every 30 seconds, next due in 8 seconds
   Invalid after 180 seconds, hold down 180, flushed after 240
   Outgoing update filter list for all interfaces is
   Incoming update filter list for all interfaces is
   Redistributing: rip
   Default version control: send version 2, receive version 2
     Interface        Send  Recv  Triggered RIP  Key-chain
     Ethernet2        2     2
     Ethernet3        2     2
     Ethernet4        2     2
     Ethernet5        2     2
   Automatic network summarization is not in effect
   Address Summarization:
     10.11.0.0/16 for Ethernet2
```

You can check summary address entries in the RIP database. These entries will appear in the database only if relevant child routes are being summarized. When the last child route for a summary address becomes invalid, the summary address is also removed from the routing table. The following example shows a summary address entry for route 10.11.0.0/16, with three child routes active:

```
Router# show ip rip database

 10.0.0.0/8    auto-summary
 10.11.11.0/24    directly connected, Ethernet2
 10.1.0.0/8    auto-summary
 10.11.0.0/16    int-summary
 ^^^^^^^^^^^^^^^^^^^^^^^^^^^
 10.11.10.0/24    directly connected, Ethernet3
 10.11.11.0/24    directly connected, Ethernet4
 10.11.12.0/24    directly connected, Ethernet5
```

Disabling Automatic Route Summarization

RIP Version 2 supports automatic route summarization by default. The software summarizes subprefixes to the classful network boundary when crossing classful network boundaries.

If you have disconnected subnets, disable automatic route summarization to advertise the subnets. When route summarization is disabled, the software sends subnet and host routing information across classful network boundaries. To disable automatic summarization, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# no auto-summary`	Disables automatic summarization.

Disabling the Validation of Source IP Addresses

By default, the software validates the source IP address of incoming RIP routing updates. If that source address is not valid, the software discards the routing update. You might want to disable this feature if you have a router that is "off network" and you want to receive its updates. However, disabling this feature is not recommended under normal circumstances.

To disable the default function that validates the source IP addresses of incoming routing updates, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# no validate-update-source`	Disables the validation of the source IP address of incoming RIP routing updates.

Enabling or Disabling Split Horizon

Normally, routers that are connected to broadcast-type IP networks and that use distance-vector routing protocols employ the *split horizon* mechanism to reduce the possibility of routing loops. Split horizon blocks information about routes from being advertised by a router out of any interface from which that information originated. This behavior usually optimizes communications among multiple routers, particularly when links are broken. However, with nonbroadcast networks (such as Frame Relay and Switched Multimegabit Digital System [SMDS]), situations can arise for which this behavior is less than ideal. For these situations, you may want to disable split horizon with RIP.

If an interface is configured with secondary IP addresses and split horizon is enabled, updates might not be sourced by the secondary address. One routing update is sourced per network number unless split horizon is disabled.

To enable or disable split horizon, use the following commands in interface configuration mode, as needed:

Command	Purposes
`Router(config-if)# ip split-horizon`	Enables split horizon.
`Router(config-if)# no ip split-horizon`	Disables split horizon.

Split horizon for Frame Relay and SMDS encapsulation is disabled by default. Split horizon is not disabled by default for interfaces using any of the X.25 encapsulations. For all other encapsulations, split horizon is enabled by default.

See the "Split Horizon Examples" section at the end of this chapter for examples of using split horizon.

Note In general, changing the state of the default is not recommended unless you are certain that your application requires making a change in order to advertise routes properly. Remember that if split horizon is disabled on a serial interface (and that interface is attached to a packet-switched network), you *must* disable split horizon for all routers in any relevant multicast groups on that network.

Configuring Interpacket Delay

By default, the software adds no delay between packets in a multiple-packet RIP update being sent. If you have a high-end router sending to a low-speed router, you might want to add such interpacket delay to RIP updates, in the range of 8 to 50 milliseconds. To do so, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# output-delay milliseconds`	Configures interpacket delay for outbound RIP updates.

Connecting RIP to a WAN

Routers are used on connection-oriented networks to allow potential connectivity to many remote destinations. Circuits on the WAN are established on demand and are relinquished when the traffic subsides. Depending on the application, the connection between any two sites for user data could be short and relatively infrequent.

There are two problems using RIP to connect to a WAN:

- Periodic broadcasting by RIP generally prevents WAN circuits from being closed.
- Even on fixed, point-to-point links, the overhead of periodic RIP transmissions could seriously interrupt normal data transfer because of the quantity of information that passes through the line every 30 seconds.

To overcome these limitations, triggered extensions to RIP cause RIP to send information on the WAN only when there has been an update to the routing database. Periodic update packets are suppressed over the interface on which this feature is enabled. RIP routing traffic is reduced on point-to-point, serial interfaces. Therefore, you can save money on an on-demand circuit for which you are charged for usage. Triggered extensions to RIP partially support RFC 2091, *Triggered Extensions to RIP to Support Demand Circuits*.

To enable triggered extensions to RIP, use the following commands in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface serial controller-number`	Configures a serial interface.
Step 2	`Router(config-if)# ip rip triggered`	Enables triggered extensions to RIP.

To display the contents of the RIP private database, use the following command in EXEC mode:

Command	Purpose
`Router# show ip rip database [prefix mask]`	Displays the contents of the RIP private database.

RIP Configuration Examples

The following section provides RIP configuration examples:

Route Summarization Examples

A correct and an incorrect configuration example of route summarization is provided.

Example 1: Correct Configuration

The following example shows how the **ip summary-address rip** router configuration command works with automatic summary addressing in RIP, starting in global configuration mode. In the example, the major network is 10.0.0.0. The summary address 10.2.0.0 overrides the automatic summary address of 10.0.0.0, so that 10.2.0.0 is advertised out Gigabit Ethernet interface 0/0/0 and 10.0.0.0 is not advertised.

Note If split horizon is enabled, neither automatic summary nor interface summary addresses (those configured with the **ip summary-address rip router configuration** command) are advertised.

```
Router(config)# router rip
Router(config-router)# network 10.0.0.0
Router(config-router)# exit
Router(config)# interface gigabitethernet 0/0/0
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if)# ip summary-address rip 10.2.0.0 255.255.0.0
Router(config-if)# no ip split-horizon
Router(config-if)# exit
```

Example 2: Incorrect Configuration

The following example shows an illegal use of the **ip summary-address rip** router configuration command, because both addresses to be summarized have the same major network. Each route summarization on an interface must have a unique major network, whether or not the addresses have unique address masks.

```
Router(config)# interface gigabitethernet 0/0/0
Router(config-if)# ip summary-address rip 10.1.0.0 255.255.0.0
Router(config-if)# ip summary-address rip 10.2.2.0 255.255.255.0
.
.
.
```

Split Horizon Examples

Two examples of configuring split horizon are provided.

Example 1

The following configuration shows a simple example of disabling split horizon on a serial link. In this example, the serial link is connected to an X.25 network.

```
Router(config)# interface serial 0/0/0
Router(config-if)# no ip split-horizon
```

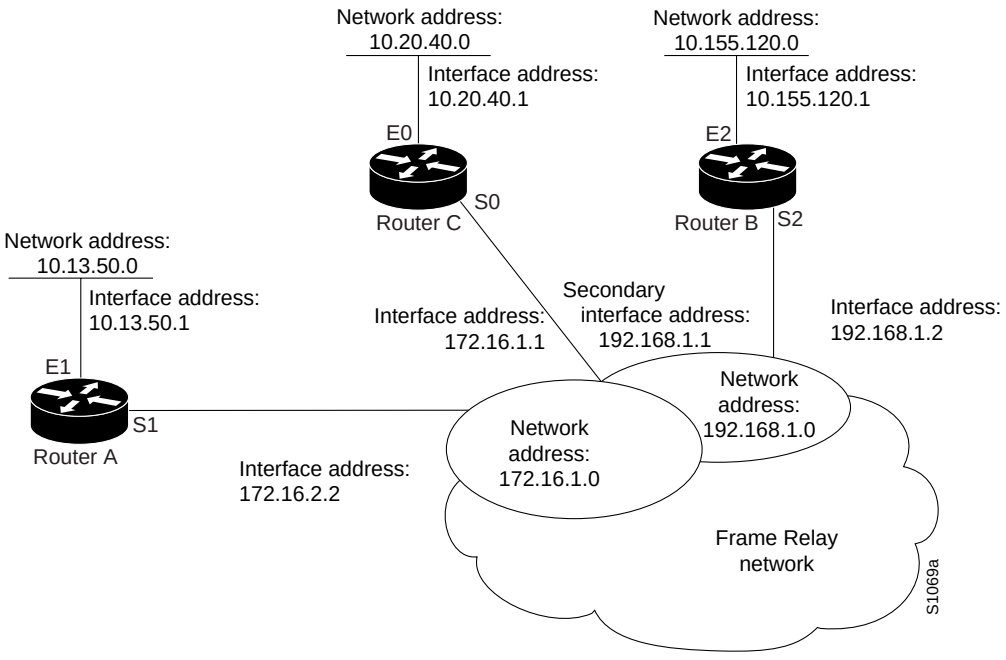
Example 2

In the next example, Figure 1 illustrates a typical situation in which the **no ip split-horizon** interface configuration command would be useful. This figure depicts two IP subnets that are both accessible via a serial interface on Router C (connected to Frame Relay network). In this example, the serial interface on Router C accommodates one of the subnets via the assignment of a secondary IP address.

The Gigabit Ethernet interfaces for Router A, Router B, and Router C (connected to IP networks 10.13.50.0, 10.155.120.0, and 10.20.40.0, respectively), all have split horizon enabled by default, while the serial interfaces connected to networks 172.16.1.0 and 192.168.1.0 all have split horizon disabled with the no ip split-horizon command. Figure 1 shows the topology and interfaces.

Note In the figure, the Gigabit Ethernet interfaces are represented by “E0,” “E1,” and so on.

Figure 1 Disabled Split Horizon Example for Frame Relay Network



In this example, split horizon is disabled on all serial interfaces. The split horizon must be disabled on Router C in order for network 172.16.0.0 to be advertised into network 192.168.0.0 and vice versa. These subnets overlap at Router C, interface S0. If split horizon were enabled on serial interface S0, it would not advertise a route back into the Frame Relay network for either of these networks.

Configuration for Router A

```
interface gigabitethernet 0/0/0
 ip address 10.13.50.1
!
interface serial 0/0/0
 ip address 172.16.2.2
 encapsulation frame-relay
 no ip split-horizon
```

Configuration for Router B

```
interface gigabitethernet 0/0/0
 ip address 10.155.120.1
!
interface serial 0/0/0
 ip address 192.168.1.2
 encapsulation frame-relay
 no ip split-horizon
```

Configuration for Router C

```
interface gigabitethernet 0/0/0
 ip address 10.20.40.1
!
interface serial 0/0/0
 ip address 172.16.1.1
 ip address 192.168.1.1 secondary
 encapsulation frame-relay
 no ip split-horizon
```

Address Family Timers Example

The following example shows how to adjust individual address family timers.
Note that the address family “notusingtimers” will use the system defaults of 30, 180, 180, and 240 even though timer values of 5, 10, 15, and 20 are used under the general RIP configuration. Address family timers are not inherited from the general RIP configuration.

```
Router(config)# router rip
Router(config-router)# version 2
Router(config-router)# timers basic 5 10 15 20
Router(config-router)# redistribute connected
Router(config-router)# network 5.0.0.0
Router(config-router)# default-metric 10
Router(config-router)# no auto-summary
Router(config-router)#!
Router(config-router)# address-family ipv4 vrf foo
Router(config-router-af)# timers basic 10 20 20 20
Router(config-router-af)# redistribute connected
Router(config-router-af)# network 10.0.0.0
Router(config-router-af)# default-metric 5
Router(config-router-af)# no auto-summary
Router(config-router-af)# version 2
Router(config-router-af)# exit-address-family
Router(config-router)# !
Router(config-router)# address-family ipv4 vrf bar
```

```
Router(config-router-af)# timers basic 20 40 60 80
Router(config-router-af)# redistribute connected
Router(config-router-af)# network 20.0.0.0
Router(config-router-af)# default-metric 2
Router(config-router-af)# no auto-summary
Router(config-router-af)# version 2
Router(config-router-af)# exit-address-family
Router(config-router)#!
Router(config-router)# address-family ipv4 vrf notusingtimers
Router(config-router-af)# redistribute connected
Router(config-router-af)# network 20.0.0.0
Router(config-router-af)# default-metric 2
Router(config-router-af)# no auto-summary
Router(config-router-af)# version 2
Router(config-router-af)# exit-address-family
Router(config-router)#!
```

Additional References

The following sections provide references related to the RIP feature.

Related Documents

Related Topic	Document Title
RIP commands	*Cisco IOS IP Routing: RIP Command Reference*
Protocol-independent features	"Configuring IP Routing Protocol-Independent Features" module

MIBs

MIB	MIBs Link
—	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 1058	*Routing Information Protocol*
RFC 2091	*Triggered Extensions to RIP to Support Demand Circuits*

Feature Information for Configuring Routing Information Protocol

Table 1 lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS XE software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the Cisco IOS XE software release that introduced support for a given feature in a given Cisco IOS XE software release train. Unless noted otherwise, subsequent releases of that Cisco IOS XE software release train also support that feature.

Table 1 Feature Information for Configuring Routing Information Protocol

Feature Name	Releases	Feature Information
RIP	Cisco IOS XE Release 2.1	This feature was introduced. The following commands were introduced or modified: • **ip rip authentication key-chain** • **ip rip authentication mode** • **ip rip receive version** • **ip rip send version** • **ip split-horizon (RIP)** • **neighbor (RIP)** • **network (RIP)** • **offset-list (RIP)** • **output-delay** • **router rip** • **timers basic (RIP)** • **validate-update-source** • **version**
IP Summary Address for RIPv2	Cisco IOS XE Release 2.1	This feature was introduced. The following section provides information about this feature: • Summarizing RIP Routes, page 6 The following commands were introduced or modified: • **auto-summary** • **ip summary-address rip** • **show ip protocols**
Triggered RIP	Cisco IOS XE Release 2.1	This feature was introduced. The following section provides information about this feature: • Connecting RIP to a WAN, page 10 The following commands were introduced or modified: • **debug ip rip triggered** • **ip rip triggered** • **show ip rip database**

RIPv2 Monitoring with SNMP Using the RFC 1724 MIB Extensions

First Published: February 27, 2006
Last Updated: May 4, 2009

This document describes the Cisco IOS XE implementation of RFC 1724, *RIP Version 2 MIB Extensions*. RFC 1724 defines Management Information Base (MIB) objects that allow you to monitor RIPv2 using the Simple Network Management Protocol (SNMP).

Finding Feature Information

For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "Feature Information for RIPv2 Monitoring with SNMP Using the RFC 1724 MIB Extensions" section on page 12.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS XE software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for RIPv2 Monitoring with SNMP Using the RFC 1724 MIB Extensions

- RIPv2 must be configured on the router.
- Your SNMP Network Management Station (NMS) must have the RFC 1724 RIPv2 MIB installed.
- Your SNMP NMS must have the following MIBs installed because RFC 1724 imports data types and object identifiers (OIDs) from them:
  - SNMPv2-SMI
  - SNMPv2-TC
  - SNMPv2-CONF
  - RFC1213-MIB

Restrictions for RIPv2 Monitoring with SNMP Using the RFC 1724 MIB Extensions

This implementation of the RIPv2 MIB does not track any data associated with a RIP Virtual Routing and Forwarding (VRF) instance. Only interfaces that are assigned IP addresses in the IP address space configured by the **network** command in RIP router configuration mode are tracked. Global data is tracked only for changes to the main routing table.

Information About RIPv2 Monitoring with SNMP Using the RFC 1724 MIB Extensions

The following sections contain information about the MIB objects standardized as part of RFC 1724 and the benefits of the RFC 1724 MIB.

RIPv2 MIB

This section describes the MIB objects that are provided by RFC 1724 definitions. The RIPv2 MIB consists of the following managed objects:

- Global counters—Used to keep track of changing routes or neighbor changes.
- Interface status table—Defines objects that are used to keep track of statistics specific to interfaces.

- Interface configuration table—Defines objects that are used to keep track of interface configuration statistics.
- Peer table—Defined to monitor neighbor relationships. This object is not implemented in Cisco IOS XE software.

Table 1, Table 2, and Table 3 show the objects that are provided by RFC 1724 RIPv2 MIB definitions. The objects are listed in the order in which they appear within the RFC 1724 RIPv2 MIB, per the tables that describe them. The statistics for all of the objects in the global counters can be obtained by querying the rip2Globals object identifier (OID) using **snmpwalk**, or a similar SNMP toolset command on your NMS.

Table 1 shows the RFC 1724 RIPv2 MIB global counter objects.

Table 1 RFC 1724 RIPv2 MIB Global Counters Objects

Global Counter	Object	Description
rip2Globals	rip2GlobalRouteChanges	Number of route changes made to the IP route database by RIP. Number is incremented when a route is modified.
	rip2GlobalQueries	Number of responses sent to RIP queries from other systems. Number is incremented when RIP responds to a query from another system.

The objects in the RFC 1724 RIPv2 MIB interface table track information on a per interface basis. All object in the RFC 1724 RIPv2 MIB interface table, except for the rip2IfStatAddress object, represent newly tracked data within RIP. There are no equivalent **show** commands for these objects. All objects in the RIPv2 MIB interface table are implemented read-only.

Table 2 shows the RFC 1724 RIPv2 MIB interface table objects. The statistics for all objects in the interface table can be obtained by querying the sequence name Rip2IfStatEntry using **snmpwalk** or a similar SNMP toolset command on your NMS.

Table 2 RFC 1724 RIPv2 MIB Interface Table Objects

Sequence Name	Object	Description
Rip2IfStatEntry	rip2IfStatAddress	The IP address of this system on the indicated subnet. For unnumbered interfaces, the value of 0.0.0.N, where the least significant 24 bits (N) are the ifIndex for the IP interface in network byte order.
	rip2IfStatRcvBadPackets	The number of RIP response packets received by the RIP process that were subsequently discarded for any reason. For example, a version 0 packet or an unknown command type.
	rip2IfStatRcvBadRoutes	The number of routes, in valid RIP packets, that were ignored for any reason. This is incremented when: • The address family identifier does not equal AF_INET. • If a RIP v2 update is received and the class D and greater. • If a RIP v2 update is received and the address is a martian address.
	rip2IfStatSentUpdates	The number of triggered RIP updates actually sent on this interface. This explicitly does *not* include full updates sent containing new information.
	rip2IfStatStatus	This value is always set to 1.

The objects in the RFC 1724 RIPv2 MIB interface configuration table track information on a per interface basis. Except for the Rip2IfConfAuthType object, the data for the objects in the RFC 1724 RIPv2 MIB interface configuration table can also be gathered with the **show ip protocol** commands. All objects in the RIPv2 MIB interface table are implemented read-only.

Table 3 shows the RIPv2 MIB interface configuration table objects. The statistics for all objects in the configuration table can be obtained by querying the sequence name rip2IfConfEntry using **snmpwalk** or a similar SNMP toolset command on your NMS.

Table 3 RFC 1724 RIPv2 MIB Interface Configuration Table Object Types

Sequence Name	Object Type	Description
rip2IfConfEntry	rip2IfConfAddress	The IP address of this system on the indicated subnet. For unnumbered interfaces, the value 0.0.0.N, where the least significant 24 bits (N) are the ifIndex for the IP interface in network byte order.
	rip2IfConfDomain	This value is always equal to "".
	rip2IfConfAuthType	The type of authentication used on this interface.
	rip2IfConfAuthKey	The value to be used as the authentication key whenever the corresponding instance of rip2IfConfAuthType has a value other than no authentication.
	rip2IfConfSend	The version of RIP updates that are sent on this interface.
	rip2IfConfReceive	The version of RIP updates that are accepted on this interface.
	rip2IfConfDefaultMetric	This variable indicates the metric that is used for the default route entry in RIP updates originated on this interface.
	rip2IfConfStatus	This value is always set to 1.
	rip2IfConfSrcAddress	The IP address that this system will use as a source address on this interface. If it is a numbered interface, this *must* be the same value as rip2IfConfAddress. On unnumbered interfaces, it must be the value of rip2IfConfAddress for some interface on the system.

Benefits of the RIPv2 MIB

The RFC 1724 RIPv2 MIB extensions allow network managers to monitor the RIPv2 routing protocol using SNMP through the addition of new global counters and table objects that previously were not supported by the RFC 1389 RIPv2 MIB. The new global counters and table objects are intended to facilitate quickly changing routes or failing neighbors.

How to Enable RIPv2 Monitoring with SNMP Using the RFC 1724 MIB Extensions

This section contains the following tasks:

- Enabling SNMP Read-Only Access on the Router, page 6 (required)
- Verifying the Status of the RIPv2: RFC1724 MIB Extensions on the Router and Your Network Management Station, page 7 (optional)

Enabling SNMP Read-Only Access on the Router

There are no router configuration tasks required for the RIPv2 Monitoring with SNMP Using the RFC 1724 MIB Extensions feature itself. SNMP read-only access to the objects in the RFC 1724 RIPv2 MIB is enabled when you configure the SNMP server read-only community string on the router.

Note When you configure an SNMP server read-only community string on the router, you are granting SNMP read-only access to the objects that support read-only access in all MIBs that are available in the version of Cisco IOS XE that is running on the router.

Perform this task to configure the SNMP server read-only community string on the router to enable SNMP read-only access to MIB objects (including the RFC 1724 RIPv2 MIB extensions) on the router.

SNMP Community Strings

Routers can have multiple read-only SNMP community strings. When you configure an SNMP read-only community string for the **snmp-server** command on the router, an existing SNMP **snmp-server** read-only community string is not overwritten. For example, if you enter the **snmp-server community** *string1* **ro** and **snmp-server community** *string2* **ro** commands on the router, the router will have two valid read-only community strings—*string1* and *string2*. If this is not the behavior that you desire, use the **no snmp-server community** *string* **ro** command to remove an existing SNMP read-only community string.

Timesaver If you already have an SNMP read-only community string configured on your router, you do not need to perform this task. After you load Cisco IOS XE Release 2.1 or a later release on your router, you can use SNMP commands on your NMS to query the RFC 1724 RIPv2 MIB on your router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server community** *string1* **ro**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server community** *string1* **ro** **Example:** `Router(config)# snmp-server community T8vCx3 ro`	Enables SNMP read-only access to the objects in the MIBs that are included in the version of Cisco IOS XE software that is running on the router. **Note** For security purposes, do not use the standard default value of *public* for your read-only community string. Use a combination of uppercase and lowercase letters and numbers for the password.
Step 4	**end** **Example:** `Router(config)# end`	Ends your configuration session and returns to privileged EXEC mode.

Verifying the Status of the RIPv2: RFC1724 MIB Extensions on the Router and Your Network Management Station

Perform this optional task on your NMS to verify the status of the RFC 1724 RIPv2 MIB extensions on the router and on your NMS.

Note This task uses the NET-SNMP toolset that is available in the public domain. The step that is documented uses a terminal session on an NMS that is running Linux. Substitute the SNMP command from the SNMP toolset on your NMS as appropriate when you perform this task.

Prerequisites

Your NMS must have the RFC 1724 MIB installed.

SUMMARY STEPS

1. **snmpwalk -m all -v2c** *ip-address* **-c** *read-only-community-string* **rip2Globals**

DETAILED STEPS

Step 1 **snmpwalk -m all -v2c** *ip-address* **-c** *read-only-community-string* **rip2Globals**

Use the **snmpwalk** command for the **rip2Globals** object in the RFC 1724 RIPv2 MIB to display the data for the objects associated with this object. This step verifies that the NMS is configured to send queries for objects in the RFC 1724 RIPv2 MIB and that the router is configured to respond to the queries.

```
$ snmpwalk -m all -v2c 10.0.0.253 -c T8vCx3 rip2Globals

RIPv2-MIB::rip2GlobalRouteChanges.0 = Counter32: 5
RIPv2-MIB::rip2GlobalQueries.0 = Counter32: 1
$
```

Configuration Examples for RIPv2 Monitoring with SNMP Using the RIPv2: RFC1724 MIB Extensions

This section contains the following examples:

Querying the RIP Interface Status Table Objects: Example

The following example shows how to send an SNMP query to obtain data for all objects in the RIP interface status table using the **snmpwalk** command.

```
$ snmpwalk -m all -v2c 10.0.0.253 -c T8vCx3 Rip2IfStatEntry

RIPv2-MIB::rip2IfStatAddress.10.0.0.253 = IpAddress: 10.0.0.253
RIPv2-MIB::rip2IfStatAddress.172.16.1.1 = IpAddress: 172.16.1.1
RIPv2-MIB::rip2IfStatAddress.172.16.2.1 = IpAddress: 172.16.2.1
RIPv2-MIB::rip2IfStatAddress.172.17.1.1 = IpAddress: 172.17.1.1
RIPv2-MIB::rip2IfStatAddress.172.17.2.1 = IpAddress: 172.17.2.1
RIPv2-MIB::rip2IfStatRcvBadPackets.10.0.0.253 = Counter32: 0
RIPv2-MIB::rip2IfStatRcvBadPackets.172.16.1.1 = Counter32: 1654
RIPv2-MIB::rip2IfStatRcvBadPackets.172.16.2.1 = Counter32: 1652
RIPv2-MIB::rip2IfStatRcvBadPackets.172.17.1.1 = Counter32: 1648
RIPv2-MIB::rip2IfStatRcvBadPackets.172.17.2.1 = Counter32: 1649
RIPv2-MIB::rip2IfStatRcvBadRoutes.10.0.0.253 = Counter32: 0
RIPv2-MIB::rip2IfStatRcvBadRoutes.172.16.1.1 = Counter32: 0
RIPv2-MIB::rip2IfStatRcvBadRoutes.172.16.2.1 = Counter32: 0
RIPv2-MIB::rip2IfStatRcvBadRoutes.172.17.1.1 = Counter32: 0
RIPv2-MIB::rip2IfStatRcvBadRoutes.172.17.2.1 = Counter32: 0
RIPv2-MIB::rip2IfStatSentUpdates.10.0.0.253 = Counter32: 0
RIPv2-MIB::rip2IfStatSentUpdates.172.16.1.1 = Counter32: 0
RIPv2-MIB::rip2IfStatSentUpdates.172.16.2.1 = Counter32: 0
RIPv2-MIB::rip2IfStatSentUpdates.172.17.1.1 = Counter32: 0
RIPv2-MIB::rip2IfStatSentUpdates.172.17.2.1 = Counter32: 0
RIPv2-MIB::rip2IfStatStatus.10.0.0.253 = INTEGER: active(1)
RIPv2-MIB::rip2IfStatStatus.172.16.1.1 = INTEGER: active(1)
RIPv2-MIB::rip2IfStatStatus.172.16.2.1 = INTEGER: active(1)
RIPv2-MIB::rip2IfStatStatus.172.17.1.1 = INTEGER: active(1)
RIPv2-MIB::rip2IfStatStatus.172.17.2.1 = INTEGER: active(1)
```

The following example shows how to send an SNMP query to obtain data for the rip2IfStatStatus object for all of the interfaces in the RIP interface status table using the **snmpwalk** command.

```
$ snmpwalk -m all -v2c 10.0.0.253 -c T8vCx3 rip2IfStatStatus

RIPv2-MIB::rip2IfStatStatus.10.0.0.253 = INTEGER: active(1)
RIPv2-MIB::rip2IfStatStatus.172.16.1.1 = INTEGER: active(1)
RIPv2-MIB::rip2IfStatStatus.172.16.2.1 = INTEGER: active(1)
RIPv2-MIB::rip2IfStatStatus.172.17.1.1 = INTEGER: active(1)
RIPv2-MIB::rip2IfStatStatus.172.17.2.1 = INTEGER: active(1)
$
```

The following example shows how to send an SNMP query to obtain data for the rip2IfStatStatus object for a specific interface IP address in the RIP interface status table using the **snmpget** command.

```
$ snmpget -m all -v2c 10.0.0.253 -c T8vCx3 rip2IfStatStatus.10.0.0.253

RIPv2-MIB::rip2IfStatStatus.10.0.0.253 = INTEGER: active(1)
$
```

Querying the RIP Interface Configuration Table Objects: Example

The following example shows how to send an SNMP query to obtain data for all objects in the RIP interface configuration table using the **snmpwalk** command.

```
$ snmpwalk -m all -v2c 10.0.0.253 -c T8vCx3 rip2IfConfEntry

RIPv2-MIB::rip2IfConfAddress.10.0.0.253 = IpAddress: 10.0.0.253
RIPv2-MIB::rip2IfConfAddress.172.16.1.1 = IpAddress: 172.16.1.1
RIPv2-MIB::rip2IfConfAddress.172.16.2.1 = IpAddress: 172.16.2.1
RIPv2-MIB::rip2IfConfAddress.172.17.1.1 = IpAddress: 172.17.1.1
RIPv2-MIB::rip2IfConfAddress.172.17.2.1 = IpAddress: 172.17.2.1
RIPv2-MIB::rip2IfConfDomain.10.0.0.253 = ""
RIPv2-MIB::rip2IfConfDomain.172.16.1.1 = ""
RIPv2-MIB::rip2IfConfDomain.172.16.2.1 = ""
RIPv2-MIB::rip2IfConfDomain.172.17.1.1 = ""
RIPv2-MIB::rip2IfConfDomain.172.17.2.1 = ""
RIPv2-MIB::rip2IfConfAuthType.10.0.0.253 = INTEGER: noAuthentication(1)
RIPv2-MIB::rip2IfConfAuthType.172.16.1.1 = INTEGER: noAuthentication(1)
RIPv2-MIB::rip2IfConfAuthType.172.16.2.1 = INTEGER: noAuthentication(1)
RIPv2-MIB::rip2IfConfAuthType.172.17.1.1 = INTEGER: noAuthentication(1)
RIPv2-MIB::rip2IfConfAuthType.172.17.2.1 = INTEGER: noAuthentication(1)
RIPv2-MIB::rip2IfConfAuthKey.10.0.0.253 = ""
RIPv2-MIB::rip2IfConfAuthKey.172.16.1.1 = ""
RIPv2-MIB::rip2IfConfAuthKey.172.16.2.1 = ""
RIPv2-MIB::rip2IfConfAuthKey.172.17.1.1 = ""
RIPv2-MIB::rip2IfConfAuthKey.172.17.2.1 = ""
RIPv2-MIB::rip2IfConfSend.10.0.0.253 = INTEGER: ripVersion2(4)
RIPv2-MIB::rip2IfConfSend.172.16.1.1 = INTEGER: ripVersion2(4)
RIPv2-MIB::rip2IfConfSend.172.16.2.1 = INTEGER: ripVersion2(4)
RIPv2-MIB::rip2IfConfSend.172.17.1.1 = INTEGER: ripVersion2(4)
RIPv2-MIB::rip2IfConfSend.172.17.2.1 = INTEGER: ripVersion2(4)
RIPv2-MIB::rip2IfConfReceive.10.0.0.253 = INTEGER: rip2(2)
RIPv2-MIB::rip2IfConfReceive.172.16.1.1 = INTEGER: rip2(2)
RIPv2-MIB::rip2IfConfReceive.172.16.2.1 = INTEGER: rip2(2)
RIPv2-MIB::rip2IfConfReceive.172.17.1.1 = INTEGER: rip2(2)
RIPv2-MIB::rip2IfConfReceive.172.17.2.1 = INTEGER: rip2(2)
RIPv2-MIB::rip2IfConfDefaultMetric.10.0.0.253 = INTEGER: 1
RIPv2-MIB::rip2IfConfDefaultMetric.172.16.1.1 = INTEGER: 1
RIPv2-MIB::rip2IfConfDefaultMetric.172.16.2.1 = INTEGER: 1
RIPv2-MIB::rip2IfConfDefaultMetric.172.17.1.1 = INTEGER: 1
RIPv2-MIB::rip2IfConfDefaultMetric.172.17.2.1 = INTEGER: 1
```

```
RIPv2-MIB::rip2IfConfStatus.10.0.0.253 = INTEGER: active(1)
RIPv2-MIB::rip2IfConfStatus.172.16.1.1 = INTEGER: active(1)
RIPv2-MIB::rip2IfConfStatus.172.16.2.1 = INTEGER: active(1)
RIPv2-MIB::rip2IfConfStatus.172.17.1.1 = INTEGER: active(1)
RIPv2-MIB::rip2IfConfStatus.172.17.2.1 = INTEGER: active(1)
RIPv2-MIB::rip2IfConfSrcAddress.10.0.0.253 = IpAddress: 10.0.0.253
RIPv2-MIB::rip2IfConfSrcAddress.172.16.1.1 = IpAddress: 172.16.1.1
RIPv2-MIB::rip2IfConfSrcAddress.172.16.2.1 = IpAddress: 172.16.2.1
RIPv2-MIB::rip2IfConfSrcAddress.172.17.1.1 = IpAddress: 172.17.1.1
RIPv2-MIB::rip2IfConfSrcAddress.172.17.2.1 = IpAddress: 172.17.2.1
$
```

The following example shows how to send an SNMP query to obtain data for the rip2IfConfAddress object for all interfaces in the RIP interface configuration table using the **snmpwalk** command.

```
$ snmpwalk -m all -v2c 10.0.0.253 -c T8vCx3 rip2IfConfAddress

RIPv2-MIB::rip2IfConfAddress.10.0.0.253 = IpAddress: 10.0.0.253
RIPv2-MIB::rip2IfConfAddress.172.16.1.1 = IpAddress: 172.16.1.1
RIPv2-MIB::rip2IfConfAddress.172.16.2.1 = IpAddress: 172.16.2.1
RIPv2-MIB::rip2IfConfAddress.172.17.1.1 = IpAddress: 172.17.1.1
RIPv2-MIB::rip2IfConfAddress.172.17.2.1 = IpAddress: 172.17.2.1
$
```

Where to Go Next

For more information about SNMP and SNMP operations, see the "Configuring SNMP Support" chapter of the *Cisco IOS XE Network Management Configuration Guide, Release 2*.

Additional References

The following sections provide references related to RIPv2 Monitoring with SNMP Using the RFC 1724 MIB Extensions.

Related Documents

Related Topic	Document Title
RIP configuration	"Configuring Routing Information Protocol"
RIP commands	*Cisco IOS IP Routing: RIPCommand Reference*
SNMP configuration	"Configuring SNMP Support"
SNMP commands	*Cisco IOS Network Management Command Reference*

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
RIPv2 MIB	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 1724	*RIP Version 2 MIB Extensions*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for RIPv2 Monitoring with SNMP Using the RFC 1724 MIB Extensions

Table 4 lists the release history for this feature.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS XE software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 4 lists only the Cisco IOS XE software release that introduced support for a given feature in a given Cisco IOS XE software release train. Unless noted otherwise, subsequent releases of that Cisco IOS XE software release train also support that feature.

Table 4 Feature Information for RIPv2: RFC 1724 MIB Extensions

Feature Name	Releases	Feature Information
RIPv2: RFC 1724 MIB Extension	Cisco IOS XE Release 2.1	This feature introduces the Cisco IOS XE implementation of RFC 1724, *RIP Version 2 MIB Extensions*. RFC 1724 defines MIB objects that allow the management and limited control of RIPv2 using SNMP. In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Glossary

OID—object identifier, A managed object within the object tree.

SNMP—Simple Network Management Protocol, a protocol used to monitor and manage networking devices.

snmpwalk—An SNMP command to query statistics from a branch in the MIB.

snmpget—An SNMP command to query statistics from a specific OID in the MIB.