IP Routing: RIP Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)

First Published: November 15, 2012

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

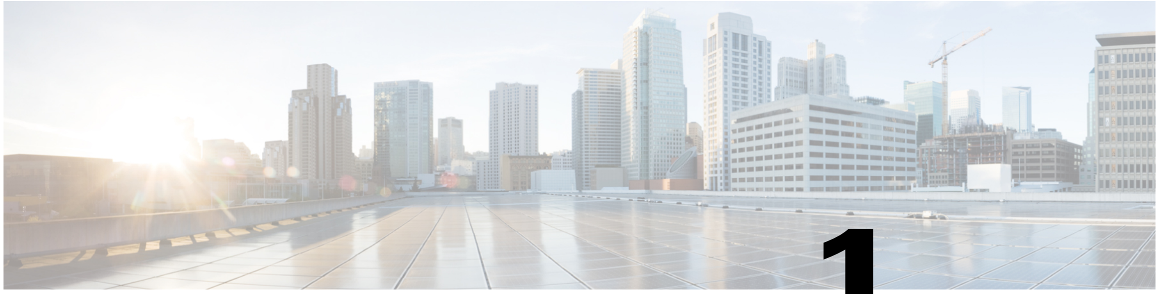
The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

CONTENTS



CHAPTER 1

RIP

RIP is a commonly used routing protocol in small to medium TCP/IP networks. Routing Information Protocol (RIP) is a stable protocol that uses a distance-vector algorithm to calculate routes.

This module describes how to configure RIP.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 table at the end of this module.

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

Prerequisites for RIP

You must configure **ip routing** command before you configure RIP.

Restrictions for RIP

Routing Information Protocol (RIP) uses hop count as the metric to rate the value of different routes. The hop count is the number of devices 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 limited metric range makes RIP unsuitable for large networks.

Information About RIP

RIP Overview

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

A device that is running RIP can receive a default network via an update from another device that is running RIP, or the device can source the default network using RIP. In both cases, the default network is advertised through RIP to other RIP neighbors.

The Cisco implementation of RIP Version 2 (RIPv2) supports plain text and message digest algorithm 5 (MD5) authentication, route summarization, classless interdomain routing (CIDR), and variable-length subnet masks (VLSMs).

RIP Routing Updates

The Routing Information Protocol (RIP) sends routing-update messages at regular intervals and when the network topology changes. When a device receives a RIP routing update that includes changes to an entry, the device updates its routing table to reflect the new route. The metric value for the path is increased by 1, and the sender is indicated as the next hop. RIP devices maintain only the best route (the route with the lowest metric value) to a destination. After updating its routing table, the device immediately begins transmitting RIP routing updates to inform other network devices of the change. These updates are sent independently of the regularly scheduled updates that RIP devices send.

Authentication in RIP

The Cisco implementation of the Routing Information Protocol (RIP) Version 2 (RIPv2) supports authentication, key management, route summarization, classless interdomain routing (CIDR), and variable-length subnet masks (VLSMs).

By default, the software receives RIP Version 1 (RIPv1) and RIPv2 packets, but sends only RIPv1 packets. You can configure the software to receive and send only RIPv1 packets. Alternatively, you can configure the software to receive and send only RIPv2 packets. To override the default behavior, you can configure the RIP version that an interface sends. Similarly, you can also control how packets received from an interface are processed.

RIPv1 does not support authentication. If you are sending and receiving RIP v2 packets, you can enable RIP authentication on an interface.

The key chain determines the set of keys that can be used on the interface. Authentication, including default authentication, is performed on that interface only if a key chain is configured. For more information on key chains and their configuration, see the "Managing Authentication Keys" section in the "Configuring IP Routing Protocol-Independent Features" chapter in the *Cisco IOS IP Routing: Protocol-Independent Configuration Guide*.

Cisco supports two modes of authentication on an interface on which RIP is enabled: plain-text authentication and message digest algorithm 5 (MD5) authentication. Plain-text authentication is the default authentication in every RIPv2 packet.

Note Do not use plain text authentication in RIP packets for security purposes, because the unencrypted authentication key is sent in every RIPv2 packet. Use plain-text authentication when security is not an issue; for example, you can use plain-text authentication to ensure that misconfigured hosts do not participate in routing.

RIP Routing Metric

The Routing Information Protocol (RIP) uses a single routing metric to measure the distance between the source and the destination network. Each hop in a path from the source to the destination is assigned a hop-count value, which is typically 1. When a device receives a routing update that contains a new or changed destination network entry, the device adds 1 to the metric value indicated in the update and enters the network in the routing table. The IP address of the sender is used as the next hop. If an interface network is not specified in the routing table, it will not be advertised in any RIP update.

RIP Versions

The original version of Routing Information Protocol (RIP), is known as RIP Version 1 (RIPv1). The specification of the RIP, defined in RFC 1058, uses classful routing. Periodic routing updates do not support variable length subnet masks (VLSM) because periodic routing updates do not contain subnet information. All subnets in a network class must be of the same size. Because RIP, as per RFC 1058, does not support VLSM, it is not possible to have subnets of varying sizes inside the same network class. This limitation makes RIP vulnerable to attacks.

To rectify the deficiencies of the original RIP specification, RIP Version 2 (RIPv2), as described in RFC 2453, was developed. RIPv2 has the ability to carry subnet information; thus, it supports Classless Inter-Domain Routing (CIDR).

Exchange of Routing Information

Routing Information Protocol (RIP) is normally a broadcast protocol, and for RIP routing updates to reach nonbroadcast networks, you must configure the Cisco software to permit this exchange of 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.

You can use an offset list to increase 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.

Routing protocols use several timers that determine variables such 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 about 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

You can adjust the IP routing support in the Cisco software to enable faster convergence of various IP routing algorithms, and hence, cause quicker fallback to redundant devices. 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 timers that explicitly apply to that address family (or Virtual Routing and Forwarding [VRF]) instance). The **timers-basic** command must be specified for an address family or the system defaults for the **timers-basic** command are used regardless of the timer that 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 the timers are explicitly changed using the **timers-basic** command.

Split Horizon Mechanism

Normally, devices 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. The split horizon mechanism blocks information about routes from being advertised by a device out of any interface from which that information originated. This behavior usually optimizes communications among multiple devices, particularly when links are broken. However, with nonbroadcast networks, such as Frame Relay and the Switched Multimegabit Digital System (SMDS), situations can arise for which this behavior is less than ideal. In such situations, you may want to disable split horizon with the Routing Information Protocol (RIP).

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

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.

Source IP Addresses of RIP Routing Updates

By default, the Cisco software validates the source IP address of incoming Routing Information Protocol (RIP) routing updates. If the source address is not valid, the software discards the routing update. You must disable this functionality if you want to receive updates from a device that is not part of this network. However, disabling this functionality is not recommended under normal circumstances.

Neighbor Router Authentication in RIP

You can prevent your device from receiving fraudulent route updates by configuring neighbor router authentication. When configured, neighbor authentication occurs whenever routing updates are exchanged between neighbor devices. This authentication ensures that a device receives reliable routing information from trusted sources.

Without neighbor authentication, unauthorized or deliberately malicious routing updates could compromise network security. A security compromise could occur if someone diverts or analyzes your network traffic. For example, an unauthorized device could send a fictitious routing update to convince your device to send traffic to an incorrect destination. This diverted traffic could be analyzed to learn confidential information about your organization or merely used to disrupt your organization's ability to effectively communicate using the network. Neighbor authentication prevents any such fraudulent route updates from reaching your device.

When neighbor authentication has been configured on a device, the device authenticates the source of each routing update packet that it receives. This is accomplished by the exchange of an authenticating key (sometimes referred to as a password) that is known to both the sending and receiving devices.

There are two types of neighbor authentication used: plain text authentication and message digest algorithm 5 (MD5) authentication. Both authentication methods work in the same way, with the exception that MD5 sends a message digest (also called a "hash") instead of the authenticating key. The message digest is created using the key and a message, but the key itself is not sent, preventing the message from being read while the message is being transmitted. Plain text authentication sends an authenticating key over the wire.

Note Plain text authentication is not recommended for use as part of your security strategy. Its primary use is to avoid accidental changes to the routing infrastructure. Using MD5 authentication, however, is a recommended security practice.

In plain text authentication, each participating neighbor device must share an authenticating key. This key is specified at each device during configuration. Multiple keys can be specified with some protocols; each key must then be identified by a key number.

In general, when a routing update is sent, the following authentication sequence occurs:

1. A device sends a routing update with a key and the corresponding key number to the neighbor device. In protocols that can have only one key, the key number is always zero. The receiving (neighbor) device checks the received key against the same key stored in its own memory.
    1. If the two keys match, the receiving device accepts the routing update packet. If the two keys do not match, the routing update packet is rejected.

Another form of neighbor device authentication is to configure key management using key chains. When you configure a key chain, you specify a series of keys with lifetimes, and the Cisco software checks each of these keys. This process decreases the likelihood that keys will be compromised. To find the complete configuration information for key chains, refer to the "Configuring IP Routing Protocol-Independent Features" module of the *Cisco IOS IP Routing: Protocol-Independent Configuration Guide*.

How to Configure RIP

Enabling RIP and Configuring RIP Parameters

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router rip**
4. **network** *ip-address*
5. **neighbor** *ip-address*
6. **offset-list** [*access-list-number* | access-list-*name*] {**in** | **out**} *offset* [*interface-type interface-number*]
7. **timers basic** *update invalid holddown flush* [*sleeptime*]
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router rip** **Example:** `Device(config)# router rip`	Enables a RIP routing process and enters router configuration mode.
Step 4	**network** *ip-address* **Example:** `Device(config-router)# network 10.1.1.0`	Associates a network with a RIP routing process.

	Command or Action	Purpose
Step 5	**neighbor** *ip-address* **Example:** `Device(config-router)# neighbor 10.1.1.2`	Defines a neighboring device with which to exchange routing information.
Step 6	**offset-list** [*access-list-number* | access-list-*name*] {**in** | **out**} *offset* [*interface-type interface-number*] **Example:** `Device(config-router)# offset-list 98 in 1 Ethernet 1/0`	(Optional) Applies an offset list to routing metrics.
Step 7	**timers basic** *update invalid holddown flush* [*sleeptime*] **Example:** `Device(config-router)# timers basic 1 2 3 4`	(Optional) Adjusts routing protocol timers.

Step 8	**end**
	Example:
	`Device(config-router)# end`
		Exits router configuration mode and returns to privileged EXEC mode.

Specifying a RIP Version and Enabling Authentication

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router rip**
4. **version** {**1** | **2**}
5. **exit**
6. **interface** *type number*
7. **ip rip send version [1] [2]**
8. **ip rip receive version [1] [2]**
9. **ip rip authentication key-chain** *name-of-chain*
10. **ip rip authentication mode** {**text** | **md5**}
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router rip** **Example:** `Device(config)# router rip`	Enters router configuration mode.

Step 4	**version** {**1** | **2**}
	Example:
	`Device(config-router)# version 2`
		Enables the Cisco software to send only RIP Version 2 (RIPv2) packets.

Step 5	**exit** **Example:** `Device(config-router)# exit`	Exits the router configuration mode and enters the global configuration mode.
Step 6	**interface** *type number* **Example:** `Device(config)# interface Ethernet 3/0`	Specifies an interface and enters interface configuration mode.
Step 7	**ip rip send version [1] [2]** **Example:** `Device(config-if)# ip rip send version 2`	Configures an interface to send only RIPv2 packets.
Step 8	**ip rip receive version [1] [2]** **Example:** `Device(config-if)# ip rip receive version 2`	Configures an interface to accept only RIPv2 packets.

	Command or Action	Purpose
Step 9	**ip rip authentication key-chain** *name-of-chain* **Example:** `Device(config-if)# ip rip authentication key-chain chainname`	Enables RIP authentication.
Step 10	**ip rip authentication mode** {**text** | **md5**} **Example:** `Device(config-if)# ip rip authentication mode md5`	Configures the interface to use message digest algorithm 5 (MD5) authentication (or let it default to plain-text authentication).

Step 11	**end**
	Example:
	`Device(config-if)# end`
		Exits interface configuration mode and returns to privileged EXEC mode.

Managing Split Horizon

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip split-horizon**
5. **no ip split-horizon**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface serial 0/0/0`	Specifies an interface and enters interface configuration mode.
Step 4	**ip split-horizon** **Example:** `Device(config-if)# ip split-horizon`	Enables split horizon.
Step 5	**no ip split-horizon** **Example:** `Device(config-if)# no ip split-horizon`	Disables split horizon.

Step 6	**end**
	Example:
	`Device(config-if)# end`
		Exits interface configuration mode and returns to privileged EXEC mode.

Disabling the Validation of Source IP Addresses

Note We recommend that you do not change the state of the default configuration unless you are certain that your application requires making a change in the configuration 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 devices in any relevant multicast groups on that network.

The summarized network will not be advertised when split horizon is enabled.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip split-horizon**
5. **exit**
6. **router rip**
7. **no validate-update-source**
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface serial 0/0/0`	Enters interface configuration mode.
Step 4	**ip split-horizon** **Example:** `Device(config-if)# ip split-horizon`	Enables split horizon.
Step 5	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode.
Step 6	**router rip** **Example:** `Device(config)# router rip`	Enters router configuration mode.

	Command or Action	Purpose
Step 7	**no validate-update-source** **Example:** `Device(config-router)# no validate-update-source`	Disables the validation of the source IP address of incoming Routing Information Protocol (RIP) routing updates.

Step 8	**end**
	Example:
	`Device(config-router)# end`
		Exits router configuration mode and returns to privileged EXEC mode.

Configuration Examples for RIP

Example: Enabling RIP and Configuring RIP Parameters

```
Device> enable
Device# configure terminal
Device(config)# router rip
Device(config-router)# network 10.1.1.0
Device(config-router)# neighbor 10.1.1.2
Device(config-router)# offset-list 98 in 1 Ethernet 1/0
Device(config-router)# timers basic 1 2 3 4
Device(config-router)# end
```

Example: Specifying a RIP Version and Enabling Authentication

```
Device> enable
Device# configure terminal
Device(config)# router rip
Device(config-router)# version 2
Device(config-router)# exit
Device(config)# interface Ethernet 3/0
Device(config-if)# ip rip send version 2
Device(config-if)# ip rip receive version 2
Device(config-if)# ip rip authentication key-chain chainname
Device(config-if)# ip rip authentication mode md5
Device(config-if)# end
```

Example: Managing Split Horizon

The following example shows how to disable split horizon on a serial link. In this example, the serial link is connected to an X.25 network.

```
Device# configure terminal
```

```
Device(config)# interface Serial 0/0/0
Device(config-if)# no ip split-horizon
Device(config-if)# end
```

The figure below 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 Device C that is connected to a Frame Relay network. In this example, the serial interface on Device C accommodates one of the subnets via the assignment of a secondary IP address.

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

The following example shows how to disable split horizon on serial interfaces. Split horizon must be disabled on Device C for network 172.16.0.0 to be advertised into network 192.168.0.0 and vice versa. These subnets overlap at Device C, interface S0. If split horizon is enabled on serial interface S0, the interface would not advertise a route back into the Frame Relay network for either of these networks.

```
! Configuration for Device 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 Device B
interface gigabitethernet 0/0/0
description - configuration for Device B
 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 Device C
interface gigabitethernet 0/0/0
 ip address 10.20.40.1
!
interface serial serial 0/0/0
 ip address 172.16.1.1
 ip address 192.168.1.1 secondary
 encapsulation frame-relay
 no ip split-horizon
```

Example: Disabling the Validation of Source IP Addresses

```
Device> enable
Device# configure terminal
Device(config)# interface serial 0/0/0
Device(config-if)# ip split-horizon
Device(config-if)# exit
Device(config)# router rip
Device(config-router)# no validate-update-source
Device(config-router)# end
```

Additional References for RIP

Related Documents

Related Topic	Document Title
Cisco IOS Commands	Cisco IOS Master Command List, All Releases
IP Routing: RIP commands	Cisco IOS IP Routing: RIP Command Reference

Standards and RFCs

Standards/RFC	Title
RFC 1058	*Routing Information Protocol*
RFC 2453	*RIP Version 2*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on he Cisco Support and Documentation we site requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for RIP

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 1: Feature Information for RIP

Feature Name	Releases	Feature Information
RIP	Cisco IOS XE Release 2.6 Cisco IOS XE Release 3.2SE	RIP is a commonly used routing protocol in small to medium TCP/IP networks. RIP is a stable protocol that uses a distance-vector algorithm to calculate routes.

CHAPTER 2

Configuring IP Summary Address for RIPv2

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 table at the end of this module.

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

Information About IP Summary Address for RIPv2

RIP Route Summarization

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 Automatic summary is enabled by default.

- 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.

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.

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.

You can verify which routes are summarized for an interface using the **show ip protocols** EXEC command. 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. To display summary address entries in the RIP routing database entries if there are relevant routes being summarized based upon a summary address, use the **show ip rip database** command in EXEC mode. When the last child route for a summary address becomes invalid, the summary address is also removed from the routing table.

Authentication in RIP

The Cisco implementation of the Routing Information Protocol (RIP) Version 2 (RIPv2) supports authentication, key management, route summarization, classless interdomain routing (CIDR), and variable-length subnet masks (VLSMs).

By default, the software receives RIP Version 1 (RIPv1) and RIPv2 packets, but sends only RIPv1 packets. You can configure the software to receive and send only RIPv1 packets. Alternatively, you can configure the software to receive and send only RIPv2 packets. To override the default behavior, you can configure the RIP version that an interface sends. Similarly, you can also control how packets received from an interface are processed.

RIPv1 does not support authentication. If you are sending and receiving RIP v2 packets, you can enable RIP authentication on an interface.

The key chain determines the set of keys that can be used on the interface. Authentication, including default authentication, is performed on that interface only if a key chain is configured. For more information on key chains and their configuration, see the “Managing Authentication Keys” section in the “Configuring IP Routing Protocol-Independent Features” chapter in the *Cisco IOS IP Routing: Protocol-Independent Configuration Guide*.

Cisco supports two modes of authentication on an interface on which RIP is enabled: plain-text authentication and message digest algorithm 5 (MD5) authentication. Plain-text authentication is the default authentication in every RIPv2 packet.

Note Do not use plain text authentication in RIP packets for security purposes, because the unencrypted authentication key is sent in every RIPv2 packet. Use plain-text authentication when security is not an issue; for example, you can use plain-text authentication to ensure that misconfigured hosts do not participate in routing.

Source IP Addresses of RIP Routing Updates

By default, the Cisco software validates the source IP address of incoming Routing Information Protocol (RIP) routing updates. If the source address is not valid, the software discards the routing update. You must disable this functionality if you want to receive updates from a device that is not part of this network. However, disabling this functionality is not recommended under normal circumstances.

How to Configure IP Summary Address for RIPv2

Summarizing RIP Routes

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

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 **no auto-summary** command in router configuration mode.

Note 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 supernet summarization is invalid:

```
Router(config)# interface gigabitEthernet 0/0/0
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 network, even if the subnet mask is unique. For example, the following configuration is not permitted:

```
Router(config)# interface gigabitEthernet 0/0/0

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

.
.
.
```

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip summary-address rip** *ip-address network-mask*
5. **exit**
6. **router rip**
7. **no auto-summary**
8. **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.

	Command or Action	Purpose
Step 3	**interface** *type number* **Example:** `Router(config)# interface gigabitEthernet 0/0/0`	Enters the interface configuration mode.
Step 4	**ip summary-address rip** *ip-address network-mask* **Example:** `Router(config-if)# ip summary-address rip 10.2.0.0 255.255.0.0`	Specifies the IP address and network mask that identify the routes to be summarized.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Exits the interface configuration mode.
Step 6	**router rip** **Example:** `Router(config)# router rip`	Enters the router configuration mode.
Step 7	**no auto-summary** **Example:** `Router(config-router)# no auto-summary`	Used in router configuration mode, disables automatic summarization.

Step 8	**end**
	Example:
	`Router(config-router)# end`
		Exits router configuration mode and returns to privileged EXEC mode.

Specifying a RIP Version and Enabling Authentication

Perform this task to specify a RIP version and enable authentication.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router rip**
4. **version** {**1** | **2**}
5. **exit**
6. **interface type number**
7. **ip rip send version [1] [2]**
8. **ip rip receive version [1] [2]**
9. **ip rip authentication key-chain** *name-of-chain*
10. **ip rip authentication mode** {**text** | **md5**}
11. **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	**router rip** **Example:** `Router(config)# router rip`	Enters router configuration mode.

Step 4	**version** {**1** | **2**}
	Example:
	`Router(config-router)# version 1`
		Configures an interface to send only RIP Version 1 packets.

Step 5	**exit** **Example:** `Router(config-router)# exit`	Exits the router configuration mode and enters the global configuration mode.

	Command or Action	Purpose
Step 6	**interface type number** **Example:** `Router(config)# interface gigabitEthernet 0/0/0`	Enters interface configuration mode.
Step 7	**ip rip send version [1] [2]** **Example:** `Router(config-if)# ip rip send version 1`	Configures an interface to send only RIP Version 1 packets.
Step 8	**ip rip receive version [1] [2]** **Example:** `Router(config-if)# ip rip receive version 1`	Configures an interface to accept only RIP Version 1 packets.
Step 9	**ip rip authentication key-chain** *name-of-chain* **Example:** `Router(config-if)# ip rip authentication key-chain chainname`	Enables RIP authentication.
Step 10	**ip rip authentication mode** {**text** | **md5**} **Example:** `Router(config-if)# ip rip authentication mode md5`	Configures the interface to use MD5 digest authentication (or let it default to plain text authentication).

Step 11	**end**
	Example:
	`Router(config-if)# end`
		Exits interface configuration mode and returns to privileged EXEC mode.

Disabling the Validation of Source IP Addresses

Note We recommend that you do not change the state of the default configuration unless you are certain that your application requires making a change in the configuration 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 devices in any relevant multicast groups on that network.

The summarized network will not be advertised when split horizon is enabled.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip split-horizon**
5. **exit**
6. **router rip**
7. **no validate-update-source**
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface serial 0/0/0`	Enters interface configuration mode.
Step 4	**ip split-horizon** **Example:** `Device(config-if)# ip split-horizon`	Enables split horizon.
Step 5	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode.
Step 6	**router rip** **Example:** `Device(config)# router rip`	Enters router configuration mode.

	Command or Action	Purpose
Step 7	**no validate-update-source** **Example:** `Device(config-router)# no validate-update-source`	Disables the validation of the source IP address of incoming Routing Information Protocol (RIP) routing updates.

Step 8	**end**
	Example:
	`Device(config-router)# end`
		Exits router configuration mode and returns to privileged EXEC mode.

Configuring Examples for IP Summary Address for RIPv2

Route Summarization Example

The following example shows how the **ip summary-address rip**router configuration command can be used to configure summarization on an interface. In this example, the subnets 10.1.3.0/25, 10.1.3.128/25, 10.2.1.0/24, 10.2.2.0/24, 10.1.2.0/24 and 10.1.1.0/24 can be summarized as shown below while sending the updates over an interface.

```
Router(config)#interface GigabitEthernet 0/2
Router(config-if)#ip summary-address rip 10.1.0.0 255.255.0.0
Router(config-if)#ip summary-address rip 10.2.0.0 255.255.0.0
Router(config-if)#ip summary-address rip 10.3.0.0 255.255.0.0
```

Additional References for RIP

Related Documents

Related Topic	Document Title
Cisco IOS Commands	Cisco IOS Master Command List, All Releases
IP Routing: RIP commands	Cisco IOS IP Routing: RIP Command Reference

Standards and RFCs

Standards/RFC	Title
RFC 1058	*Routing Information Protocol*

Standards/RFC	Title
RFC 2453	*RIP Version 2*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on he Cisco Support and Documentation we site requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IP Summary Address for RIPv2

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 2: Feature Information for IP Summary Address for RIPv2

Feature Name	Releases	Feature Information
IP Summary Address for RIPv2	12.0(7)T 12.1(3)T 12.1(14) 12.2(2)T 12.2(27)SBB 12.2(33)SRE 15.0(1)M 15.0S	The IP Summary Adddress for RIPv2 feature introduced the ability to summarize 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. The following commands were introduced or modified: **ip summary-address rip**.