CHAPTER 23

Configuring RIP

This chapter describes how to configure the adaptive security appliance to route data, perform authentication, and redistribute routing information, using the Routing Information Protocol (RIP).

The chapter includes the following sections:

Overview

The Routing Information Protocol, or RIP, as it is more commonly called, is one of the most enduring of all routing protocols. RIP has four basic components: routing update process, RIP routing metrics, routing stability, and routing timers. Devices that support RIP send routing-update messages at regular intervals and when the network topology changes. These RIP packets contain information about the networks that the devices can reach, as well as the number of routers or gateways that a packet must travel through to reach the destination address. RIP generates more traffic than OSPF, but is easier to configure.

RIP is a distance-vector routing protocol that uses hop count as the metric for path selection. When RIP is enabled on an interface, the interface exchanges RIP broadcasts with neighboring devices to dynamically learn about and advertise routes.

The adaptive security appliance support both RIP Version 1 and RIP Version 2. RIP Version 1 does not send the subnet mask with the routing update. RIP Version 2 sends the subnet mask with the routing update and supports variable-length subnet masks. Additionally, RIP Version 2 supports neighbor authentication when routing updates are exchanged. This authentication ensures that the adaptive security appliance receives reliable routing information from a trusted source.

RIP has advantages over static routes because the initial configuration is simple, and you do not need to update the configuration when the topology changes. The disadvantage to RIP is that there is more network and processing overhead than static routing.

Routing Update Process

RIP sends routing-update messages at regular intervals and when the network topology changes. When a router receives a routing update that includes changes to an entry, it 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 routers maintain only the best route (the route with the lowest metric value) to a destination. After updating its routing table, the router immediately begins transmitting routing updates to inform other network routers of the change. These updates are sent independently of the regularly scheduled updates that RIP routers send.

RIP Routing Metric

RIP uses a single routing metric (hop count) to measure the distance between the source and a destination network. Each hop in a path from source to destination is assigned a hop count value, which is typically 1. When a router receives a routing update that contains a new or changed destination network entry, the router 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.

RIP Stability Features

RIP prevents routing loops from continuing indefinitely by implementing a limit on the number of hops allowed in a path from the source to a destination. The maximum number of hops in a path is 15. If a router receives a routing update that contains a new or changed entry, and if increasing the metric value by 1 causes the metric to be infinity (that is, 16), the network destination is considered unreachable. The downside of this stability feature is that it limits the maximum diameter of a RIP network to less than 16 hops.

RIP includes a number of other stability features that are common to many routing protocols. These features are designed to provide stability despite potentially rapid changes in network topology. For example, RIP implements the split horizon and hold-down mechanisms to prevent incorrect routing information from being propagated.

RIP Timers

RIP uses numerous timers to regulate its performance. These include a routing-update timer, a route-timeout timer, and a route-flush timer. The routing-update timer clocks the interval between periodic routing updates. Generally, it is set to 30 seconds, with a small random amount of time added whenever the timer is reset. This is done to help prevent congestion, which could result from all routers simultaneously attempting to update their neighbors. Each routing table entry has a route-timeout timer associated with it. When the route-timeout timer expires, the route is marked invalid but is retained in the table until the route-flush timer expires.

Licensing Requirements for RIP

Model	License Requirement
All models	Base License.

Guidelines and Limitations

This section includes the guidelines and limitations for this feature.

Context Mode Guidelines

Supported in single and multiple context mode.

Firewall Mode Guidelines

Supported in routed and transparent mode.

IPv6 Guidelines

Does not support IPv6.

Additional Guidelines

The following information applies to RIP Version 2 only:

- If using neighbor authentication, the authentication key and key ID must be the same on all neighbor devices that provide RIP Version 2 updates to the interface.
- With RIP Version 2, the adaptive security appliance transmits and receives default route updates using the multicast address 224.0.0.9. In passive mode, it receives route updates at that address.
- When RIP Version 2 is configured on an interface, the multicast address 224.0.0.9 is registered on that interface. When a RIP Version 2 configuration is removed from an interface, that multicast address is unregistered.

Limitations

RIP has the following limitations:

- The adaptive security appliance cannot pass RIP updates between interfaces.
- RIP Version 1 does not support variable-length subnet masks.
- RIP has a maximum hop count of 15. A route with a hop count greater than 15 is considered unreachable.
- RIP convergence is relatively slow compared to other routing protocols.
- You can only enable a single RIP process on the adaptive security appliance.

Configuring RIP

This section describes how to enable and restart the RIP process on the adaptive security appliance.

After you have enabled RIP, see the "Customizing RIP" section on page 23-4, to learn how to customize the RIP process on the adaptive security appliance.

Note If you want to redistribute a route by defining which of the routes from the specified routing protocol are allowed to be redistributed into the target routing process, you must first generate a default route. For information, see the "Configuring a Default Static Route" section on page 20-4 and then define a route map. For information, see the "Defining a Route Map" section on page 21-4.

Enabling RIP

You can only enable one RIP routing process on the adaptive security appliance. After you enable the RIP routing process, you must define the interfaces that will participate in that routing process using the **network** command. By default, the adaptive security appliance sends RIP Version 1 updates and accepts RIP Version 1 and Version 2 updates.

To enable the RIP routing process, enter the following command:

Command	Purpose

`router rip`
 	
Example:
`hostname(config)# router rip`
	Starts the RIP routing process and places you in router configuration mode.
	
	Use the **no router rip** command to remove the entire RIP configuration that you have enabled. After the configuration is cleared, you must reconfigure RIP using the **router rip** command.

Customizing RIP

This section describes how to configure RIP and includes the following topics:

Configure the RIP Version

To specify the version of RIP used by the adaptive security appliance, perform the following steps:

Detailed Steps

	Command	Purpose
Step 1	**router rip** **Example:** `hostname(config)# router rip`	Starts the RIP routing process and places you in router configuration mode.

Step 2	**network** *network_address*
	
	Example:
	`hostname(config)# router rip`
	`hostname(config-router)# network 10.0.0.0`
		Specifies the interfaces that will participate in the RIP routing process.
		
		If an interface belongs to a network defined by this command, the interface will participate in the RIP routing process. If an interface does not belong to a network defined by this command, the interface will not send or receive RIP updates.

Step 3	Enter one of the following numbers to customize an interface to participate in RIP routing:	
	version [1 | 2] **Example:** `hostname(config-router):# version [1]`	Specifies the version of RIP used by the adaptive security appliance. You can override this setting on a per-interface basis. In this example, Version 1 is entered.

Configuring Interfaces for RIP

If you have an interface that you do not want to participate in RIP routing, but that is attached to a network that you want advertised, you can configure the network (using a **network** command) that covers the network the interface is attached to, and configure the passive interfaces (using the **passive-interface** command) to prevent that interface from sending RIP. Additionally, you can specify the version of RIP that is used by the adaptive security appliance for updates.

To configure interfaces for RIP, perform the following steps:

Detailed Steps

	Command	Purpose
Step 1	**router rip** **Example:** `hostname(config)# router rip`	Starts the RIP routing process and places you in router configuration mode.

Step 2	**network** *network_address*
	
	Example:
	`hostname(config)# router rip`
	`hostname(config-router)# network 10.0.0.0`
		Specifies the interfaces that will participate in the RIP routing process.
		
		If an interface belongs to a network defined by this command, the interface will participate in the RIP routing process. If an interface does not belong to a network defined by this command, it will not send or receive RIP updates.

Step 3	**passive-interface [default | *if_name*]**
	
	Example:
	`hostname(config-router):#`
	`passive-interface [default]`
		Specifies an interface to operate in passive mode.
		
		Using the **default** keyword causes all interfaces to operate in passive mode. Specifying an interface name sets only that interface to passive mode. In passive mode, RIP routing updates are accepted by, but not sent out of, the specified interface. You can enter this command for each interface that you want to set to passive mode.

Configuring the RIP Send and Receive Version on an Interface

You can override the globally-set version of RIP that the adaptive security appliance uses to send and receive RIP updates on a per-interface basis.

To configure the RIP version for sending and receiving updates, perform the following steps:

Detailed Steps

	Command	Purpose
Step 1	**interface** *phy_if* **Example:** `hostname(config)# interface phy_if`	Enters interface configuration mode for the interface that you are configuring.
Step 2	Do one of the following to send or receive RIP updates on a per-interface basis.	

Command	Purpose
rip send version {[1] [2]} **Example:** `hostname(config-if)# rip send version 1`	Specifies the version of RIP to use when sending RIP updates out of the interface. In this example, Version 1 is selected.
rip receive version {[1] [2]} **Example:** `hostname(config-if)# rip receive version 2`	Specifies the version of RIP advertisements permitted to be received by an interface. In this example, Version 2 is selected. RIP updates received on the interface that do not match the allowed version are dropped.

Configuring Route Summarization

Note RIP Version 1 always uses automatic route summarization. You cannot disable this feature for RIP Version 1. RIP Version 2 uses automatic route summarization by default.

The RIP routing process summarizes on network number boundaries, which can cause routing problems if you have noncontiguous networks.

For example, if you have a router with the networks 192.168.1.0, 192.168.2.0, and 192.168.3.0 connected to it, and those networks all participate in RIP, the RIP routing process creates the summary address 192.168.0.0 for those routes. If an additional router is added to the network with the networks 192.168.10.0 and 192.168.11.0, and those networks participate in RIP, they will also be summarized as 192.168.0.0. To prevent the possibility of traffic being routed to the wrong location, you should disable automatic route summarization on the routers that are creating conflicting summary addresses.

Because RIP Version 1 always uses automatic route summarization, and RIP Version 2 always uses automatic route summarization by default, when configuring automatic route summarization, you only need to disable it.

To disable automatic route summarization, enter the following command:

Detailed Steps

	Command	Purpose
Step 1	**router rip** **Example:** `hostname(config)# router rip`	Enables the RIP routing process and places you in router configuration mode.
Step 2	**no auto-summarize** **Example:** `hostname(config-router):# no auto-summarize`	Disables automatic route summarization.

Filtering Networks in RIP

To filter the networks received in updates, perform the following steps:

Note Before you begin, you must create a standard access list that permits the networks that you want the RIP process to allow in the routing table and denies the networks that you want the RIP process to discard.

Detailed Steps

	Command	Purpose
Step 1	**router rip** **Example:** `hostname(config)# router rip`	Enables the RIP routing process and places you in router configuration mode.

Step 2	**distribute-list** ***acl*** **in [interface** ***if_name*****]**
	distribute-list ***acl*** **out [connected | eigrp | interface** ***if_name*** **| ospf | rip | static]**
	
	Example:
	`hostname(config-router)# distribute-list acl2 in [interface interface1]`
	`hostname(config-router)# distribute-list acl3 out [connected]`
		Filters the networks sent in updates.
		You can specify an interface to apply the filter to only those updates that are received or sent by that interface. You can enter this command for each interface to which you want to apply a filter. If you do not specify an interface name, the filter is applied to all RIP updates.

Redistributing Routes into the RIP Routing Process

You can redistribute routes from the OSPF, EIGRP, static, and connected routing processes into the RIP routing process.

Note Before you begin this procedure, you must create a route-map to further define which routes from the specified routing protocol are redistributed in to the RIP routing process. See Chapter 21, "Defining Route Maps," for more information about creating a route map.

To redistribute a routes into the RIP routing process, enter one of the following commands:

Command	Purpose
Choose one of the following to redistribute the selected route type into the RIP routing process. You must specify the RIP metric values in the **redistribute** command if you do not have a **default-metric** command in the RIP router configuration.	
redistribute connected [metric <*metric-value*> **| transparent] [route-map** <*route-map-name*>**]** **Example:** hostname(config-router): # redistribute connected [metric <*metric-value*> | transparent] [route-map <*route-map-name*>]	Redistributes connected routes into the RIP routing process.
redistribute static [metric {*metric_value* | transparent}] [route-map *map_name*] **Example:** hostname(config-router):# redistribute static [metric {*metric_value* | transparent}] [route-map *map_name*]	Redistributes static routes into the EIGRP routing process.
redistribute ospf *pid* [match {internal | external [1 | 2] | nssa-external [1 | 2]}] [metric {*metric_value* | transparent}] [route-map *map_name*] **Example:** hostname(config-router):# redistribute ospf pid [match {internal | external [1 | 2] | nssa-external [1 | 2]}] [metric {*metric_value* | transparent}] [route-map *map_name*]	Redistributes routes from an OSPF routing process into the RIP routing process.
redistribute eigrp *as-num* [metric {*metric_value* | transparent}] [route-map *map_name*] **Example:** hostname(config-router):# redistribute eigrp *as-num* [metric {metric_value | transparent}] [route-map *map_name*]	Redistributes routes from an EIGRP routing process into the RIP routing process.

Enabling RIP Authentication

Note The adaptive security appliance supports RIP message authentication for RIP Version 2 messages.

RIP route authentication provides MD5 authentication of routing updates from the RIP routing protocol. The MD5 keyed digest in each RIP packet prevents the introduction of unauthorized or false routing messages from unapproved sources.

RIP route authentication is configured on a per-interface basis. All RIP neighbors on interfaces configured for RIP message authentication must be configured with the same authentication mode and key for adjacencies to be established.

Note Before you can enable RIP route authentication, you must enable RIP.

To enable RIP authentication on an interface, perform the following steps:

Detailed Steps

	Command	Purpose
Step 1	**router rip** *as-num* **Example:** `hostname(config)# router rip 2`	Creates the RIP routing process and enters router configuration mode for this RIP process. The *as-num* argument is the autonomous system number of the RIP routing process.
Step 2	**interface** *phy_if* **Example:** `hostname(config)# interface phy_if`	Enters interface configuration mode for the interface on which you are configuring RIP message authentication.
Step 3	**rip authentication mode** {**text** | **md5**} **Example:** `hostname(config-if)# rip authentication mode md5`	Sets the authentication mode. By default, text authentication is used. We recommend that you use MD5 authentication.
Step 4	**rip authentication key** *key* **key-id** *key-id* **Example:** `hostname(config-if)# rip authentication key cisco key-id 200`	Configures the authentication key used by the MD5 algorithm. The *key* argument can include up to 16 characters. The *key-id* argument is a number from 0 to 255.

. Restarting the RIP Process

To remove the entire RIP configuration, enter the following command:

Command	Purpose
clear rip *pid* {**process** | **redistribution** | **counters** [**neighbor** [*neighbor-interface*] [*neighbor-id*]]} **Example:** `hostname(config)# clear ospf`	Removes the entire RIP configuration that you have enabled. After the configuration is cleared, you must reconfigure RIP again using the **router rip** command.

Monitoring RIP

We recommend that you only use the **debug** commands to troubleshoot specific problems or during troubleshooting sessions with Cisco TAC.

Debugging output is assigned high priority in the CPU process and can render the adaptive security appliance unusable. It is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect performance. For examples and descriptions of the command output, see the *Cisco ASA 5500 Series Command Reference*.

To monitor or debug various RIP routing statistics, enter one of the following commands:

Command	Purpose
Monitoring RIP Routing	
show rip database	Display the contents of the RIP routing database.
show running-config router rip	Displays the RIP commands.
Debugging RIP	
debug rip events	Displays RIP processing events.
debug rip database	Displays RIP database events.

Configuration Example for RIP

The following example shows how to enable and configure RIP with various optional processes:

Step 1 Enable RIP:

```
hostname(config)# router rip 2
```

Step 2 Configure a default route into RIP:

```
hostname(config-router)# default-information originate
```

Step 3 Specify the version of RIP to use:

```
hostname(config-router)# version [1]
```

Step 4 Specify the interfaces that will participate in the RIP routing process:

```
hostname(config-router)# network 225.25.25.225
```

Step 5 Specify an interface to operate in passive mode:

```
hostname(config-router)# passive-interface [default]
```

Step 6 Redistribute a connected route into the RIP routing process:

```
hostname(config-router)# redistribute connected [metric bandwidth delay reliability
loading mtu] [route-map map_name]
```

Feature History for RIP

Table 23-1 lists each feature change and the platform release in which it was implemented.

Table 23-1 Feature History for RIP

Feature Name	Releases	Feature Information
RIP Support	7.0(1)	Support for routing data, performing authentication, and redistributing and monitoring routing information using the Routing Information Protocol (RIP). The **route rip** command was introduced. The **route rip** command is introduced to route data, perform authentication, redistribute and monitor routing information, using the Routing Information Protocol (RIP).