Configuring RIP

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

This chapter includes the following sections:

Information About RIP

This section includes the following topics:

- Routing Update Process
- RIP Routing Metric
- RIP Stability Features
- RIP Timers

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 include 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 ASA supports 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 ASA 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 in 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 context mode only.

Firewall Mode Guidelines

Supported in routed and transparent firewall 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 ASA 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 ASA 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 ASA.

Configuring RIP

Enabling RIP

You can only enable one RIP routing process on the ASA. After you enable the RIP routing process, you must define the interfaces that will participate in that routing process using the **network** command.

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.

CLI

Procedure

	Command or Action	Purpose
Step 1	**router rip** **Example:** `ciscoasa(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.
Step 2	**network network_address** *network_address* **Example:** `ciscoasa(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.

ASDM

Step 1 In the main Adaptive Security Device Manager (ASDM) window, choose **Configuration** > **Device Setup** > **Routing** > **RIP** > **Setup**.

The main RIP Setup pane appears.

From this pane, you can perform the following tasks:

- Enable Auto-summarization. See the "Configuring Route Summarization" section
- Enable RIP version. See the "Configuring the RIP Version" section
- Enable default information origination.

- Define an IP Address for a Network to Add. See the "Filtering Networks in RIP" section
- Configure an Interface. See the "Configuring Passive Interfaces for RIP" section

Step 2 Check the **Enable RIP routing** check box.

After the Enable RIP routing box has been checked, you can enable RIP on the ASA and configure global RIP protocol parameters. You can only enable a single RIP process on the ASA. When you enable RIP, it is enabled on all interfaces. Checking this check box also enables the other fields in this pane. Uncheck this check box to disable RIP routing on the ASA.

Step 3 Click **Apply**.

Configuring the RIP Version

By default, the ASA sends RIP Version 1 updates and accepts RIP Version 1 and Version 2 updates. To specify the version of RIP used by the ASA, perform the following steps.

CLI

Procedure

	Command or Action	Purpose
Step 1	**router rip** **Example:** `ciscoasa(config)# router rip`	Enters router configuration mode.

Step 2	**version {1 | 2}**
	Example:
	`ciscoasa(config-router)# version 2`
		Specifies the version of RIP used by the ASA. Version 1 specifies that the ASA only sends and receives RIP Version 1 updates. Any Version 2 updates received are dropped. Version 2 specifies that the ASA only sends and receives RIP Version 2 updates. Any Version 1 updates received are dropped.
		You can override this setting on a per-interface basis.

ASDM

Step 1 In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **RIP** > **Setup**.

Step 2 Check the **Enable RIP version** check box.

Checking this check box specifies the version of RIP used by the ASA. If this check box is unchecked, then the ASA sends RIP Version 1 updates and accepts RIP Version 1 and Version 2 updates. This setting can be overridden on a per-interface basis in the Interface pane. Indicate the version of RIP to be used by choosing one of the following:

- Version 1, which specifies that the ASA only sends and receives RIP Version 1 updates. Any Version 2 updates received are dropped.

- Version 2, which specifies that the ASA only sends and receives RIP Version 2 updates. Any Version 1 updates received are dropped.

Step 3 Click **Apply**.

Configuring Passive Interfaces for RIP

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

CLI

Procedure

	Command or Action	Purpose
Step 1	**router rip** **Example:** `ciscoasa(config)# router rip`	Enters router configuration mode.
Step 2	**passive-interface** [**default** | *if_name*] **Example:** `ciscoasa(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.

ASDM

Step 1 In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **RIP** > **Setup**.

Step 2 In the Passive Interfaces area, check the check box in the Passive column for those interfaces that youwant to have operate in passive mode. The other interfaces will still send and receive RIP broadcasts.

Note Individual interfaces can be made passive only if the global passive mode is not enabled. Uncheck the **Global Passive** check box to make individual interfaces passive using the Passive Interfaces table.

Step 3 Click **Apply**.

Configuring the RIP Send and Receive Version on an Interface

You can override the globally-set version of RIP that the ASA 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:

CLI

Procedure

	Command or Action	Purpose
Step 1	**interface** *phy_if* **Example:** `ciscoasa(config)# interface phy_if`	Enters interface configuration mode for the interface that you are configuring.

Step 2	**rip send version** {[**1**] [**2**]}
	Example:
	`ciscoasa(config-if)# rip send version 1`
		Specifies the version of RIP to use when sending RIP updates out of the interface.

Step 3	**rip receive version** {[**1**] [**2**]}
	Example:
	`ciscoasa(config-if)# rip receive version 2`
		Specifies the version of RIP advertisements permitted to be received by an interface. RIP updates received on the interface that do not match the allowed version are dropped.

ASDM

Step 1 In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **RIP** > **Setup**.

Step 2 Choose **Configuration** > **Device Setup** > **Routing** > **RIP** > **Interfaces**.

Step 3 Click **Edit**.

The Edit RIP Interface Entry dialog box appears, which allows you to configure the interface-specific RIP settings for sending and receiving.

Step 4 In the Send Version area, check the **Override global send version** check box to specify the RIP versionsent by the interface. Choose one of the following:

- Version 1
- Version 2
- Version 1 & 2

Unchecking this check box restores the global setting.

Step 5 In the Receive Version area, check the **Override global receive version** check box to specify the RIP version accepted by the interface. If a RIP updated from an unsupported version of RIP is received by the interface, it is dropped. Choose one of from the following:

- Version 1

- Version 2
- Version 1 & 2

Unchecking this check box restores the global setting.

Step 6 Click **Apply**.

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.

CLI

Procedure

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

ASDM

Step 1 In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **RIP** > **Setup**.

Step 2 Check the **Enable Auto-Summarization** check box.

Uncheck this check box to disable automatic route summarization. Check this check box to reenable automatic route summarization. RIP Version 1 always uses automatic summarization. You cannot disable automatic route summarization for RIP Version 1. If you are using RIP Version 2, you can turn off automatic route summarization by unchecking this check box. Disable automatic route summarization if you must perform routing between disconnected subnets. When automatic route summarization is disabled, subnets are advertised.

Step 3 Click **Apply**.

Filtering Networks in RIP

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

Note Before you begin, you must create a standard ACL 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.

CLI

Procedure

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

Step 2	**distribute-list***acl***in** [**interfaces** *if_name*] **distribute-list***acl***out** [**connected** | **eigrp** | **interface** *if_name* | **ospf** | **rip** | **static**]
	Example:
	`ciscoasa(config-router)# distribute-list acl2 in [interface interface1]`
	`ciscoasa(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.

ASDM

Step 1 In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **RIP** > **Setup**.

Step 2 Choose **Configuration** > **Device Setup** > **Routing** > **RIP** > **Filter Rules**.

Step 3 Click **Add** or **Edit**.

The Add or Edit Filter Rule dialog box appears, which allows you to create or edit filter rules that apply to all interfaces or to a specific interface.

Step 4 From the Direction drop-down list, choose the direction in which the filter should act.

Choosing In filters networks on incoming RIP updates. Additionally, only the Interface drop-down list is visible.

If you choose Out as the filter direction, skip to Step 8.

Step 5 Choose the Interface type from the Interface drop-down list.

This setting allows you to choose a specific interface for the filter rule, or you can choose the All Interfaces option to apply the filter to all interfaces.

Step 6 (Optional) Add a network rule by clicking **Add**.

The Network Rule dialog box appears.

Step 7 Choose the action from the Action drop-down list. The default is Permit.

- Choose Permit if the specified network is not filtered from incoming or outgoing RIP advertisements.
- Choose Deny if the specified network is to be filtered from incoming or outgoing RIP advertisements.

Step 8 Enter the IP address for the network being filtered, if different than what is displayed, in the IP Address field.

By default, the IP Address field displays the IP Address for the network being filtered.

Step 9 Enter the netmask, if different than what is displayed, in the Netmask field.

By default, the Netmask field displays the network mask applied to the IP address.

Step 10 Click **OK**.

Step 11 Choose Out to filter networks from outgoing RIP updates. Additionally, the Interface and Routing Process drop-down list becomes visible.

- Click the **Interface** radio button to choose a specific interface for the filter rule from the Interface drop-down list, or click the **All Interfaces** option to apply the filter to all interfaces.
- Click the **Routing Process** radio button to activate the Routing process drop-down list. Choose from the following routing process types:

  – connected

  – static

  – OSPF

  – RIP

  – EIGRP

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.

CLI

Procedure

	Command or Action	Purpose
Step 1	**redistribute connected** [**metric** *metric-value* | **transparent**] [**route-map** *route-map-name*] **Example:** `ciscoasa(config-router): # redistribute connected [metric metric-value | transparent] [route-map route-map-name]`	Redistributes connected routes 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.
Step 2	**redistribute static** [**metric** {*metric_value* | **transparent**}] [**route-map** *map_name*] **Example:** `ciscoasa(config-router):# redistribute static [metric {metric_value | transparent}] [route-map map_name]`	Redistributes static routes into the EIGRP routing process.
Step 3	**redistribute ospf** *pid* [**match** {**internal** | **external** [**1 | 2**] | **nssa-external** [**1 | 2**] }] [**metric** {*metric_value* | **transparent**}] [**route-map** *map_name*] **Example:** `ciscoasa(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.
Step 4	**redistribute eigrp** *as-num* [**metric** {*metric_value* | **transparent**}] [**route-map** *map_name*] **Example:** `ciscoasa(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.

ASDM

Step 1 In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **RIP** > **Redistribution**.

The Redistribution pane displays the routes that are being redistributed from other routing processes into the RIP routing process.

Step 2 Click **Add** or **Edit**.

If you clicked **Add**, the Add Route Redistribution dialog box allows you to add a new redistribution rule.

If you clicked **Edit**, the Edit Route Redistribution dialog box allows you to change an existing rule.

Step 3 In the Protocol area, choose the routing protocol to redistribute into the RIP routing process:

- Static, for static routes.
- Connected, for directly connected networks.
- OSPF and OSPF ID, for routes discovered by the OSPF routing process. If you choose OSPF, you must also enter the OSPF process ID. Additionally, you can select the specific types of OSPF routes to redistribute from the Match area.
- EIGRP and EIGRP ID, for routes discovered by the EIGRP routing process. If you choose EIGRP, you must also specify the autonomous system number of the EIGRP routing process in the EIGRP ID field.

Step 4 In the Metrics area, check the **Configure Metric Type** check box to specify a metric for the redistributed routes. If not specified, the routes are assigned a default metric of 0. When the check box is checked, choose from one of the following available values:

- **Transparent** to cause the current route metric to be used.
- **Value** to assign a specific metric value. Valid values range from 0 to 16.

Step 5 In the Optional area, choose the route map from the Route Map drop-down list. This route map specifies the name of a route map that must be specified before the route can be redistributed into the RIP routing process. Click **Manage** to configure a specific route map.

Step 6 In the Match area, choose specific types of OSPF routes to redistribute by checking the check box next to the route type. This area is not active unless OSPF has been chosen in the Protocol area.

If you do not check any route types, Internal, External 1, and External 2 routes are redistributed by default. The Match types are:

- Internal, in which routes internal to the AS are redistributed.
- External 1, in which Type 1 routes external to the AS are redistributed.
- External 2, in which Type 2 routes external to the AS are redistributed.
- NSSA External 1, in which Type 1 routes external to an NSSA are redistributed.
- NSSA External 2, in which Type 2 routes external to an NSSA are redistributed.

Step 7 Click **OK**.

Enabling RIP Authentication

Note The ASA 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.

CLI

Procedure

	Command or Action	Purpose
Step 1	**router rip** *as-num* **Example:** `ciscoasa(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:** `ciscoasa(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:
	`ciscoasa(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:** `ciscoasa(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.

ASDM

Step 1 Choose **Configuration** > **Device Setup** > **Routing** > **RIP** > **Interface**.

Step 2 Click **Edit**.

The Edit RIP Interface Entry dialog box appears, which allows you to configure the interface-specific RIP settings.

Step 3 In the Authentication area, check the **Enable Authentication** check box to enable RIP authentication. Uncheck this check box to disable RIP authentication.

Step 4 In the Key field, enter the key used by the authentication method. This entry can include up to 16 characters.

Step 5 In the Key ID field, enter the key ID. Valid values range from 0 to 255.

Step 6 Choose the type of authentication mode that you want to use by clicking one of the following options:

- **MD5** to use MD5 for RIP message authentication.
- **cleartext** to use cleartext for RIP message authentication (not recommended).

Step 7 Click **Apply**.

Restarting the RIP Process

To remove the entire RIP configuration, enter the following commandperform the following steps:

CLI

Procedure

	Command or Action	Purpose

Step 1	**clear rip** *pid* { **process** | **redistribution** | **counters** [**neighbor** [*neighbor-interface*] [*neighbor-id*]] }
	Example:
	`ciscoasa(config)# clear rip`
		Removes the entire RIP configuration that you have enabled. After the configuration is cleared, you must reconfigure RIP again using the **router rip** command.

ASDM

Step 1 In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **RIP** > **Setup**.

Step 2 Click **Reset**.

Monitoring RIP

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

Debugging output is assigned high priority in the CPU process and can render the ASA 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 command reference.

CLI

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

- **Monitoring RIP Routing:**
  - **show rip database**— Display the contents of the RIP routing database.
  - **show running-config router rip**— Displays the RIP commands.
  - **show route cluster**— Displays additional route synchronization details for clustering.

- **Debugging RIP:**
  - **debug rip events**— Displays RIP processing events.
  - **debug rip database**— Displays RIP database events.
  - **debug rip database**— Enables RIB table replication trace messages to determine if the RIB is correctly synchronized to the slave units in clustering.

ASDM

To monitor or display various RIP routing statistics in ASDM, perform the following steps:

Step 1 In the main ASDM window, choose **Monitoring** > **Routing** > **Routes**.

Step 2 From this pane, you can choose to monitor the following:

- **IPv4**
- **IPv6**
- **Both**

Configuration Example for RIP

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

```
ciscoasa(config)# router rip 2
ciscoasa(config-router)# default-information originate
ciscoasa(config-router)# version [1]
ciscoasa(config-router)# network 225.25.25.225
ciscoasa(config-router)# passive-interface [default]
ciscoasa(config-router)# redistribute connected [metric bandwidth delay reliability
loading mtu][route-mapmap_name]
```

Step 1 In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **RIP** > **Setup**.

Step 2 Check the **Enable RIP routing** check box and click **Apply**.

Step 3 Check the **Enable default information originate** check box.

Step 4 Check the **Enable RIP version** check box and choose **Version 1**.

Step 5 In the Networks area, enter **225.25.24.225** in the IP Network to Add field.

Step 6 In the Passive Interface area, click the check box next to the interface that you want to be passive in the Passive Interfaces table.

Step 7 Click **Apply**.

Step 8 Choose **Configuration** > **Device Setup** > **Routing** > **RIP** > **Redistribution**.

Step 9 Click **Edit**.

Step 10 In the Protocol area, choose **Connected**.

Step 11 In the Metric area, check the **Configure Metric Type** check box and choose **Transparent Mode** (default).

Step 12 In the Optional area, choose a route map from the Route Map drop-down list.

Step 13 Click **Manage** to configure a specific route map.

Step 14 Click **OK**.

Feature History for RIP

Table 1-1 lists each feature change and the platform release in which it was implemented. ASDM is backward-compatible with multiple platform releases, so the specific ASDM release in which support was added is not listed.

Table 1: Feature History for RIP

Feature Name	Releases	Feature Information
RIP support	7.0(1)	Support was added for routing data, performing authentication, and redistributing and monitoring routing information using the Routing Information Protocol (RIP). We introduced the **route rip** command. We introduced the following screen: Configuration > Device Setup > Routing > RIP.
Clustering	9.0(1)	For RIP, bulk synchronization, route synchronization, and layer 2 load balancing are supported in the clustering environment. We introduced or modified the following commands: **show route cluster, debug route cluster, show mfib cluster, debug mfib cluster**.