17

IP Configuration: RIPv2

This section describes the Routing Information Protocol (RIP) version 2 feature.

It covers the following topics:

- **Overview**
- **How Rip Operates on the Device**
- **Configuring RIP**
- **Access Lists**

Overview

Routing Information Protocol (RIP) is an implementation of a distance-vector protocol for local and wide-area networks. It classifies routers as either *active* or *passive* (silent). Active routers advertise their routes to others; passive routers listen and update their routes based on advertisements, but do not advertise. Typically, routers run RIP in active mode, while hosts use passive mode.

The default gateway is a static route and it is advertised by RIP in the same way as all other static routers, if it is enabled by configuration.

When IP Routing is enabled, RIP works fully. When IP Routing is disabled, RIP works in the passive mode, meaning that it only learns routes from the received RIP messages and does not send them.

NOTE To enable IP Routing, go to the **IPv4 Interface** page.

The device supports RIP version 2, which is based on the following standards:

- RFC2453 RIP Version 2, November 1998
- RFC2082 RIP-2 MD5 Authentication, January 1997
- RFC1724 RIP Version 2 MIB Extension

Received RIPv1 packets are dropped.

How Rip Operates on the Device

The following section describes enabling, offset configuration, passive mode, authentication, statistical counters, and peers database of RIP.

Enabling RIP

Enabling RIP

- RIP must be enabled globally and per interface.
- RIP can only be configured if it is enabled.
- Disabling RIP globally deletes the RIP configuration on the system.
- Disabling RIP on an interface deletes the RIP configuration on the specified interface.
- If IP Routing is disabled, RIP messages are not sent, although when RIP messages are received, they are used to update the routing table information.

NOTE RIP can only be defined on manually-configured IP interfaces, meaning that RIP cannot be defined on an interface whose IP address was received from a DHCP server or whose IP address is the default IP address.

Offset Configuration

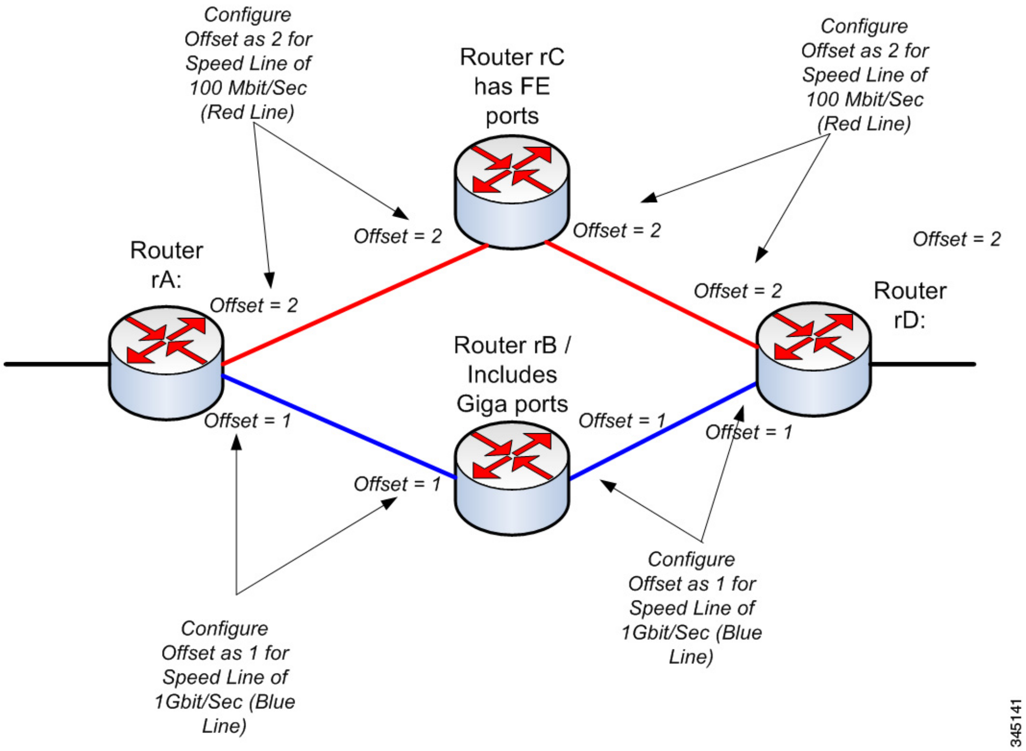
A RIP message includes a metric (number of hops) for each route.

An offset is an additional number that is added to a metric to affect the cost of paths. The offset is set per interface and, for example, can reflect the speed, delay, or some other quality of that particular interface. In this way, the relative cost of the interfaces can be adjusted as desired.

It is your responsibility to set the offset for each interface (1 by default).

The following illustrates the configuration of the metric offset for various interfaces, based on port speed.

Configuring the Offset (Based on Port Speed)


Configure Offset as 2 for Speed Line of 100 Mbit/Sec (Red Line)
Router rC has FE ports
Configure Offset as 2 for Speed Line of 100 Mbit/Sec (Red Line)
Offset = 2
Offset = 2
Offset = 2
Router rA:
Offset = 2
Offset = 2
Router rD:
Router rB / Includes Giga ports
Offset = 1
Offset = 1
Offset = 1
Offset = 1
Configure Offset as 1 for Speed Line of 1Gbit/Sec (Blue Line)
Configure Offset as 1 for Speed Line of 1Gbit/Sec (Blue Line)
345141

Router rD can send data to rA via rB or rC. Since rC only supports Fast Ethernet (FE) ports, and rB supports Gigabit Ethernet (GE) ports, the path cost from router rD to router rA is higher via router rC (additional 4 to the cost path) as opposed to the path via router rB (additional 2 to the cost path), Therefore, forwarding traffic via routing rB is preferred. To achieve this, you configure a different offset (metric value) on each interface based on its line speed.

See **Offset Configuration** for more information.

Passive Mode

Transmission of routing update messages over a specific IP interface can be disabled. In this case, the router is passive, and only receives the updated RIP information on this interface. By default, transmission of routing updates on an IP interface is enabled.

See **RIPv2 Settings** for more information.

Filtering Routing Updates

You can filter incoming and outgoing routes for a given IP interface using two Standard Access Lists - one for input and one for output.

The Standard Access List is a named, ordered list of pairs of IP prefix (IP address and IP mask length) and action. The action can be deny or permit.

If an access list is defined, each route from the RIP message is checked against the list starting from the first pair: if it matches the first pair and the action is permit, the route is passed; if the action is deny, the route is not passed. If the route does not match, the following pair is considered.

If there is no pair that the route matches, the deny action is applied.

Advertising Default Route Entries on IP Interfaces

The special address 0.0.0.0 is used for describing a default route. A default route is used to avoid listing every possible network in the routing updates, when one or more closely-connected routers in the system are prepared to transfer traffic to the networks that are not listed explicitly. These routers create RIP entries for the address 0.0.0.0, just as if it were a network to which they are connected.

You can enable the default route advertisement and configure it with a given metric.

Redistribution Feature

The following type of routes exist and can be distributed by RIP:

- **Connected—**RIP routes that correspond to defined IP interfaces on which RIP is not enabled (defined locally). By default, the RIP Routing Table only includes routes that correspond to IP interfaces on which RIP is enabled.
- **Static—**Manually-defined (remote) routes.

You can determine whether static or connected routes are redistributed by RIP by configuring the **Redistribute Static Route** or **Redistribute Connected Route** feature, respectively.

These feature are disabled by default and can be enabled globally.

If these features are enabled, rejected routes are advertised by routes with a metric of 16.

The route configurations can be propagated using one of the following options:

- **Default Metric**

  Causes RIP to use the predefined default metric value for the propagated route configuration.

- **Transparent** (default)

  Causes RIP to use the routing table metric as the RIP metric for the propagated route configuration.

  This results in the following behavior:

  - If the metric value of a route is equal to or less than 15, this value is used in the RIP protocol when advertising this route.
  - If the metric value of a static route is greater than 15, the route is not advertised to other routers using RIP.

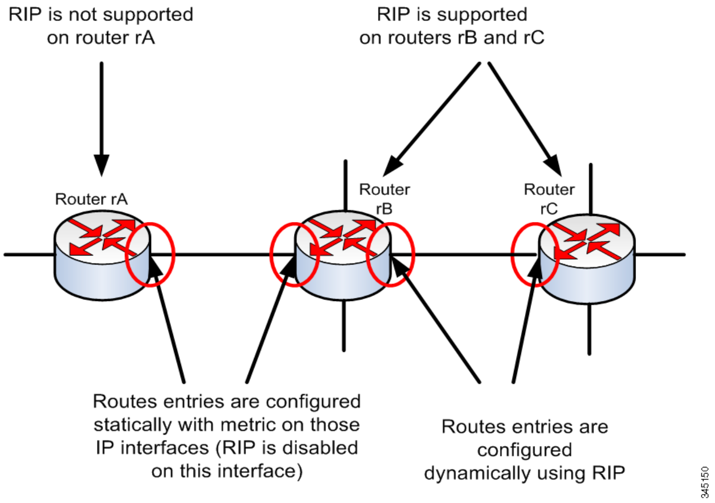
- **User Defined Metric**

  Causes RIP to use the metric value entered by the user.

Using RIP in Network with Non-Rip Devices

Static route configuration and connected interfaces must be taken into account when using RIP. This is shown in the following, which illustrates a network where some routers support RIP and others do not.

A Network with RIP and non-RIP Routers


RIP is not supported on router rA
RIP is supported on routers rB and rC
Router rA
Router rB
Router rC
Routes entries are configured statically with metric on those IP interfaces (RIP is disabled on this interface)
Routes entries are configured dynamically using RIP
345150

Router rA does not support RIP. Therefore, routing entries with an appropriate metric are configured statically on this router. While on router rB the route to router rA is considered a connected route. In contrast, routers rB and rC derive and distribute their routing entries using RIP.

The connected route configuration of router rB, can be propagated to router rC using either the default metric or transparent system. A static/connected route is *redistributed* either with the route's metric (transparent metric) or with the metric defined by the default-metric command.

See **Redistribution Feature** for more information.

RIP Authentication

You can disable authentication of RIP messages per IP interface or enable one of the following types of authentication:

- **Plain text or password**—Uses a key password (string) that is sent along with the route to another router. The receiving router compares this key to its own configured key. If they are the same, it accepts the route.
- **MD5**—Uses MD5 digest authentication. Each router is configured with a set of secret keys. This set is called a **key chain**. Each key chain consists of one or more keys. Each key has an identifying number (**key identifier**), **key string** and optionally, a **send-lifetime** and **accept-lifetime** value. The send-lifetime is the time period during which an authentication key on a key chain is valid to be sent; the accept-lifetime is the time period during which the authentication key on a key chain is received as valid.

  Each transmitted RIP message contains the calculated MD5 digest of the message (containing the key chain), plus the key identifier of the used key string. The receiver also has the key chain configured on it. The key identifier is used by the receiver to select the key for validating the MD5 digest.

RIP Statistical Counters

You can monitor the RIP operation by checking statistical counters per IP interface. See **Displaying RIPv2 Statistic Counters** for a description of these counters.

RIP Peers Database

You can monitor the RIP peers database per IP interface. See **Displaying the RIPv2 Peers Database** for a description of these counters

Configuring RIP

The following actions can be performed.

- Mandatory actions:
    - Globally enable/disable RIP protocol, using the **RIPv2 Properties** page.
    - Enable/disable RIP protocol on an IP interface, using the **RIPv2 Settings** page.
- Optional actions (if these are not performed, default values are used by the system)
    - Enable/disable RIP to advertise static or connected routes and its metric on the IP interface, using the **RIPv2 Properties** page.
    - Configure the offset added to the metric for incoming routes on an IP interface, using the**RIPv2 Settings** page.
    - Enable passive mode on an IP interface, using the **RIPv2 Settings** page.
    - Control which routes are processed in the incoming/outgoing routing updates by specifying an IP address list on the IP interface (see **Access Lists**).
    - Advertise default route entries on the IP interface, using the **RIPv2 Settings** page.
    - Enable RIP authentication on an IP Interface, using the **RIPv2 Settings** page.

RIPv2 Properties

To enable/disable RIP on the device.

STEP 1 Click **IP Configuration** > **IPv4 Management and Interfaces**> **RIPv2 > RIPv2 Properties**.

STEP 2 Select the following options as required:

- **RIP—**The following options are available:
  - *Enable*—Enable RIP.
  - *Disable*—Disable RIP. Disabling RIP deletes the RIP configuration on the system.
  - *Shutdown*—Set the RIP global state to shutdown.
- **RIP Advertisement—**Select to enable sending routing updates on all RIP IP interfaces.
- **Default Route Advertisement—**Select to enable sending the default route to the RIP domain. This route will serve as the default router.
- **Default Metric—**Enter the value of the default metric (refer to **Redistribution Feature**).

STEP 3 **Redistribute Static Route—**Select to enable this feature (described in **Redistribution Feature**.

STEP 4 If **Redistribute Static Route** is enabled, select an option for the **Redistribute Static Metric** field. The following options are available:

- **Default Metric—**Causes RIP to use the default metric value for the propagated static route configuration (refer to **Redistribution Feature**).
- **Transparent—**Causes RIP to use the routing table metric as the RIP metric for the propagated static route configuration. This results in the following behavior:
  - If the metric value of a static route is equal to or less than 15, this value is used in the RIP protocol when advertising this static route.
  - If the metric value of a static route is greater than 15, the static route is not advertised to other routers using RIP.
- **User Defined Metric—**Enter the value of the metric.

STEP 5 **Redistribute Connected Route—**Select to enable this feature (described in Redistributing Static Route Configuration.

STEP 6 If **Redistribute Connected Route** is enabled, select an option for the **Redistribute Connected Metric** field. The following options are available:

- **Default Metric—**Causes RIP to use the default metric value for the propagated static route configuration (refer to **Redistribution Feature**).
- **Transparent—**Causes RIP to use the routing table metric as the RIP metric for the propagated static route configuration. This results in the following behavior:
  - If the metric value of a static route is equal to or less than 15, this value is used in the RIP protocol when advertising this static route.
  - If the metric value of a static route is greater than 15, the static route is not advertised to other routers using RIP.
- **User Defined Metric—**Enter the value of the metric.

STEP 7 Click **Apply**. The settings are written to the Running Configuration file.

RIPv2 Settings

To configure RIP on an IP interface:

STEP 1 Click **IP Configuration** > **RIPv2 > RIPv2 Settings**.

STEP 2 RIP parameters are displayed per IP interface. To add a new IP interface, click **Add** and enter the following fields:

- **IP Address—**Select an IP interface defined on the Layer 2 interface.
- **Shutdown—**Select to enable RIP on the interface even in the shutdown state.
- **Passive—**Specifies whether sending RIP route update messages is allowed on the specified IP interface. If this field is not enabled, RIP updates are not sent (passive).
- **Offset—**Specifies the metric number of the specified IP interface. This reflects the additional cost of using this interface, based on the speed of the interface.

- **Default Route Advertisement**—This option is defined globally in the **RIPv2 Properties** page. You can use the global definition or define this field for the specific interface. The following options are available:
  - *Global*—Use the global settings defined in the **RIPv2 Properties**. screen.
  - *Disable*—On this RIP interface, do not advertise the default route.
  - *Enable*—Advertise the default route on this RIP interface.
- **Default Route Advertisement Metric**—Enter the metric for the default route for this interface.
- **Authentication Mode**—RIP authentication state (enable/disable) on a specified IP interface. The following options are available:
  - *None*—There is no authentication performed.
  - *Text*—The key password entered below is used for authentication.
  - *MD5*—The MD5 digest of the key chain selected below is used for authentication.
- **Key Password**—If **Text** was selected as the authentication type, enter the password to be used.
- **Key Chain**—If **MD5** was selected as the authentication mode, enter the key chain to be digested. This key chain is created as described in the **Key Management** section.

- **Distribute-list In** —Select to configure filtering on RIP incoming routes for the specified IP address(es) in the Access List Name. If this field is enabled, select the Access List Name below:
- **Access List Name**—Select the Access List name (which includes a list of IP addresses)) of RIP incoming routes filtering for a specified IP interface. See **Access List Settings** for a description of access lists.
- **Distribute-list Out**—Select to configure filtering on RIP outgoing routes for the specified IP address(es) in the Access List Name. If this field is enabled, select the Access List Name below:
- **Access List Name**—Select the Access List name (which includes a list of IP addresses)) of RIP outgoing routes filtering for a specified IP interface. See **Access List Settings**for a description of access lists.

STEP 3 Click **Apply**. The settings are written to the Running Configuration file.

Displaying RIPv2 Statistic Counters

To view the RIP statistical counters for each IP address:

STEP 1 Click **IP Configuration** > **RIPv2 > RIPv2 Statistics**.

The following fields are displayed:

- **IP Interface**—IP interface defined on the Layer 2 interface.
- **Bad Packets Received**—Specifies the number of bad packets identified by RIP on the IP interface.
- **Bad Routes Received**—Specifies the number of bad routes received and identified by RIP on the IP interface. Bad routes mean that the route parameters are incorrect. For example, the IP destination is a Broadcast address, or the metric is 0 or greater than 16
- **Update Sent**—Specifies the number of packets sent by RIP on the IP interface.

STEP 2 To clear all interface counters, click **Clear All Interface Counters**.

Displaying the RIPv2 Peers Database

To view the RIP Peers (neighbors) database:

STEP 1 Click **IP Configuration** > **RIPv2 > RIPv2 Peer Router Database**.

The following fields are displayed for the peer router database:

- **Router IP Address—**IP interface defined on the Layer 2 interface.
- **Bad Packets Received—**Specifies the number of bad packets identified by RIP on the IP interface.
- **Bad Routes Received—**Specifies the number of bad routes received and identified by RIP on the IP interface. Bad routes mean that the route parameters are incorrect. For example, the IP destination is a Broadcast, or the metric is 0 or greater than 16
- **Last Updated—**Indicates the last time RIP received RIP routes from the remote IP address.

STEP 2 To clear all counters, click **Clear All Interface Counters**.

Access Lists

See **Filtering Routing Updates** for a description of access lists.

To create access lists, do the following:

1. Create an access list with a single IP address, using the **Access Lists** pages.
2. Add additional IP addresses if required, using the **Source IPv4 Access List** page.

Access List Settings

To set the global configuration of an access list.

STEP 1 Click **IP Configuration** > **IPv4 Management and Interfaces > Access List** > **Access List Settings**.

STEP 2 To add a new Access List, click **Add** to open the Add Access List page and enter the following fields:

- **Name**—Define a name for the access list.
- **Source IPv4 Address**—Enter the source IPv4 address. The following options are available:
  - *Any*—All IP addresses are included.
  - *User Defined*—Enter an IP address.
- **Source IPv4 Mask**—Enter the source IPv4 address mask type and value. The following options are available:
  - *Network Mask*—Enter the network mask.
  - *Prefix Length*—Enter the prefix length.
- **Action**—Select an action for the access list. The following options are available:
  - *Permit*—Permit entry of packets from the IP address(es) in the access list.
  - *Deny*—Reject entry of packets from the IP address(es) in the access list.

STEP 3 Click **Apply**. The settings are written to the Running Configuration file.

Source IPv4 Access List

To populate an access list with IP addresses.

STEP 1 Click **IP Configuration** > > **IPv4 Management and Interfaces > Access List** > **Source IPv4 Address List**.

STEP 2 To modify the parameters of an access list, click **Add** and modify any of the following fields:

- **Access List Name**—Name of the access list.
- **Source IPv4 Address**—Source IPv4 address. The following options are available:
  - *Any*—All IP addresses are included.
  - *User Defined*—Enter an IP address.
- **Source IPv4 Mask**—Source IPv4 address mask type and value. The following options are available:
  - *Network Mask*—Enter the network mask (for example 255.255.0.0).
  - *Prefix Length*—Enter the prefix length.
- **Action**—Action for the access list. The following options are available:
  - *Permit*—Permit entry of packets from the IP address(es) in the access list.
  - *Deny*—Reject entry of packets from the IP address(es) in the access list.