Routing Information Protocol

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.

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 Routing Information Protocol

RIP Overview

The Routing Information Protocol (RIP) Version 1 uses broadcast UDP data packets, and RIPv2 uses multicast packets to exchange the 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.

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.

Neighbor Router Authentication

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

Without neighbor authentication, unauthorized or deliberately malicious routing updates could compromise the security of your network traffic. A security compromise could occur if an unfriendly party diverts or analyzes your network traffic. For example, an unauthorized router could send a fictitious routing update to convince your router 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 being received by your router.

When neighbor authentication has been configured on a router, the router 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 the receiving router.

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

Note Note that 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 router must share an authenticating key. This key is specified at each router 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 router sends a routing update with a key and the corresponding key number to the neighbor router. In protocols that can have only one key, the key number is always zero. The receiving (neighbor) router checks the received key against the same key stored in its own memory.
2. If the two keys match, the receiving router accepts the routing update packet. If the two keys do not match, the routing update packet is rejected.

MD5 authentication works similarly to plain text authentication, except that the key is never sent over the wire. Instead, the router uses the MD5 algorithm to produce a "message digest" of the key (also called a "hash"). The message digest is then sent instead of the key itself. This ensures that nobody can eavesdrop on the line and learn keys during transmission.

Another form of neighbor router 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 IOS software rotates through each of these keys. This decreases the likelihood that keys will be compromised.

How to Configure Routing Information Protocol

Enabling RIP and Configuring RIP Parameters

Procedure

	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.
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	**auto-summary** **Example:** `Device(config-router)# auto-summary`	Restores the default behavior of automatic summarization of subnet routes into network-level routes.
Step 7	**offset-list** [*access-list-number* | access-list-*name*] {**in** | **out**} *offset* [*interface-type interface-number*] **Example:**	(Optional) Applies an offset list to routing metrics.

	Command or Action	Purpose
	`Device(config-router)# offset-list 98 in 1 Ethernet 1/0`	
Step 8	**timers basic** *update invalid holddown flush* [*sleeptime*] **Example:** `Device(config-router)# timers basic 1 2 3 4`	(Optional) Adjusts routing protocol timers.
Step 9	**maximum-paths** *maximum* **Example:** `Device(config-router)# maximum-paths 16`	Configures the maximum number of equal cost parallel routes that RIP will install into the routing table.
Step 10	**distance** *admin-distance* [*prefix prefix-length* | *prefix-mask*] **Example:** `Device(config-router)# distance 85 192.168.10.0/24`	Defines the administrative distance assigned to routes discovered by RIP.
Step 11	**end** **Example:** `Device(config-router)# end`	Exits router configuration mode and returns to privileged EXEC mode.

Specifying a RIP Version and Enabling Authentication

Procedure

	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.

	Command or Action	Purpose
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 GigabitEthernet 0/0`	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.
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.

Configuration Examples for Routing Information Protocol

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)# auto-summary
Device(config-router)# offset-list 98 in 1 GigabitEthernet 1/0
Device(config-router)# timers basic 1 2 3 4
Device(config-router)# maximum-paths 16
Device(config-router)# distance 85 192.168.10.0/24
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 GigabitEthernet 0/0
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
```

Additional References for RIP

Related Documents

Related Topic	Document Title
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 (Routing Information Protocol)	Cisco IOS Release 15.2(5)E2	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.