Contents

1 Configuring RIP

1.1 Introduction

1.1.1 Overview

Routing Information Protocol (RIP) is a unicast routing protocol applied to IPv4 networks. RIP-enabled devices exchange routing information to automatically obtain routes to remote networks.

As an Interior Gateway Protocol (IGP), RIP can run only within an autonomous system (AS). RIP is a distance vector routing protocol, which can control packet interaction through UDP (Port 520) and applies to small-scale networks. Due to simplicity, ease of use, and low workload of configuration and maintenance, the RIP routing protocol is widely used for small networks.

1.1.2 Principles

1. Basic Concepts

- IGP and EGP

  IGP runs within an AS. For example, RIP is a type of IGP.

  Exterior Gateway Protocol (EGP) runs between ASs. For example, BGP is a type of EGP.

- Classful routing protocol and classless routing protocol

  Protocols can be classified based on the type of routes supported:

  Classful routing protocol: It supports classful routes. For example, RIPv1 is a classful routing protocol.

  Classless routing protocol: It supports classless routes. For example, RIPv2 is a classless routing protocol.

- RIP timer
  - Update timer: Route update packets are sent regularly, and the update interval is 30s by default.
  - Invalid timer: If an update packet for refreshing the existing route has not been received after 180s (default value), the metric for the route to set to 16, marking the route as invalid.
  - Flush timer: By default, the flush timer is set to 240s, 60s greater than the invalid timer. When the flush timer times out, the route is deleted from the routing table.
  - Hold-down timer: It prevents route loop caused by route flapping. When the device receives a route update with a metric value of 16, the route will be set to hold-down state, and the hold-down timer will be started at the same time. Before the hold-down timer expires, even if an update packet with a metric less than 16 for this route is received, the route will not be updated.

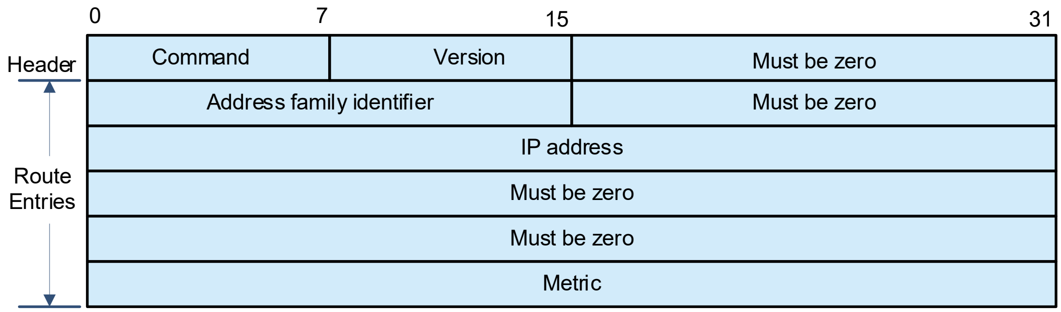
2. RIPv1 and RIPv2

RIP is available in two versions: RIPv1 and RIPv2.

- RIPv1

  RIPv1 packets are broadcast. The broadcast address is 255.255.255.255, and the UDP port ID is 520. No subnet mask is carried in RIPv1 packet, so RIPv1 cannot identify the subnet mask, and supports only classful routes. Meanwhile, RIPv1 does not support routing aggregation and discontinuous subnet.

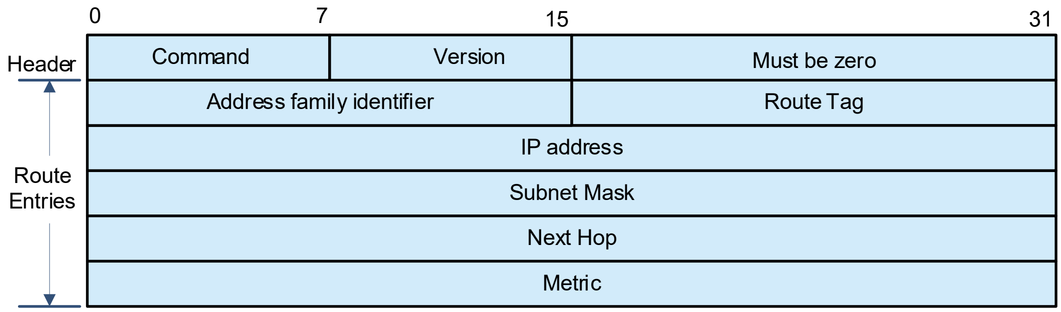
Figure 1-1 RIPv1 Packet Format



- RIPv2

  RIPv2 packets are multicast. The multicast address is 224.0.0.9, and the UDP port ID is 520. RIPv2 can identify the subnet mask, and supports classless routes, summarized route, and supernetting routes. RIPv2 supports plain text authentication and message digest 5 (MD5) authentication. During route redistribution, tags can be added to external routes, and the policy route can control RIP routes according to tags.

Figure 1-2 RIPv2 Packet Format



3. Route Control

Compared with static routing, the dynamic routing protocol shows an advantage, that is, by exchanging routing information, devices can automatically obtain routes to a remote network and update the routes in real time.

- Initialization

After RIP is enabled on a device, the device sends a request packet to its neighbor device, asking for all routing information, that is, the routing table. After receiving the request packet, the neighbor device returns a response packet containing the local routing table. After receiving the response packet, the device updates the local routing table, and sends an update packet to the neighbor device, informing the neighbor device of the route update information. After receiving the update packet, the neighbor device updates the local routing table, and sends the update packet to other adjacent devices. After receiving the update advertisement, all devices can obtain and retain the latest routing information.

- Periodical update

  By default, periodical update is enabled for RIP. Adjacent devices exchange complete routing information with each other every 30s, that is, the entire routing table is sent to neighbor devices. One update packet contains at most 25 routes. Therefore, a lot of update packets may be required to send the entire routing table. You can set the sending delay between update packets to avoid loss of routing information.

Note

For every non-local route, if the route is not updated within 180s (Invalid timer), the metric of the route is changed to 16 (unreachable). If the route is still not updated in the next 120s (Flush timer), the route is deleted from the routing table.

- Triggered update

  After the triggered update function is enabled, periodical update is automatically disabled. When routing information changes on a device, the device immediately sends routes related to the change (instead of the complete routing table) to the neighbor device, and use the acknowledgment and retransmission mechanisms to ensure that the neighbor device receives the routes successfully. Compared with periodical update, triggered update helps reduce flooding and accelerates route convergence.

  Events that can trigger update include router startup, interface status change, changes in routing information (such as the metric), and reception of a request packet.

- Route summarization

  When sending routing information to a neighbor device, the RIP-enabled device summarizes subnet routes that belong to the same classful network into a route, and sends the route to the neighbor device. For example, summarize 80.1.1.0/24 (metric = 2) and 80.1.2.0/24 (metric = 3) into 80.0.0.0/8 (metric = 2).

  You can manually specify the aggregation address to summarize routes into a classless route. For example, summarize 80.1.1.0/24 (metric = 2) and 80.1.2.0/24 (metric = 3) into 80.1.0.0/16 (metric = 2).

Note

Only RIPv2 supports route summarization. Route summarization can reduce the size of the routing table and improve the efficiency of routing information exchange. The best metric is selected for the summarized route.

- Supernetting route

If the subnet mask length of a route is smaller than the natural mask length, this route is called supernetting route. For example, 80.0.0.0/6. As 80.0.0.0 is a Class A network address and the natural mask is 8 bits, 80.0.0.0/6 route is a supernetting route.

Note

Only RIPv2 supports supernetting routes.

- Default route

  In the routing table, a route to the destination network 0.0.0.0/0 is called default route.

  The default route can be learned from a neighbor device, or sent to a neighbor device.

- Route redistribution

  For RIP, other types of routes (such as direct routes, static routes, and routes of other routing protocols) are called external routes.

  External routes (excluding the default route) can be redistributed to RIP and advertised to neighbors.

- Route filtering

  Filtering conditions can be configured to limit the routing information exchanged between adjacent routers. Only the routing information that meets filtering conditions can be sent or received.

4. Routing Algorithm

RIP is a protocol based on the distance-vector algorithm. It uses the vector addition method to compute the routing information.

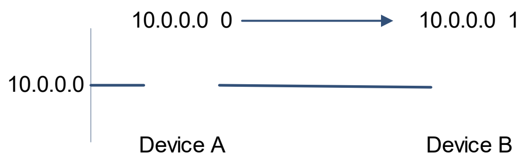
- Distance-vector algorithm

  RIP is a protocol based on the distance-vector algorithm. The distance-vector algorithm treats a route as a vector that consists of the destination network and distance. The device obtains a route from its neighbor and adds the distance vector from itself to the neighbor to the route to form its own route.

  RIP uses the hop count to evaluate the distance to the destination network. By default, the hop count from a device to its directly connected network is 0, the hop count from a device to a network that can be reached through a device is 1, and so on. That is, the metric is equal to the number of devices from the local network to the destination network. To restrict the convergence time, RIP stipulates that the metric must be an integer in the range from 0 to 15. If the metric is equal to or greater than 16, the destination network or host is unreachable. For this reason, RIP cannot be applied to a large-scale network.

  As shown in Figure 1-1, Device A is connected to the network 10.0.0.0. Device B obtains the route (10.0.0.0,0) from Device A and adds the metric 1 to the route to obtain its own route (10.0.0.0,1), and the next hop points to Device A.

Figure 1-1 Diagram of RIP Distance-Vector Algorithm

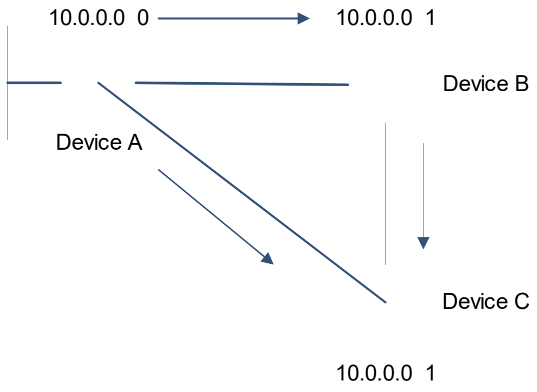


- Selecting the optimum route

RIP selects an optimum route based on the following principle: If multiple routes to the same destination network is available, a device preferentially selects the route with the smallest metric.

As shown in Figure 1-2, Device A is connected to the network 10.0.0.0. Device C obtains the route (10.0.0.0,0) from Device A and the route (10.0.0.0,1) from Device B. Device C will select the route that is obtained from Device A and add metric 1 to this route to form its own route (10.0.0.0,1), and the next hop points to Device A.

Figure 1-2 Diagram of Selecting the Optimum Route



Note

When routes coming from different sources exist on a device, the route with the smaller distance is preferentially selected.

Table 1-1 Default Distance of Routing Protocol

Route Source	Default Distance
Directly-connected network	0
Static route	1
OSPF route	110

Route Source	Default Distance
IS-IS route	115
RIP route	120
Unreachable route	255

5. Avoiding Route Loops

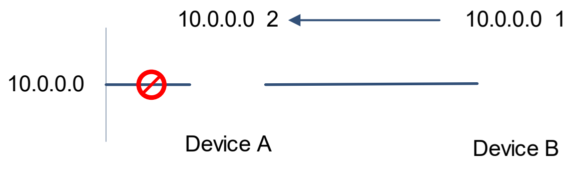
RIP uses functions such as split horizon and poison reverse to avoid route loops.

- Route loop

  A RIP route loop occurs due to inherent defects of the distance-vector algorithm.

  As shown in Figure 1-1, Device A is connected to the network 10.0.0.0, and sends an update packet every 30s. Device B receives the route 10.0.0.0 from Device A every 30s. If Device A is disconnected from 10.0.0.0, the route to 10.0.0.0 will be deleted from the routing table on Device A. Next time, the update packet sent by Device A no longer contains this route. As Device B does not receive an update packet related to 10.0.0.0, Device B determines that the route to 10.0.0.0 is valid within 180s and uses the update packet to send this route to Device A. As the route to 10.0.0.0 does not exist on Device A, the route learned from Device B is added to the routing table. Device B determines that data can reach 10.0.0.0 through Device A, and Device A determines that data can reach 10.0.0.0 through Device B. In this way, a route loop is formed.

Figure 1-1 Diagram of Route Loop



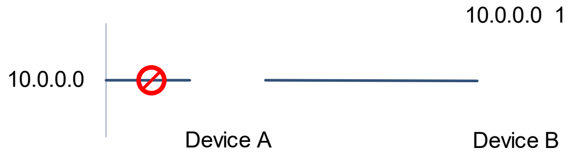
- Split horizon

  Split horizon can prevent route loops. After split horizon is enabled on an interface, a route received on this interface will not be sent out from this interface.

  As shown in Figure 1-2, after split horizon is enabled on the interface between Device A and Device B, Device B will not send the route 10.0.0.0 back to Device A. Device B will learn 180s later that 10.0.0.0 is not reachable.

  On a non broadcast multiple access (NBMA) network, there are multiple neighbors on an interface, and the device communicates with neighbors in unicast form. The routes received by the interface are distinguished by neighbors, and a route learned from a neighbor will not be sent back to this neighbor.

Figure 1-2 Diagram of Split Horizon



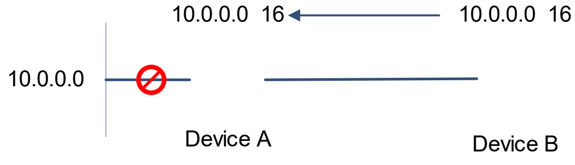
- Poison reverse

  Poison reverse can also prevent route loops. Compared with split horizon, poison reverse is more reliable, but brings more protocol packets, which makes network congestion more severe.

  After poison reverse is enabled on an interface, a route received from this interface will be sent out from this interface again, but the metric of this router will be changed to 16 (unreachable).

  As shown in Figure 1-3, after learning the route 10.0.0.0 from Device A, Device B sets the metric of this route to 16 and sends the route back to Device A. After this route becomes invalid, Device B advertises the route 10.0.0.0 (metric = 16) to Device A to accelerate the process of deleting the route from the routing table.

Figure 1-3 Diagram of Poison Reverse



6. Security Measures

RIP uses functions such as authentication and source address verification to ensure protocol security.

- Authentication

  RIPv2 supports authentication, but RIPv1 does not.

  The authentication function is used to prevent unauthorized devices from accessing the RIP routing domain. After authentication is enabled on an interface, the routing information cannot be exchanged between adjacent devices if authentication fails. Authentication is classified into plain text authentication and MD5 authentication:

  Plain text authentication: The configured password is directly added to the packet in the form of plain text, so the security of this authentication mode is low.

  MD5 authentication: The configured password is added to the packet after calculated by MD5 algorithm, so the security of this authentication mode is high.

- Source address verification

When a RIP-enabled device receives an update packet, it checks whether the source IP address in the packet and the IP address of the inbound interface are in the same network segment. If not, the device drops the packet. Source address verification is used to ensure that RIP routing information is exchanged only between adjacent routing devices.

Note

- On an unnumbered IP interface, source address verification is not performed (not configurable).
- If the triggered updates function is enabled, source address verification is automatically enabled (not configurable).
- If split horizon is disabled, source address verification is automatically enabled (not configurable).

7. Reliability Measures

Use RIP.

Correlate with Bidirectional Forwarding Detection (BFD).

Use fast reroute.

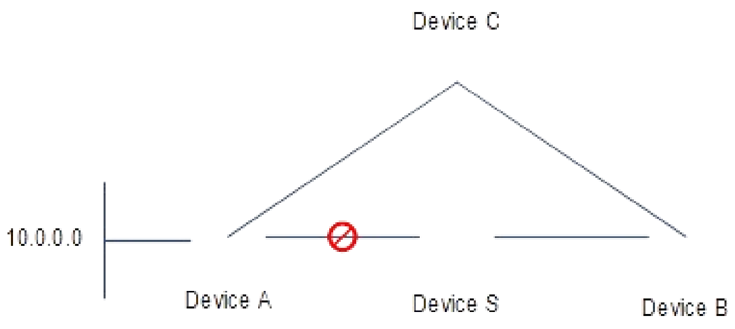
Use graceful restart (GR) and other functions to enhance reliability of the protocol.

- Correlate with BFD.
- Use fast reroute.

When a link or a device is faulty on the network, packets transmitted through this route will be lost until the route is converged again.

As shown in Figure 1-1, after the link between Device A and Device S is faulty, Device B may wait for 180s before it can detect the failure of the route (destination network: 10.0.0.0; next hop: Device A). Later, Device B may need to wait for 30s to re-obtain the route (destination network: 10.0.0.0; next hop: Device C) from Device C. Therefore, the traffic is interrupted for 210s.

Figure 1-1 Diagram of Fast Reroute



Quick detection of a route failure or fast switchover to the standby route helps shorten the traffic interruption time.

  - A BFD session can be set up between Device A and Device B, and correlated with RIP. BFD can quickly test the connectivity between adjacent devices. Once a link is faulty, RIP can detect the route failure within 1s.
  - The fast reroute function can be enabled. A backup route (destination network: 10.0.0.0; next hop: Device C) can be configured on Device B in advance. Once RIP detects a route failure, the backup route is immediately enabled.

- GR

  GR ensures uninterrupted data transmission when the protocol is restarted. If RIP is restarted on a GR-enabled device, the forwarding table before restart will be retained and a request packet will be sent to the neighbor so that the route can be learned again. During the GR period, RIP completes re-convergence of the route. After the GR period expires, RIP updates the forwarding entry and advertises the routing table to the neighbor.

8. Multiple VPN Instances

Multiple VPN instances may exist on a device.

RIP supports multiple instances. You can enable the RIP process in VPN routing and forwarding (VRF) address family mode to run RIP on VPN instances. One VRF address family is mapped to one VPN instance.

VPN instances cannot be distinguished from each other when you perform RIP operations using SNMP. You must bind the management information base (MIB) of RIP with a VPN instance before the SNMP operations take effect on the VPN instance.

1.1.3 Protocols and Standards

- RFC 1058: Routing Information Protocol
- RFC 2453: RIP Version 2

1.2 Configuration Task Summary

The RIP configuration includes the following tasks:

(1) Configuring Basic Features

  a Enabling RIP Process

  b Configuring Association with the Local Network

  c (Optional) Configuring RIP Version

  d (Optional) Configuring Split Horizon

  e (Optional) Configuring a Passive Interface

  f (Optional) Enabling Triggered Updates

(2) (Optional) Enabling RIP Route Summarization

  a Configuring to Enable Automatic Route Summarization Function b Configuring RIP Route Summarization on an Interface

(3) (Optional) Configuring RIP Route Filtering Rules The following configuration tasks are optional. Select tasks for configuration according to actual condition.

- o Configuring to Filter the Received RIP Routing Information
- o Configuring to Filter the Sent RIP Routing Information

(4) (Optional) Configuring to Adjust RIP Routing The following configuration tasks are optional. Select tasks for configuration according to actual condition.

- o Configuring to Modify the Management Distance of a RIP Route
- o Configuring to Increase the Metric of a Received or Sent RIP Route Metric
- o Configuring the Default Metric of an External Route Redistributed to RIP

(5) (Optional) Modifying Timers The following configuration tasks are optional. Select tasks for configuration according to actual condition.

- o Configuring to Modify the Update Timer, Invalid Timer, Flush Timer, and Holddown Timer of a RIP Route
- o Configuring the Sending Delay Between RIP Route Update Packets

(6) (Optional) Configuring RIP Route Distribution The following configuration tasks are optional. Select tasks for configuration according to actual condition.

- o Configuring to Advertise a Default Route to Neighbors
- o Configuring to Advertise a Default Route to Neighbors on an Interface
- o Configuring Route Redistribution

(7) (Optional) Controlling Interaction of RIP Packets The following configuration tasks are optional. Select tasks for configuration according to actual condition.

- o Configuring to Send Unicast RIP Route Update Packets
- o Configuring to Send Broadcast RIPv2 Packets on an Interface
- o Configuring to Allow an Interface to Receive RIP Packets
- o Configuring to Allow an Interface to Send RIP Packets
- o Configuring to Allow an Interface to Send RIP Packets of a Specified Version
- o Configuring to Allow an Interface to Receive RIP Packets of a Specified Version

(8) (Optional) Configuring to Enable RIPv2 Authentication

a Configuring RIP Authentication Mode

b Configuring a Key Chain for Authentication

c Configuring a Key Chain for RIP Plain Text Authentication

(9) (Optional) Configuring BFD Correlation with RIP

- o Configuring BFD Correlation with RIP Globally

- o Configuring BFD Correlation with RIP on an Interface

(10) (Optional) Configuring to Enable RIP Fast Reroute

(11) (Optional) Enabling GR

(12) (Optional) Configuring to Enable RIP Supernetting Routes

(13) (Optional) Configuring RIP to Enable Multiple VRF Instances

a Configuring a VRF Instance

b Configuring to Bind a RIP MIB with a VRF Instance

(14) (Optional) Configuring a Super VLAN to Enable RIP

(15) (Optional) Enabling Source Address Verification

1.3 Configuring Basic Features

1.3.1 Overview

Build a RIP routing domain on the network. Devices in the domain obtain routes to a remote network through RIP.

1.3.2 Restrictions and Guidelines

- IPv4 addresses must be configured.
- IPv4 unicast routes must be enabled.

1.3.3 Configuration Tasks

The basic function configuration of RIP includes the following tasks:

(1) Enabling RIP Process

(2) Configuring Association with the Local Network

(3) (Optional) Configuring RIP Version

(4) (Optional) Configuring Split Horizon

(5) (Optional) Configuring a Passive Interface

(6) (Optional) Enabling Triggered Updates

1.3.4 Enabling RIP Process

1. Overview

This command is used to create a RIP routing process and enter the RIP routing process configuration mode.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable a RIP routing process and enter the RIP routing process configuration mode.

router rip

The RIP routing process is disabled by default.

1.3.5 Configuring Association with the Local Network

1. Overview

To add an interface to the RIP domain, you need to first advertise the interface network in the RIP process.

2. Restrictions and Guidelines

- RIP can run and learn direct routes and RIP packets can be exchanged only on an interface covered by the **network**.
- If **network** 0.0.0.0 255.255.255.255 is configured, all interfaces are covered.
- If the *wildcard* parameter is not configured, the classful address range is used by default, that is, the interfaces whose addresses fall into the classful address range participate in RIP operations.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the RIP routing process configuration mode.

router rip

(4) Configure association with the local network.

network *network-number* [*wildcard*]

1.3.6 Configuring RIP Version

1. Overview

You can run this command to define the versions of RIP packets sent or received on all interfaces. This command takes effect on the entire device.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the RIP routing process configuration mode.

router rip

(4) Configure a RIP version.

version { **1** | **2** }

By default, route update packets of RIPv1 and RIPv2 can be received, but only route update packets of RIPv1 are sent.

1.3.7 Configuring Split Horizon

1. Overview

This function prevents route loop. After split horizon is enabled on an interface, a route received on this interface will not be sent out from this interface.

2. Restrictions and Guidelines

After poison reverse is enabled, split horizon is automatically disabled.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable split horizon.

ip rip split-horizon [**poisoned-reverse**]

By default, the split horizon function is enabled, but poison reverse is disabled.

1.3.8 Configuring a Passive Interface

1. Overview

The interface set to a passive interface suppresses RIP update packets. A passive interface defines the boundary of RIP routing domain to avoid unwanted flooding of RIP packets. If the interface connection device does not run the RIP routing protocol (such as a PC and a device running other routing protocols), you are advised to configure this interface as a passive interface.

2. Restrictions and Guidelines

You are advised to set all interfaces to passive interfaces in RIP routing process configuration mode, and then enter the device interconnection interface in the specific domain to disable the passive interface function.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the RIP routing process configuration mode.

router rip

(4) Configure passive interfaces.

passive-interface { **default** | *interface-type interface-number* }

The passive-interface function is disabled by default.

1.3.9 Enabling Triggered Updates

1. Overview

Enable the RIP triggered updates function, after which RIP does not periodically send route update packets. This function can quickly obtain network changes, avoid route loops, and improve the convergence speed.

2. Restrictions and Guidelines

- The basic functions of RIP must be configured.
- It is recommended that split horizon with poison reverse be enabled; otherwise, invalid routing information may exist.
- This function cannot be enabled together with the function of correlating RIP with BFD.
- Ensure that the triggered updates function is enabled on every router on the same link; otherwise, the routing information cannot be exchanged properly.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable triggered updates.

ip rip triggered [**retransmit-timer** *timer* | **retransmit-count** *count*]

The RIP triggered updates function is disabled by default.

1.4 Enabling RIP Route Summarization

1.4.1 Overview

This function can reduce the size of the routing table, improve the routing efficiency, avoid route flapping to some extent, and improve scalability and effectiveness of the network.

1.4.2 Restrictions and Guidelines

- The basic functions of RIP must be configured.
- The range of supernetting routes is larger than that of the classful network. Therefore, the automatic route summarization function is invalid for supernetting routes.
- RIPv1 performs automatic route summarization by default. If the detailed routes should be advertised, you must set the RIP version to RIPv2.

1.4.3 Configuration Tasks

The configuration for enabling RIP route summarization includes the following tasks:

(1) Configuring to Enable Automatic Route Summarization Function

(2) Configuring RIP Route Summarization on an Interface

1.4.4 Configuring to Enable Automatic Route Summarization Function

1. Overview

This function can be configured to reduce the size of the routing table, improve the routing efficiency, avoid route flapping to some extent, and improve scalability and effectiveness of the network.

2. Restrictions and Guidelines

- Route summarization is enabled by default for RIPv1 and RIPv2.
- You can disable automatic route summarization only when RIPv2 is configured.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the RIP routing process configuration mode.

router rip

(4) Enable the automatic route summarization function.

auto-summary

The automatic summarization function of RIP routes is enabled by default.

1.4.5 Configuring RIP Route Summarization on an Interface

1. Overview

This function is used to manually summarize an address or a subnet on a specified interface.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure RIP route summarization on an interface.

ip rip summary-address *ipv4-address mask*

By default, RIP route summarization is not configured on an interface.

1.5 Configuring RIP Route Filtering Rules

1.5.1 Overview

Routes that do not meet filtering criteria cannot be loaded to the routing table, or advertised to neighbors. In this way, users within the network can be prevented from accessing specified destination networks.

1.5.2 Restrictions and Guidelines

- The basic functions of RIP must be configured.
- In regard to the filtering rules of sent routes, you must configure route redistribution first, and then filter the redistributed routes.

1.5.3 Configuration Tasks

The configuration of RIP route filtering rules includes the following tasks, and these tasks are optional. Select tasks for configuration according to actual condition.

- Configuring to Filter the Received RIP Routing Information
- Configuring to Filter the Sent RIP Routing Information

1.5.4 Configuring to Filter the Received RIP Routing Information

1. Overview

You can configure the route distribution control list to refuse to receive some specified routes. If no interface is specified, the route update packets received on all interfaces will be filtered.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an ACL or prefix list. Please configure only one task.

- Configure an ACL.

  access-list *acl-number* { **deny** | **permit** } { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } [**time-range** *tm-range-name*] [**log**]

- Configure a prefix list.

  ip prefix-list *prefix-list-name* [**seq** *seq-number*] { **deny** | **permit** } *ipv4-prefix* [**ge** *minimum-prefix-length*] [**le** *maximum-prefix-length*]

(4) Enter the RIP routing process configuration mode.

router rip

(5) Filter the received RIP routing information.

distribute-list { [*acl-number* | *acl-name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*] } **in** [*interface-type interface-number*]

There is no inbound distribution list by default.

1.5.5 Configuring to Filter the Sent RIP Routing Information

1. Overview

You can configure the route distribution control list to prohibit distributing some specified routes. If no interface is specified, the route update packets sent to all interfaces will be filtered.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the RIP routing process configuration mode.

router rip

(4) Configure an ACL or prefix list. Please configure only one task.

- Configure an ACL.

  access-list *acl-number* { **deny** | **permit** } { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } [**time-range** *tm-range-name*] [**log**]

- Configure a prefix list.

  ip prefix-list *prefix-list-name* [**seq** *seq-number*] { **deny** | **permit** } *ipv4-prefix* [**ge** *minimum-prefix-length*] [**le** *maximum-prefix-length*]

(5) Filter the sent RIP routing information.

distribute-list { [*acl-name* | *acl-number*] | **prefix** *prefix-list-name* } **out** [*interface-type interface-number* | **bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **rip** | **static**]

There is no outbound distribution list by default.

1.6 Configuring to Adjust RIP Routing

1.6.1 Overview

This function can be used to change a RIP route so that the traffic passes through specified nodes or bypasses specified nodes. Change the sequence that a device selects various types of routes so as to change the priorities of RIP routes.

1.6.2 Restrictions and Guidelines

The basic functions of RIP must be configured.

1.6.3 Configuration Tasks

The configuration of RIP routing adjustment includes the following tasks, and these tasks are optional. Select tasks for configuration according to actual condition.

- Configuring to Modify the Management Distance of a RIP Route
- Configuring to Increase the Metric of a Received or Sent RIP Route Metric
- Configuring the Default Metric of an External Route Redistributed to RIP

1.6.4 Configuring to Modify the Management Distance of a RIP Route

1. Overview

This function is used to set the management distance of RIP routes and change the priority of a device in routing.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the RIP routing process configuration mode.

router rip

(4) Configure to modify the management distance of a RIP route.

distance *distance* [*ipv4-address wildcard*]

The management distance is **120** by default.

1.6.5 Configuring to Increase the Metric of a Received or Sent RIP Route

1. Overview

You can use this function to increase the metric of a received or sent RIP route. If an interface is specified, the configuration takes effect only on the specified interface; otherwise, the configuration takes effect globally.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the RIP routing process configuration mode.

router rip

(4) Configure to increase the metric of a received or sent RIP route.

offset-list { *acl-number* | *acl-name* } { **in** | **out** } *offset* [*interface-type interface-number*]

The metric of a received or sent RIP route is not increased by default.

1.6.6 Configuring the Default Metric of an External Route Redistributed to RIP

1. Overview

The default metric of a redistributed route is 1. If you want to preferably select an internal RIP route on some networks, just increase the default metric.

2. Restrictions and Guidelines

This function needs to be used together with the routing protocol redistribution function.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the RIP routing process configuration mode.

router rip

(4) Configure the default metric of an external route redistributed to RIP.

default-metric *metric-value*

By default, the metric of a redistributed route is 1.

1.7 Modifying Timers

1.7.1 Overview

This function can be used to change the durations of RIP timers to accelerate or slow down change to the protocol state or occurrence of an event.

1.7.2 Restrictions and Guidelines

- The basic functions of RIP must be configured.
- Modifying the protocol control parameters may result in protocol running failures. Therefore, you are advised not to modify the timers.

1.7.3 Configuration Tasks

The configuration of RIP timer modification includes the following tasks, and these tasks are optional. Select tasks for configuration according to actual condition.

- Configuring to Modify the Update Timer, Invalid Timer, Flush Timer, and Holddown Timer of a RIP Route
- Configuring the Sending Delay Between RIP Route Update Packets

1.7.4 Configuring to Modify the Update Timer, Invalid Timer, Flush Timer, and Holddown Timer of a RIP Route

1. Overview

By adjusting the timers, you can reduce the convergence time and fault rectification time of the routing protocol.

2. Restrictions and Guidelines

For devices connected to the same network, the values of RIP timers must be consistent. Generally, you are not advised to modify the RIP timers unless otherwise required.

Setting timers to small values on a low-speed link brings risks because a lot of update packets consume the bandwidth. You can set timers to small values generally on the Ethernet or a link of 2 Mbps (or above) to reduce the convergence time of network routes.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the RIP routing process configuration mode.

router rip

(4) Configure to modify the update timer, invalid timer, flush timer, and holddown timer of a RIP route.

timers basic *update invalid flush* [**holddown** *holddown*]

By default, the update timer is 30s, the invalid timer is 180s, the flush timer is 120s, and the holddown timer is 0s.

1.7.5 Configuring the Sending Delay Between RIP Route Update Packets

1. Overview

A RIP route update packet is 512 bytes long and can contain 25 routes. If the number of routes to be updated exceeds 25, more than one update packet will be sent as fast as possible. When a high-speed device sends a lot of update packets to a low-speed device, the low-speed device may fail to process all update packets in time, causing loss of routing information. This function can be used to increase the sending delay between packets on a high-speed device so that a low-speed device can receive and process all the update packets.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the sending delay between RIP route update packets.

output-delay *delay*

The sending delay between update packets is 0 by default.

1.8 Configuring RIP Route Distribution

1.8.1 Overview

In the RIP domain, you can introduce a unicast route or default route of another AS so that the unicast routing service to this AS can be provided for users in the RIP domain.

To enable a RIP routing domain to communicate with other ASs, a default route to another AS can be injected into the RIP routing domain, or the route of another AS can be redistributed to the RIP routing domain.

1.8.2 Restrictions and Guidelines

- The basic functions of RIP must be configured.
- Route redistribution cannot introduce default routes of other protocols to the RIP routing domain.

1.8.3 Configuration Tasks

The configuration of RIP route distribution includes the following tasks, and these tasks are optional. Select tasks for configuration according to actual condition.

- Configuring to Advertise a Default Route to Neighbors
- Configuring to Advertise a Default Route to Neighbors on an Interface
- Configuring Route Redistribution

1.8.4 Configuring to Advertise a Default Route to Neighbors

1. Overview

RIP will not advertise the default route in the routing table to neighbors by default. If you need to advertise the default route to the neighbors, use this function.

2. Restrictions and Guidelines

You still need to run the **default-information originate** command to introduce the default route generated by **ip default-network** to RIP.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the RIP routing process configuration mode.

router rip

(4) Advertise the default route to neighbors.

default-information originate [**always**] [**metric** *metric-value*] [**route-map** *route-map-name*]

1.8.5 Configuring to Advertise a Default Route to Neighbors on an Interface

1. Overview

If a default route needs to be advertised to some neighbors only, the default route to be advertised can be configured on the related interfaces, and RIP will advertise it to neighbors on the configured interfaces only.

2. Restrictions and Guidelines

- If you configure the **ip rip default-information** command for the interface, and the **default-information originate** command for the RIP process at the same time, only the default route configured for the interface is advertised.
- So far as the **ip rip default-information** command is configured for an interface, RIP does not learn the default route advertised by the neighbor.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Advertise the default route to neighbors on an interface.

ip rip default-information { **only** | **originate** } [**metric** *metric-value*]

By default, default route advertisement is disabled on an interface.

1.8.6 Configuring Route Redistribution

1. Overview

The function redistributes the routes of other protocols to the RIP domain to implement internetworking between the RIP domain and other routing domains.

2. Restrictions and Guidelines

- If the **level** parameter is not carried when IS-IS route redistribution is configured, only level-2 routes can be redistributed by default. If the **level** parameter is carried during initial configuration of redistribution, the routes configured with the **level** parameter can be redistributed. If both **level 1** and **level 2** are configured, the two levels are combined and saved as **level-1-2**.

- If you configure redistribution of OSPF routes without specifying the **match** parameter, OSPF routes of all sub-types can be distributed by default. The latest setting of the **match** parameter is used as the initial **match** parameter. Only routes that match the sub-types can be redistributed. You can run the **no** form of the command to restore the default value of **match**.
- The configuration rules for the **no** form of the **redistribute** command are as follows:
  - If some parameters are specified in the **no** form of this command, default values of these parameters will be restored.
  - If no parameter is specified in the **no** form of this command, the entire command will be deleted.
- For example, if **redistribute isis 112 level-2** is configured, you can run the **no redistribute isis 112 level-2** command to restore the default value of level-2. As **level-2** itself is the default value of the parameter, the configuration saved is still **redistribute isis 112 level-2** after the preceding **no** form of the command is executed. To delete the entire command, run the **no redistribute isis 112** command.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Redistribute routes and advertise external routes to neighbors.

redistribute { **bgp** | **connected** | **isis** [*area-tag*] [**level-1** | **level-1-2** | **level-2**] | **ospf** *process-id* [**match** { **external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**] } *] | **static** } [**metric** *metric-value* | **route-map** *route-map-name*] *

The redistribution function is not configured by default.

If OSPF redistribution is configured, the routes of all sub-types of the instance will be redistributed.

If IS-IS redistribution is configured, redistribute the level-2 routes of the IS-IS process.

In other cases, all routes of this type are redistributed.

1.9 Controlling Interaction of RIP Packets

1.9.1 Overview

This function can be used to change the default running mechanism of RIP through configuration and control the interaction mode of RIP packets.

The following interaction modes of RIP packets can be implemented:

Allowing or prohibiting the sending of unicast RIP packets to a specified neighbor on an interface

Allowing or prohibiting the sending of unicast RIPv2 packets instead of broadcast packets to a specified neighbor on an interface

Allowing or prohibiting the receiving of RIP packets on an interface

Allowing or prohibiting the sending of RIP packets on an interface

Allowing or prohibiting the receiving of RIP packets of a specified version on an interface

Allowing or prohibiting the sending of RIP packets of a specified version on an interface

1.9.2 Restrictions and Guidelines

- The basic functions of RIP must be configured.
- On an interface connecting to a neighbor device, the configured version of sent RIP packets must be the same as the version of received RIP packets.

1.9.3 Configuration Tasks

The configuration of RIP packet interaction includes the following tasks, and these tasks are optional. Select tasks for configuration according to actual condition.

- Configuring to Send Unicast RIP Route Update Packets
- Configuring to Send Broadcast RIPv2 Packets on an Interface
- Configuring to Allow an Interface to Receive RIP Packets
- Configuring to Allow an Interface to Send RIP Packets
- Configuring to Allow an Interface to Send RIP Packets of a Specified Version
- Configuring to Allow an Interface to Receive RIP Packets of a Specified Version

1.9.4 Configuring to Send Unicast RIP Route Update Packets

1. Overview

This function can be configured if you hope that only some of devices connected to an interface can receive the updated routing information or when RIP is used for a non-broadcast network.

2. Restrictions and Guidelines

Generally, you can first enable the passive interface function in routing process configuration mode, and then specify the neighbors that can receive the routing information. This command does not affect the receiving of RIP packets. After an interface is configured as a passive interface, the interface does not send a request packet even after the device is restarted.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the RIP routing process configuration mode.

router rip

(4) Configure to send unicast RIP route update packets to a specified neighbor.

neighbor *ipv4-address*

No RIP neighbor is configured by default.

1.9.5 Configuring to Send Broadcast RIPv2 Packets on an Interface

1. Overview

This function can be configured if the neighbor device does not support receiving of multicast RIPv2 packets.

2. Restrictions and Guidelines

- The default behavior depends on the configuration of the **version** command.
- The configuration result of this command can overwrite the default configuration of the **version** command.
- This command affects the behavior of sending RIP packets on the current interface, and the interface is allowed to send RIPv1 and RIPv2 packets simultaneously.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure to send broadcast RIPv2 packets on an interface.

ip rip v2-broadcast

By default, RIPv2 packets are multicast on an interface.

1.9.6 Configuring to Allow an Interface to Receive RIP Packets

1. Overview

If you want to prevent an interface from receiving RIP packets, you can enable this function.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure to allow an interface to receive RIP packets.

ip rip receive enable

By default, an interface can receive RIP packets normally.

1.9.7 Configuring to Allow an Interface to Send RIP Packets

1. Overview

If you want to prevent an interface from sending RIP packets, you can disable this function.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure to allow an interface to send RIP packets.

ip rip send enable

By default, the RIP packet sending function is enabled on an interface.

1.9.8 Configuring to Allow an Interface to Send RIP Packets of a Specified Version

1. Overview

To be compatible with the RIP version running on the peer device, use this function to change the version of RIP packets sent by the interface.

2. Restrictions and Guidelines

- The default behavior depends on the configuration of the **version** command.

- The configuration result of this command can overwrite the default configuration of the **version** command.
- This command affects the behavior of sending RIP packets on the current interface, and the interface is allowed to send RIPv1 and RIPv2 packets simultaneously. If this command does not contain any parameter, the behavior of receiving RIP packets depends on the configuration of the **version** command.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure to allow an interface to send RIP packets of a specified version.

ip rip send version [**1**] [**2**]

By default, the default behavior depends on the configuration of the **version** command.

1.9.9 Configuring to Allow an Interface to Receive RIP Packets of a Specified Version

1. Overview

To be compatible with the RIP version running on the peer device, use this function to change the version of RIP packets that can be received by the interface.

2. Restrictions and Guidelines

- The default behavior depends on the configuration of the **version** command.
- The configuration result of this command can overwrite the default configuration of the **version** command.
- This command affects the behavior of receiving RIP packets on the current interface, and the interface is allowed to receive RIPv1 and RIPv2 packets simultaneously. If this command does not contain any parameter, the behavior of receiving RIP packets depends on the configuration of the **version** command.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure to allow an interface to receive RIP packets of a specified version.

ip rip receive version [**1**] [**2**]

By default, the default behavior depends on the configuration of the **version** command.

1.10 Configuring to Enable RIPv2 Authentication

1.10.1 Overview

This function prevents learning unauthenticated and invalid routes and advertising valid routes to unauthenticated devices, ensuring stability of the routing system, and protecting the system against intrusions.

1.10.2 Restrictions and Guidelines

- The basic functions of RIP must be configured.
- Only RIPv2 supports authentication of RIP packets, and RIPv1 does not.

1.10.3 Configuration Tasks

The configuration for enabling RIPv2 authentication includes the following tasks:

(1) Configuring RIP Authentication Mode

(2) Configuring a Key Chain for Authentication

(3) Configuring a Key Chain for RIP Plain Text Authentication

1.10.4 Configuring RIP Authentication Mode

1. Overview

RIPv2 supports plain text authentication and cipher text authentication, and ensures secure transmission of RIP packets.

2. Restrictions and Guidelines

- For all devices that need to directly exchange the RIP routing information, the RIP authentication mode of these devices must be the same.
- Cipher text authentication is recommended because the plain text password is saved in the configuration file and the security is low.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable the RIP authentication mode.

ip rip authentication mode { **text** | **md5** }

Plain text authentication mode is used by default.

1.10.5 Configuring a Key Chain for Authentication

1. Overview

A key chain can be used to change the key dynamically to improve the security.

2. Restrictions and Guidelines

- The specified key chain must be defined using the **key chain** command in global configuration mode in advance.
- If this command and the **ip rip authentication mode md5** command are configured, MD5 mode authentication is adopted. If the **ip rip authentication mode** command is not configured, authentication is performed according to the authentication mode specified by the configured **key chain**. MD5 authentication and SM3 authentication are supported at present.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure a key chain for authentication.

ip rip authentication key-chain *name-of-keychain*

No key chain is set by default.

1.10.6 Configuring a Key Chain for RIP Plain Text Authentication

1. Overview

This function uses a string to implement plain text encryption and improve the security of RIP packet transmission.

2. Restrictions and Guidelines

- This function takes effect only in plain text authentication mode.

- Encrypted strings can be displayed in plain text or cipher text. Cipher text is recommended.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable RIP plain text authentication and configure a key chain.

ip rip authentication text-password [**0** | **7**] *password-string*

No character string of plain text authentication is set by default.

1.11 Configuring BFD Correlation with RIP

1.11.1 Overview

Once a link fails, RIP can quickly detect the failure of the route. This function helps shorten the traffic interruption time.

1.11.2 Restrictions and Guidelines

- The basic functions of RIP must be configured.
- The BFD correlation configured in interface configuration mode takes precedence over the global configuration.

1.11.3 Configuration Tasks

The configuration for enabling BFD correlation with RIP includes the following tasks:

- Configuring BFD Correlation with RIP Globally
- Configuring BFD Correlation with RIP on an Interface

1.11.4 Configuring BFD Correlation with RIP Globally

1. Overview

This function enables BFD correlation with RIP globally. Once a link fails, RIP can quickly detect the failure of the route, which helps shorten the traffic interruption time.

After BFD is enabled on RIP, a BFD session will be set up for the RIP routing information source (that is, the source address of RIP route update packets). Once the BFD neighbor fails, the corresponding RIP route directly enters the invalid state and is not forwarded.

2. Restrictions and Guidelines

The BFD configured on an interface takes precedence over that configured in process configuration mode.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the RIP routing process configuration mode.

router rip

(4) Configure to enable BFD correlation with RIP globally.

bfd all-interfaces

The BFD function is disabled by default.

1.11.5 Configuring BFD Correlation with RIP on an Interface

1. Overview

This function enables BFD correlation with RIP on an interface. Once an interface link fails, RIP can quickly detect the failure of the route, which helps shorten the traffic interruption time.

2. Restrictions and Guidelines

- By default, the BFD configuration is subject to that configured in RIP process configuration mode.
- This configuration must be performed if you need to enable or disable BFD correlation on a specified interface.
- The BFD configured on an interface takes precedence over that configured in RIP process configuration mode.
- According to the actual environment, you can select to enable BFD on the specified interface, or enable BFD globally in RIP process, or disable BFD on the specified interface.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure BFD correlation with RIP on an interface.

ip rip bfd [**disable**]

By default, BFD link detection on an interface is disabled by default.

1.12 Configuring to Enable RIP Fast Reroute

1.12.1 Overview

Once RIP detects a route failure, the router immediately switches to the second-best route. This configuration helps shorten the traffic interruption time.

1.12.2 Restrictions and Guidelines

- The basic functions of RIP must be configured.
- The route map and the backup next hop must be configured.
- To accelerate convergence, set **carrier-delay** of the interface to **0** and enable BFD correlation with RIP.

1.12.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a routing policy.

route-map *route-map-name* [{ **permit** | **deny** } *sequence*]

(4) Run this command to configure the interface-based matching rule.

match interface { *interface-type interface-number* }&<1-n>

(5) Return to the global configuration mode.

exit

(6) Enter the RIP routing process configuration mode.

router rip

(7) Enable fast reroute.

fast-reroute route-map *route-map-name*

The fast reroute function is disabled by default.

1.13 Enabling GR

1.13.1 Overview

The GR period is the maximum time from restart of the RIP process to completion of the restart. During this period, RIP performs route recovery and the forwarding table remains unchanged. After the restart period expires, RIP exits the GR state and performs common RIP operations.

1.13.2 Restrictions and Guidelines

- The basic functions of RIP must be configured.
- The GR period is at least twice the RIP route update period.

1.13.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the RIP routing process configuration mode.

router rip

(4) Enable GR.

graceful-restart [**grace-period** *grace-period*]

The GR function is enabled by default.

1.14 Configuring to Enable RIP Supernetting Routes

1.14.1 Overview

This function is used to allow RIP to send RIP supernetting routes on a specified interface. The concept of supernetting is similar to that of subnet. Subnet means dividing a large network segment into several small network segments, while supernetting means aggregating some small network segments into a large network segment. The number of network address bits allowed by supernetting is larger than that allowed by a classful network.

1.14.2 Restrictions and Guidelines

The basic functions of RIP must be configured.

1.14.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable supernetting routes.

ip rip send supernet-routes

By default, the supernetting route sending function is enabled on an interface.

1.15 Configuring RIP to Enable Multiple VRF Instances

1.15.1 Overview

This function is used to run RIP on VPN instances.

1.15.2 Restrictions and Guidelines

The RIP basic functions (with the VRF parameter) must be configured.

1.15.3 Configuration Tasks

The RIP configuration for enabling multiple VRF instances includes the following tasks:

(1) Configuring a VRF Instance

(2) Configuring to Bind a RIP MIB with a VRF Instance

1.15.4 Configuring a VRF Instance

1. Overview

This function is used to create a VRF instance.

2. Restrictions and Guidelines

This function must be configured if you need to configure multiple RIP instances and associate these RIP instances with VRF.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the RIP routing process configuration mode.

router rip

(4) Create a VRF instance and enter the IPv4 VRF address family configuration mode.

address-family ipv4 vrf *vrf-name*

The address family of RIP is disabled by default.

(5) Exit the IPv4 VRF address family.

exit-address-family

1.15.5 Configuring to Bind a RIP MIB with a VRF Instance

1. Overview

If multiple RIP instances have been configured, this function can be used to manage non-default RIP instances using the MIB.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the RIP routing process configuration mode.

router rip

(4) Configure to bind a RIP MIB with a VRF instance.

enable mib-binding

By default, the MIB is bound with the RIP instance of the default VRF.

1.16 Configuring a Super VLAN to Enable RIP

1.16.1 Overview

This function is used to run RIP on a super VLAN. A super VLAN is also called VLAN aggregation. Multiple sub VLANs are associated with one super VLAN. All sub VLANs share the SVI interface of the super VLAN and use it as the gateway of Layer-3 communication to save IP resources.

In normal cases, a super VLAN contains multiple sub VLANs. Multicast packets of a super VLAN are also sent to its sub VLANs. In this case, when RIP multicast packets are sent over a super VLAN containing multiple sub VLANs, the RIP multicast packets are replicated multiple times, and the device processing capability is insufficient. As a result, a large number of packets are discarded, causing protocol flapping.

In most scenarios, the RIP function does not need to be enabled on a super VLAN, and it is disabled by default. However, in some scenarios, the RIP function must be run on the super VLAN, but packets need to be sent to only one sub VLAN. In this case, you can decide to send multicast packets to a certain sub VLAN or to all sub VLANs as actually needed. You can run this command to specify a particular sub VLAN. You must be cautious when configuring packet transmission to all sub VLANs, as the large number of sub VLANs may cause a device processing bottleneck, which will lead to the neighbor flapping.

1.16.2 Restrictions and Guidelines

- The basic functions of RIP must be configured.
- The designated sub VLAN must be connected to neighbors.

1.16.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the inbound interface configuration mode.

interface vlan *vlan-id*

(4) Configure to enable RIP.

ip rip subvlan [**all |** *vlan-id*]

By default, RIP is disabled on a super VLAN.

1.17 Enabling Source Address Verification

1.17.1 Overview

You can run the command to validate the source address of a RIP route update packet. The purpose is to ensure that the RIP routing process receives only the route update packets coming from the same IP subnet neighbor.

1.17.2 Restrictions and Guidelines

- The basic functions of RIP must be configured.
- After split horizon is disabled on an interface, the RIP routing process will perform source address validation on the update packet no matter whether the **validate-update-source** command is executed in routing process configuration mode.
- For an interface not configured with an IP address, the RIP routing process does not perform source address validation for the update packet no matter whether the **validate-update-source** command is executed in routing process configuration mode.

1.17.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the RIP routing process configuration mode.

router rip

(4) Enables source address verification.

validate-update-source

The source address validation function for update packets is enabled by default.

1.18 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Run the **debug** command to output debugging information.

⚠ Caution

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Table 1-1 RIP Monitoring

Command	Purpose
show ip rip [**vrf** *vrf-name*]	Displays the basic information about a RIP process.
show ip rip database [**vrf** *vrf-name*] [*network-number network-mask*] [**count**]	Displays the RIP routing table.
show ip rip external [**bgp** | **connected** | **isis** [*process-id*] | **ospf** *process-id* | **static**] [**vrf** *vrf-name*]	Displays information about external routes redistributed by RIP.
show ip rip interface [**vrf** *vrf-name*] [*interface-type interface-number*]	Displays the RIP interface information.
show ip rip peer [*ipv4-address*] [**vrf** *vrf-name*]	Displays the RIP neighbor information.
debug ip rip event	Debugs events that occur when the RIP process is running.
debug ip rip nsm	Debugs interaction with the NSM process.

Command	Purpose
debug ip rip packet [**interface** *interface-type interface-number* | **recv** | **send**]	Debugs the sent and received packets.
debug ip rip restart	Debugs the RIP GR process.
debug ip rip route	Debugs the route changes of the RIP process.

1.19 Configuration Examples

1.19.1 Building a RIP Routing Domain

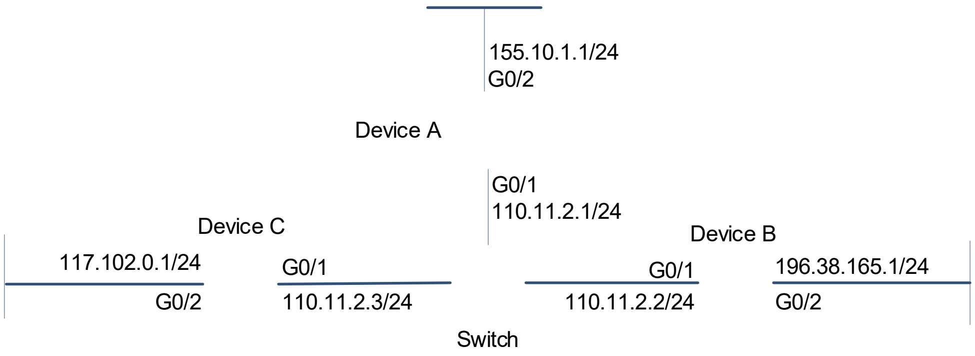
1. Requirements

Device A, Device B, and Device C implement interworking through the RIPv2 routing protocol.

To save the device performance, all interfaces of the three devices are configured as passive interfaces by default, and passive interface is disabled only for the interfaces directly connected to RIP neighbors.

2. Topology

Figure 1-1 Topology for Building a RIP Routing Domain



3. Notes

- Configure interface IP addresses for all the devices.
- Configure the RIP basic functions for all the devices.

4. Procedure

(1) Configure an IP address for each interface and start the unicast routing protocol.

Configure Device A.

```
Device A> enable
Device A# configure terminal
Device A(config)# interface GigabitEthernet 0/1
Device A(config-if-GigabitEthernet 0/1)# no switchport
Device A(config-if-GigabitEthernet 0/1)# ip address 110.11.2.1 255.255.255.0
Device A(config-if-GigabitEthernet 0/1)# exit
Device A(config)# interface GigabitEthernet 0/2
Device A(config-if-GigabitEthernet 0/2)# no switchport
Device A(config-if-GigabitEthernet 0/2)# ip address 155.10.1.1 255.255.255.0
Device A(config-if-GigabitEthernet 0/2)# exit
```

Configure Device B.

```
Device B> enable
Device B# configure terminal
Device B(config)# interface GigabitEthernet 0/1
Device B(config-if-GigabitEthernet 0/1)# no switchport
Device B(config-if-GigabitEthernet 0/1)# ip address 110.11.2.2 255.255.255.0
Device B(config-if-GigabitEthernet 0/1)# exit
Device B(config)# interface GigabitEthernet 0/2
Device B(config-if-GigabitEthernet 0/2)# no switchport
Device B(config-if-GigabitEthernet 0/2)# ip address 196.38.165.1 255.255.255.0
Device B(config-if-GigabitEthernet 0/2)# exit
```

Configure Device C.

```
Device C> enable
Device C# configure terminal
Device C(config)# interface GigabitEthernet 0/1
Device C(config-if-GigabitEthernet 0/1)# no switchport
Device C(config-if-GigabitEthernet 0/1)# ip address 110.11.2.3 255.255.255.0
Device C(config-if-GigabitEthernet 0/1)# exit
Device C(config)# interface GigabitEthernet 0/2
Device C(config-if-GigabitEthernet 0/2)# no switchport
Device C(config-if-GigabitEthernet 0/2)# ip address 117.102.0.1 255.255.0.0
Device C(config-if-GigabitEthernet 0/2)# exit
```

(2) Configure the RIP basic functions for the devices. Except the RIP neighbor interface, configure the other interfaces as passive interfaces.

Configure Device A.

```
Device A(config)# router rip
Device A(config-router)# version 2
Device A(config-router)# network 0.0.0.0 255.255.255.255
Device A(config-router)# passive-interface default
Device A(config-router)# no passive-interface GigabitEthernet 0/1
```

Configure Device B.

```
Device B(config)# router rip
Device B(config-router)# version 2
Device B(config-router)# network 0.0.0.0 255.255.255.255
Device B(config-router)# passive-interface default
Device B(config-router)# no passive-interface GigabitEthernet 0/1
```

Configure Device C.

```
Device C(config)# router rip
Device C(config-router)# version 2
Device C(config-router)# no auto-summary
Device C(config-router)# network 0.0.0.0 255.255.255.255
Device C(config-router)# passive-interface default
Device C(config-router)# no passive-interface GigabitEthernet 0/1
```

5. Verification

Check the IP routing tables on Device A, Device B, and Device C. Verify that RIP has learned the routes to remote networks.

- Device A

```
Device A# show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    110.11.2.0/24 is directly connected, GigabitEthernet 0/1
C    110.11.2.1/32 is local host.
R    117.0.0.0/8 [120/1] via 110.11.2.2, 00:00:47, GigabitEthernet 0/1
C    155.10.1.0/24 is directly connected, GigabitEthernet 0/2
C    155.10.1.1/32 is local host.
C    192.168.217.0/24 is directly connected, VLAN 1
C    192.168.217.233/32 is local host.
R    196.38.165.0/24 [120/1] via 110.11.2.3, 00:19:18, GigabitEthernet 0/1
```

- Device B

```
Device B# show ip route

```

```
Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    110.11.2.0/24 is directly connected, GigabitEthernet 0/1
C    110.11.2.2/32 is local host.
R    155.10.0.0/16 [120/1] via 110.11.2.1, 00:15:21, GigabitEthernet 0/1
C    196.38.165.0/24 is directly connected, GigabitEthernet 0/2
C    196.38.165.1/32 is local host.
R    117.0.0.0/8 [120/1] via 110.11.2.2, 00:00:47, GigabitEthernet 0/1
```

- Device C

```
Device C# show ip route
Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    110.11.2.0/24 is directly connected, GigabitEthernet 0/1
C    110.11.2.3/32 is local host.
C    117.102.0.0/16 is directly connected, GigabitEthernet 0/2
C    117.102.0.1/32 is local host.
R    155.10.0.0/16 [120/1] via 110.11.2.1, 00:20:55, GigabitEthernet 0/1
R    196.38.165.0/24 [120/1] via 110.11.2.3, 00:19:18, GigabitEthernet 0/1
```

6. Configuration Files

- Device A configuration file.

```
!
interface GigabitEthernet 0/1
 no switchport
 ip address 110.11.2.1 255.255.255.0
!
interface GigabitEthernet 0/2
 no switchport
 ip address 155.10.1.1 255.255.255.0
```

```
!
router rip
 version 2
 passive-interface default
 no passive-interface GigabitEthernet 0/1
 network 0.0.0.0
!
```

- Device B configuration file.

```
!
interface GigabitEthernet 0/1
 no switchport
 ip address 110.11.2.2 255.255.255.0
!
interface GigabitEthernet 0/2
 no switchport
 ip address 196.38.165.1 255.255.255.0
!
router rip
 version 2
 passive-interface default
 no passive-interface GigabitEthernet 0/1
 network 0.0.0.0
!
```

- Device C configuration file.

```
!
interface GigabitEthernet 0/1
 no switchport
 ip address 110.11.2.3 255.255.255.0
!
interface GigabitEthernet 0/2
 no switchport
 ip address 117.102.0.1 255.255.255.0
!
router rip
 version 2
 no auto-summary
 passive-interface default
 no passive-interface GigabitEthernet 0/1
 network 0.0.0.0
!
```

7. Common Errors

- The IPv4 address is not configured on an interface.
- The RIP version is not defined on a device, or the RIP version No. on the device is different from that on other devices.
- The address range configured using the **network** command does not cover a specific interface.
- The IP address comparison bit parameter in the **network** command is not correctly configured. Value 0 indicates accurate matching, and 1 indicates that no comparison is performed.
- The interface used for interworking between devices is configured as a passive interface.

1.19.2 Configuring RIP to Prevent Route Loop

1. Requirements

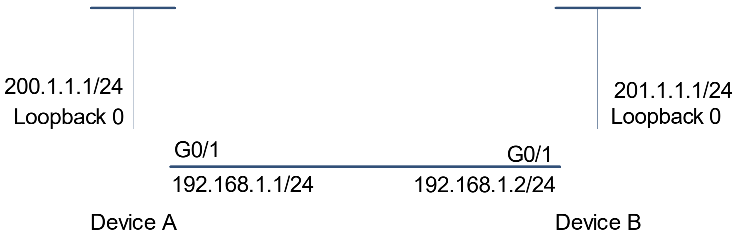
Device A, Device B, and Device C implement interworking through the RIP routing protocol.

To avoid route loop, you need to configure split horizon with poison reverse and triggered updates.

To improve reliability, enable GR, and then enable BFD on the connection interface of Device A and Device B.

2. Topology

Figure 1-1 Topology for Enabling Triggered Updates



3. Notes

(1) Configure interface IP addresses for all devices (omitted).

(2) Configure the RIP basic functions for all the devices.

(3) Enable RIP triggered updates and poison reverse on Device A and Device B.

4. Procedure

(1) Configure interface IP addresses for all devices (omitted).

(2) Enable the RIP process of the device and advertise the network information of each interface.

Configure Device A.

```
Device A> enable
Device A# configure terminal
Device A(config)# router rip
Device A(config-router)# network 192.168.1.0
Device A(config-router)# network 200.1.1.0
Device A(config-router)# exit
```

Configure Device B.

```
Device B> enable
Device B# configure terminal
Device B(config)# router rip
Device B(config-router)# network 192.168.1.0
Device B(config-router)# network 201.1.1.0
Device B(config-router)# exit
```

(3) Enable RIP poison reverse and triggered updates.

Configure Device A.

```
Device A(config)# interface GigabitEthernet 0/1
Device A(config-if-GigabitEthernet 0/1)# ip rip triggered
Device A(config-if-GigabitEthernet 0/1)# ip rip split-horizon poisoned-reverse
```

Configure Device B.

```
Device B(config)# interface GigabitEthernet 0/1
Device B(config-if-GigabitEthernet 0/1)# ip rip triggered
Device B(config-if-GigabitEthernet 0/1)# ip rip split-horizon poisoned-reverse
```

5. Verification

Check the RIP databases of Device A and Device B, and verify that the corresponding route attributes are permanent.

- Device A

```
Device A# show ip rip database
201.1.1.0/24   auto-summary
201.1.1.0/24
[1] via 192.168.12.2 GigabitEthernet 0/1  06:25    permanent
```

- Device B

```
Device B# show ip rip database
200.1.1.0/24   auto-summary
200.1.1.0/24
    [1] via 192.168.12.1 GigabitEthernet 0/1  06:25    permanent
```

6. Configuration Files

- Device A configuration file

```
!
interface GigabitEthernet 0/1
ip rip split-horizon poisoned-reverse
 ip rip triggered
!
!
router rip
network 192.168.1.0
network 200.1.1.0
!
```

- Device B configuration file

```
!
interface GigabitEthernet 0/1
ip rip split-horizon poisoned-reverse
 ip rip triggered
!
router rip
network 192.168.1.0
network 201.1.1.0
!
```

7. Common Errors

- The triggered updates function is enabled when the RIP configurations at both ends of the link are consistent.
- Both the triggered updates and BFD functions are enabled.
- The triggered updates function is not enabled on all devices on the same link.

1.19.3 Configuring External Routes Imported by RIP

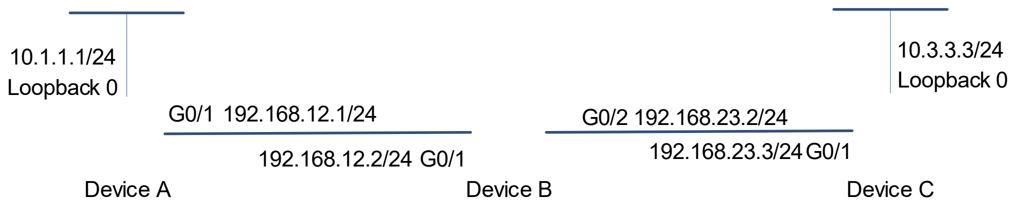
1. Requirements

Device B communicates with Device A through RIP, and Device B obtains the route 10.3.3.3 through a static route.

To enable Device A to obtain the routing information of 10.3.3.3, enable the OSPF routing protocol in Device B. The reliability of introducing external routes is low. Set the external default metric to 5.

2. Topology

Figure 1-1 Topology for Configuring External Routes Imported by RIP



3. Notes

(1) Configure an IP address for each interface and start the unicast routing protocol (omitted).

(2) Configure a static route for Device B.

(3) Configure the basic functions of RIP on Device A and Device B (omitted).

(4) Configure route redistribution on Device B and set the default metric of the redistributed route.

4. Procedure

(1) Configure an IP address for each interface and start the unicast routing protocol (omitted).

(2) Configure a static route to 10.3.3.3/24 on Device B, and set the next hop to 192.168.23.3.

```
Device B> enable
Device B# configure terminal
Device B(config)# ip route 10.3.3.3 255.255.255.0 192.168.23.3
```

(3) Configure the basic functions of RIP on Device A and Device B (omitted).

(4) Set the default metric of the redistributed route to 5 on Device B.

```
Device B(config)# router rip
Device B(config-router)# default-metric 5
```

(5) Configure the redistribution of static route to RIP on Device B.

```
Device B(config-router)# redistribute static
```

5. Verification

Check the routing table on Device A. Verify that the RIP route of 10.3.3.0/24 is available, and the metric is 6.

```
Device A# show ip route rip
R    10.3.3.0/24 [120/6] via 192.168.12.2, 00:06:11, GigabitEthernet 0/1
```

6. Configuration Files

Device B configuration file.

```
!
```

```
ip route 10.3.3.3 255.255.255.0 192.168.23.3
!
router rip
 default-metric 5
 redistribute static
!
```

1.19.4 Configuring Increasing the Metric of a RIP Interface

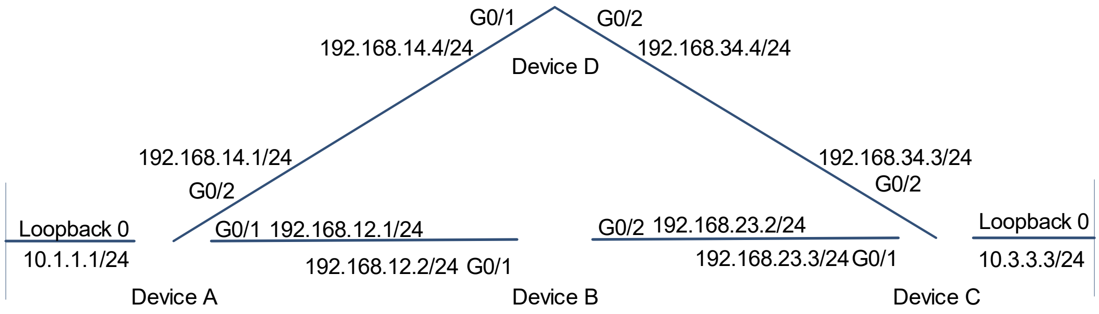
1. Requirements

Device A, Device B, Device C, and Device D implement interworking through the RIPv2 routing protocol.

There are two equal-cost paths from Device A to 10.3.3.3/24 of Device C. In consideration of the old model and low performance of Device D, increase the metric of the Gigabit Ethernet 0/2 interface of Device A so that Device A can go to 10.3.3.3 to prefer Device B.

2. Topology

Figure 1-1 Topology for Increasing the Metric of a RIP Interface



3. Notes

(1) Configure interface IP addresses for all the devices. (Omitted)

(2) Configure the RIP basic functions for all the devices. (Omitted)

(3) Configure ACL on Device C, and enable offset-list on the interface connected to Device B.

4. Procedure

(1) Configure ACL on Device C, and match the route 10.3.3.3/24.

```
Device C> enable
Device C# configure terminal
Device C(config)# access-list 1 permit 10.3.3.3 0.0.0.255
```

(2) Configure **offset** on Device C, associate with ACL 1, and enable the offset-list on the GigabitEthernet 0/2 interface.

```
Device C(config)# router rip
Device C(config-router)# offset-list 1 out 3 gigabitEthernet 0/2
```

5. Verification

Check the routing table of Device A.

```
Device A# show ip route rip
R    10.3.3.0/24 [120/5] via 192.168.14.4, 00:06:11, GigabitEthernet 0/1
```

6. Configuration Files

Device C configuration file.

```
!
access-list 1 permit 10.3.3.3 0.0.0.255
!
router rip
 offset-list 1 out 3 gigabitEthernet 0/2
!
```

1.19.5 Configuring RIP to Distribute a Summarized Route

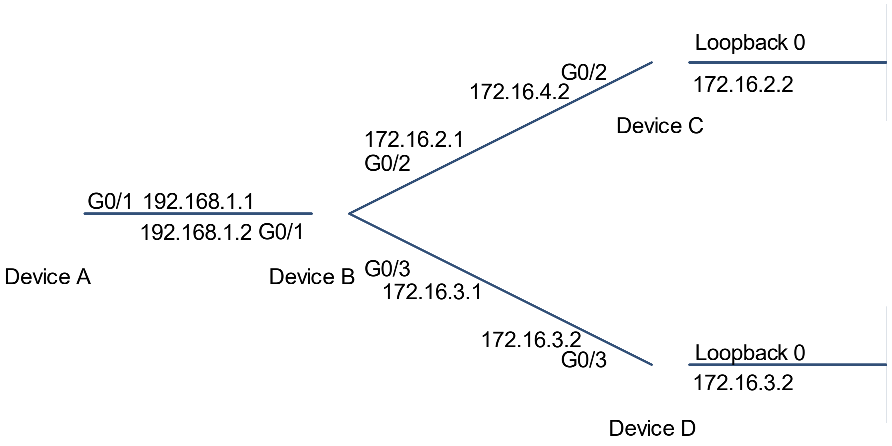
1. Requirements

Device B, implements interworking with Device A, Device C, and Device D through the RIPv2 routing protocol.

To reduce the size of the routing table of Device A, configure route summarization to 172.16.0.0/21 on Device B.

2. Topology

Figure 1-1 Topology for Configuring RIP to Distribute a Summarized Route



3. Notes

(1) Configure interface IP addresses for all devices (omitted).

(2) Configure the RIP basic functions for all the devices (omitted).

(3) Disable automatic summarization on Device B and configure route summarization.

4. Procedure

(1) Configure an IP address for each interface and start the unicast routing protocol (omitted).

(2) Configure RIP basic functions on the devices (omitted).

(3) Disable automatic summarization on Device B.

```
Device B> enable
Device B# configure terminal
Device B(config)# router rip
Device B(config-router)# version 2
Device B(config-router)# no auto-summary
Device B(config-router)# exit
```

(4) Configure 172.16.0.0/21 route summarization on the GigabitEthernet 0/1 interface of Device B.

```
Device B(config)# interface GigabitEthernet 0/1
Device B(config-if-GigabitEthernet 0/1)# ip rip summary-address 172.16.0.0
255.255.248.0
```

5. Verification

Check the routing table of Device A, and verify that the entry 172.16.0.0/16 is generated.

```
Device A# show ip route rip
R 172.16.0.0/21 [120/2] via 192.168.1.2, 00:01:04, GigabitEthernet 0/1
```

6. Configuration Files

Device B configuration file.

```
!
interface GigabitEthernet 0/1
ip address 196.38.165.1 255.255.255.0
!
router rip
 version 2
 no auto-summary
!
```