Contents

1 Configuring RIPng

1.1 Introduction

1.1.1 Overview

RIP next generation (RIPng) is a unicast routing protocol that applies to IPv6 networks. RIPng-enabled routers exchange routing information to obtain routes to remote networks.

As an Interior Gateway Protocol (IGP), RIPng can run only within an autonomous system (AS) and is applicable to small-sized networks.

Note

In this chapter, the term “router” refers to any network device that supports the routing function. These network devices can be Layer-3 switches, routers, or firewalls.

1.1.2 Principles

1. Basic Concepts

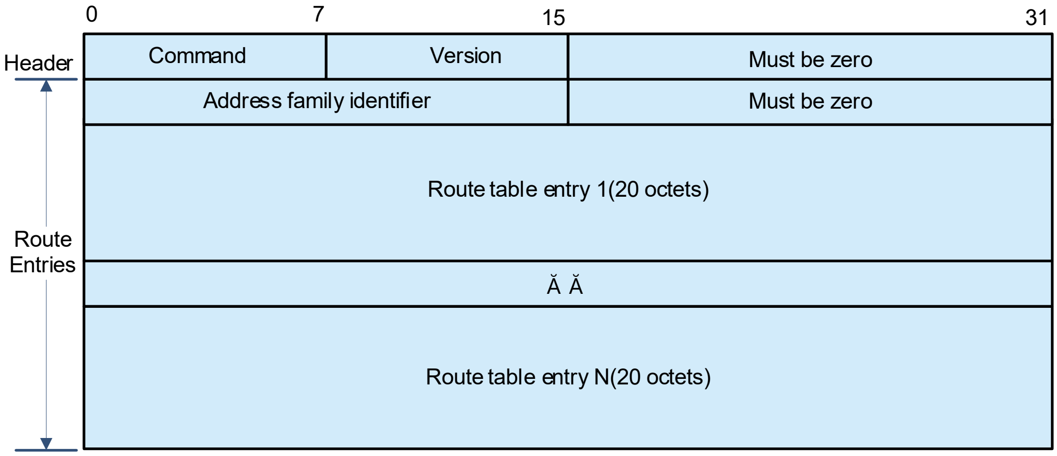
- IGP and EGP

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

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

- RIPng packet format

Figure 1-1 RIPng Packet Format


0
7
15
31
Header
Command
Version
Must be zero
Address family identifier
Must be zero
Route table entry 1(20 octets)
Route
Entries
Ă Ă
Route table entry N(20 octets)

RIPng packets can contain one or more routing table entries. The number of routing table entries depends on the size of the maximum transmission unit (MTU) value of the interface. Route table entry (RTE) is classified into two types:

- ○ Next hop RTE: Located in the foremost of a set of routing table entries with the same next hop, that is, the position of Route table entry 1 shown in Figure 1-1.
- ○ IPv6 prefix RTE: Located behind the next hop RTE. Multiple different IPv6 prefix RTEs can exist after a next hop RTE. An IPv6 prefix RTE describes the destination IP address, prefix length, route tag, and metric of an RIPng route.

Figure 1-2 Format of Next Hop RTE

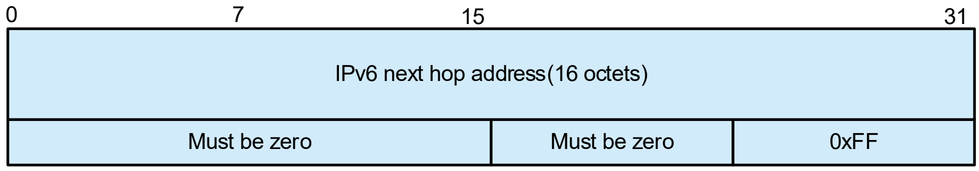
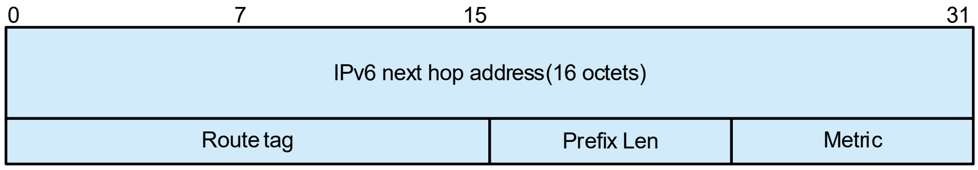


Figure 1-3 Format of IPv6 Prefix RTE



2. RIPng and RIP

RIP applies to IPv4 networks. Two RIP versions are available: RIPv1 and RIPv2.

RIPng is an extension of RIPv2 on the basis of IPv6. Both are similar in functions and configurations. The main differences are as follows:

- The UDP port ID of RIP is 520, and that of RIPng is 521.
- IPv6 features.
  - ○ The RIPv2 multicast address is 224.0.0.9, and the RIPng multicast address is FF02::9.
  - ○ The source address of RIPng route update packets is FE80::/10.

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.

- Routing switching process

  After RIPng is enabled on a router, the router sends a request packet to its neighbor router, requesting 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 router updates the local routing table, and sends an update packet to the neighbor router, informing the neighbor router of the route update information. After receiving the update packet, the neighbor router updates the local routing table, and sends the update packet to other adjacent routers. After receiving and processing an update advertisement, all the routers can obtain and retain the latest routing information.

- Periodical update

By default, periodical update is enabled for RIPng. Adjacent routers exchange complete routing information with each other every 30s, that is, the entire routing table is sent to neighbor routers.

ⓘ 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.

The timer details are as follows:

- ○ 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 cost 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.

- Default route

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

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

- Route redistribution

  For RIPng, 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 RIPng 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

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

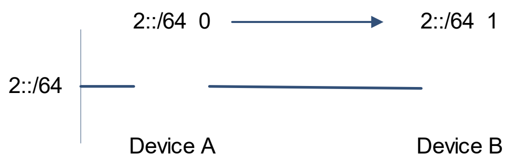
- Distance-vector algorithm

  RIPng 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 router obtains a route from its neighbor and adds the distance vector from itself to the neighbor to the route to form its own route.

  RIPng uses the hop count to evaluate the distance to the destination network. By default, the hop count from a router to its directly connected network is 0, the hop count from a router to a network that can be reached through a router is 1, and so on. That is, the metric is equal to the number of routers from the local network to the destination network. To restrict the convergence time, RIPng 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, RIPng cannot be applied on a large-scale network.

As shown in Figure 1-1, Device A is connected to the network 2::/64. Device B obtains the route (2::/64, 0) from Device A and adds the metric 1 to the route to obtain its own route (2::/64, 1), and the next hop points to Device A.

Figure 1-1 Diagram of Distance-vector Algorithm

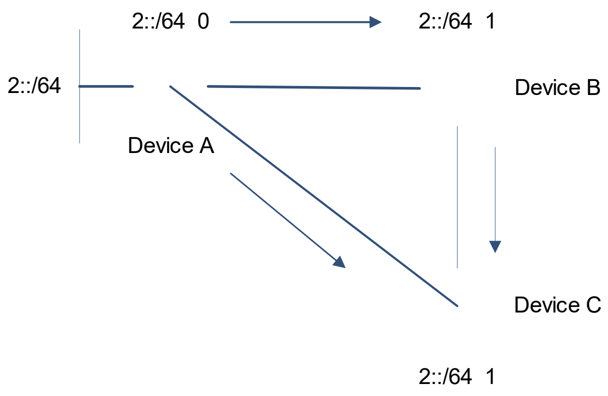


- Selecting the optimum route

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

  As shown in Figure 1-2, Device A is connected to the network 2::/64. Device C obtains the route (2::/64, 0) from Device A and the route (2::/64, 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 (2::/64, 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 router, the route with the smallest distance is preferentially selected.

Table 1-1 Distance-vector Table

Route Source	Default Distance
Directly-connected network	0

Route Source	Default Distance
Static route	1
OSPF route	110
IS-IS route	115
RIP route	120
Unreachable route	255

5. Avoiding Route Loops

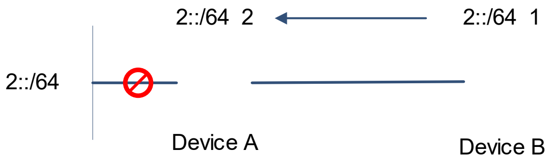
RIPng uses functions such as split horizon and poison reverse to avoid route loops.

- Route loop

An RIPng 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 2::/ 64, and sends an update packet every 30s. Device B receives the route to 2::/64 from Device A every 30s. If Device A is disconnected from 2::/64, the route to 2::/64 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 2::/64, Device B determines that the route to 2::/64 is valid within 180s and uses the update packet to send this route to Device A. As the route to 2::/64 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 2::/64 through Device A, and Device A determines that data can reach 2::/64 through Device B. In this way, a route loop is formed.

Figure 1-1 Diagram of Route Loop

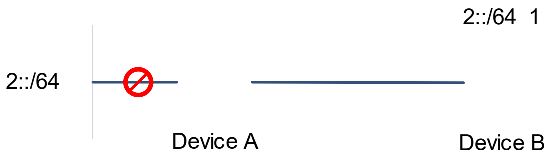


- Split horizon

Split horizon can prevent route loops. After split horizon is enabled, 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 Device B, Device B will not send the route to 2::/64 back to Device A. Device B will learn 180s later that 2::/64 is not reachable.

Figure 1-2 Diagram of Split Horizon



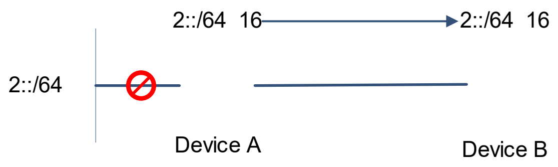
- Poison reverse

  Poison reverse can also prevent route loops. Compared with slit 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 poison reverse is enabled on Device A, if Device A detects a disconnection from 2::/64, Device A will not delete the route to 2::/64. Instead, Device A changes the number of hops to **16**, and advertises the route through the update packet. Upon receiving the update packet, Device B learns that 2::/64 is not reachable.

Figure 1-3 Diagram of Poison Reverse



1.1.3 Protocols and Standards

- RFC2080: RIPng for IPv6
- RFC 2081: RIPng Protocol Applicability Statement

1.2 Configuration Task Summary

The RIPng configuration includes the following tasks:

(1) Configuring RIPng Basic Functions

   a Enabling an RIPng Routing Process

   b Configuring RIPng on an Interface

   c (Optional) Configuring Split Horizon or Poison Reverse

   d (Optional) Configuring a Passive Interface

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

   o Generating a Default Route

   o Configuring External Route Redistribution

(3) (Optional) Configuring RIPng Route Filtering Rules

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

   o Configuring to Modify the Management Distance of an RIPng Route

   o Configuring to Modify the Metric Offset on an Interface

   o Configuring the Default Metric of a Route Redistributed to RIPng Metric

(5) (Optional) Modifying Timers

(6) (Optional) Enabling GR

(7) (Optional) Configuring a Super VLAN to Enable RIPng

1.3 Configuring RIPng Basic Functions

1.3.1 Overview

This function can be used to build an RIPng routing domain on the network, and routers in the domain obtain routes to a remote network through RIPng.

1.3.2 Restrictions and Guidelines

- IPv6 addresses must be configured.
- IPv6 unicast routes must be enabled.

1.3.3 Configuration Tasks

The basic function configuration of RIPng includes the following tasks:

(1) Enabling an RIPng Routing Process

(2) Configuring RIPng on an Interface

(3) (Optional) Configuring Split Horizon or Poison Reverse

(4) (Optional) Configuring a Passive Interface

1.3.4 Enabling an RIPng Routing Process

1. Overview

This command is used to create an RIPng routing process and enter routing process configuration mode.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable an RIPng routing process and enter route configuration mode.

ipv6 router rip

The RIPng routing process is disabled by default.

1.3.5 Configuring RIPng on an Interface

1. Overview

In RIPv2, the **network** command is configured in routing process configuration mode to define an IP address range. In RIPng, if the IP address of an interface belongs to this IP address range, RIPng automatically runs on this interface.

After RIPng runs on an interface, RIPng packets can be exchanged on the interface and RIPng can learn routes to the network segments directly connected to the device.

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 RIPng on an interface.

ipv6 rip enable

By default, an interface is not added to the RIPng process.

1.3.6 Configuring Split Horizon or Poison Reverse

1. Overview

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

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 will be changed to **16** (unreachable).

2. Restrictions and Guidelines

- You are advised to enable split horizon on the interfaces of broadcast type network (such as Ethernet) and point-to-point type network (such as PPP and HDLC). (Retain the default setting.)
- It is recommended that split horizon and poison reverse be disabled on an interface to a non-broadcast multi-access network such as FR and X.25; otherwise, some devices cannot learn the complete routing information.
- If the secondary IP address is configured for an interface connected to a non-broadcast network, it is recommended that split horizon and poison reverse be disabled.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the routing process configuration mode.

ipv6 router rip

(4) Configure split horizon.

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

By default, split horizon is enabled and poison reverse is disabled on an interface.

1.3.7 Configuring a Passive Interface

1. Overview

A passive interface is set with the boundary of RIPng routing domain. The network segment of the passive interface belongs to the RIPng routing domain, but RIPng packets cannot be sent over the passive interface.

The interface set to a passive interface suppresses RIPng update packets. The passive interface defines the boundary of RIPng routing domain to avoid unwanted flooding of RIPng packets. If the interface connection device does not run the RIPng 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

If RIPng routes need to be exchanged on an interface (such as the router interconnect interface) in the RIPng routing domain, this interface cannot be configured as a passive interface.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the routing process configuration mode.

ipv6 router rip

(4) Configure passive interfaces.

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

The passive interface function is disabled by default.

1.4 Configuring RIPng Route Distribution

1.4.1 Overview

RIPng can distribute the routes of other routing protocols or default routes in the local routing domain so that the devices in the routing domain can access other routing domains.

1.4.2 Configuration Tasks

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

- Generating a Default Route
- Configuring External Route Redistribution

1.4.3 Generating a Default Route

1. Overview

This function is used to introduce a default route to an AS edge router so that other routers in the RIPng domain access other AS domains through this AS edge router by default. In the routing table, a route to the destination network ::/0 is called default route. The default route can be learned from a neighbor device, or sent to a neighbor device. Please configure and distribute the default route according to the actual situation of networking, or specify the cost of the distributed default route.

2. Restrictions and Guidelines

- When there are no special requirements and this command is configured on the interface, an IPv6 default route is advertised to the external devices through this interface, but the route itself is not added to the route forwarding table of the device and the RIPng route database.
- To prevent occurrence of a route loop, once this command is configured on an interface, RIPng refuses to receive the default route updates advertised by neighbors.

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 external route redistribution.

ipv6 rip default-information { **only** | **originate** } [**metric** *metric-value*]

1.4.4 Configuring External Route Redistribution

1. Overview

This function is used to introduce external routes of the RIPng domain to the AS edge device.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the routing process configuration mode.

ipv6 router rip

(4) Generate a default route.

redistribute { **bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **static** } [**metric** *metric-value* | **route-map** *route-map-name*] *

The redistribution function is not configured by default. This function redistributes the routes of all subtypes of the specified routing process.

1.5 Configuring RIPng 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 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) 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 routing process configuration mode.

ipv6 router rip

(5) Configure to filter the received RIP routing information.

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

By default, the distribution list is disabled.

1.6 Configuring to Adjust RIPng Routing

1.6.1 Overview

Change the RIPng routes to enable the traffic pass through specified nodes or avoid passing through specified nodes. Change the sequence that a router selects various types of routes so as to change the priorities of RIPng routes.

1.6.2 Configuration Tasks

The configuration for modifying routing parameters includes the following tasks, and these tasks are optional. Select tasks for configuration according to actual condition.

- Configuring to Modify the Management Distance of an RIPng Route
- Configuring to Modify the Metric Offset on an Interface
- Configuring the Default Metric of a Route Redistributed to RIPng Metric

1.6.3 Configuring to Modify the Management Distance of an RIPng Route

1. Overview

This function is used to set the management distance of an RIPng route and change the priority of a router in routing.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the routing process configuration mode.

ipv6 router rip

(4) Configure to modify the management distance of an RIPng route.

distance *distance*

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

1.6.4 Configuring to Modify the Metric Offset on an Interface

1. Overview

Before a route is added to the routing table, the metric of the route must be added with the metric offset set on the interface. You can control the use of a route by setting the interface metric offset.

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 modify the metric offset to be added to the interface of an RIPng route.

ipv6 rip metric-offset *value*

By default, the metric on an interface is **1**.

1.6.5 Configuring the Default Metric of a Route Redistributed to RIPng

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

- Unless otherwise required, perform this configuration on an AS edge device to which external routes are introduced.
- If the metric is not specified during redistribution of a routing protocol process, RIPng uses the metric defined by the **default-metric** command. If the metric is specified, the metric defined by the **default-metric** command is overwritten by the specified metric.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the routing process configuration mode.

ipv6 router rip

(4) Configure the default metric of a route redistributed to RIPng.

default-metric *metric*

By default, the metric for route redistribution is 1.

1.7 Modifying Timers

1.7.1 Overview

By adjusting the timers, you can reduce the convergence time and fault rectification time of the routing protocol. For devices connected to the same network, values of the three RIPng timers must be the same. 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 2 Mbps (or above) link to reduce the convergence time of network routes.

1.7.2 Restrictions and Guidelines

- The RIPng basic functions 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 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the routing process configuration mode.

ipv6 router rip

(4) Configure to modify the RIPng timers.

timers *update invalid flush*

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

1.8 Enabling GR

1.8.1 Overview

GR ensures uninterrupted data transmission when the protocol is restarted. The GR period is the maximum time from restart of the RIPng process to completion of GR. During this period, the forwarding table before the restart is retained, and the RIPng route is restored so as to restore the RIPng state before the restart. After the restart period expires, RIPng exits the GR state and performs common RIPng operations.

1.8.2 Restrictions and Guidelines

- The RIPng basic functions must be configured.
- The GR period is at least twice the RIP route update period.
- The **graceful-restart grace-period** command allows you to explicitly modify the GR period. Note that GR must be completed before the invalid timer of the RIPng route expires. An inappropriate GR period cannot ensure uninterrupted data forwarding during the GR process. A typical case is as follows: If the GR period is longer than the duration of the invalid timer, GR is not completed when the invalid timer expires. The route is not re-advertised to the neighbor, and forwarding of the route of the neighbor stops after the invalid timer expires, causing interruption of data forwarding on the network. Unless otherwise required, you are not advised to adjust the GR period. If it is necessary to adjust the GR period, ensure that the GR period is at least twice the RIP route update period based on the configuration of the **timers** command. The GR period must be also smaller than the duration of the invalid timer.
- During the RIPng GR process, ensure that the network environment is stable.

1.8.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the routing process configuration mode.

ipv6 router rip

(4) Enable GR.

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

The GR function is enabled by default.

1.9 Configuring a Super VLAN to Enable RIPng

1.9.1 Overview

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 RIPng function does not need to be enabled on a super VLAN, and it is disabled by default. However, in some scenarios, the RIPng 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.

1.9.2 Restrictions and Guidelines

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

1.9.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the SVI interface mode.

interface vlan *vlan-id*

(4) Configure a super VLAN to enable RIPng.

ipv6 rip subvlan [**all |** *vlan-id*]

By default, the RIPng function is disabled on a super VLAN.

1.10 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

Command	Purpose
show ipv6 rip	Displays information about the RIPng process.
show ipv6 rip database	Displays the RIPng routing table.
debug ipv6 rip [interface *interface-type interface-number* | **nsm** | **restart** | **event** [**ipsec**]]	Debugs RIPng.

1.11 Configuration Examples

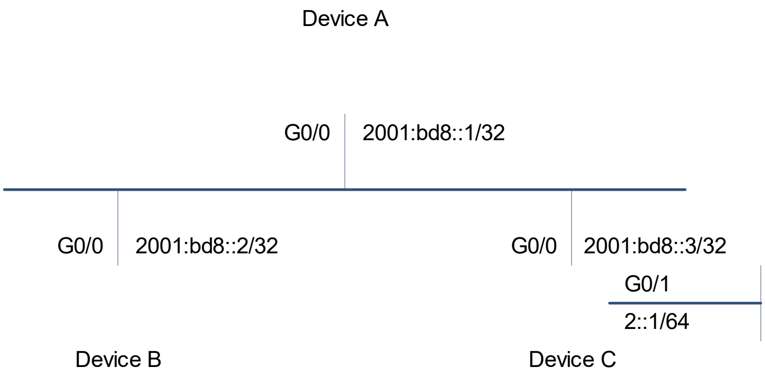
1.11.1 Configuring Basic Functions of RIPng

1. Requirements

On an IPv6 network, configure RIPng to realize internetworking.

2. Topology

Figure 1-1 Topology for Basic Features of RIPng



3. Notes

- Configure IPv6 addresses on the related devices.
- Enable the RIPng routing function on all the devices.

4. Procedure

(1) Configure an IPv6 address for each interface.

Configure Device A.

```
Device A> enable
Device A# configure terminal
Device A(config)# interface GigabitEthernet 0/0
Device A(config-if-GigabitEthernet 0/0)# ipv6 address 2001:db8::1/32
Device A(config-if-GigabitEthernet 0/0)# exit
```

Configure Device B.

```
Device B> enable
Device B# configure terminal
Device B(config)# interface GigabitEthernet 0/0
Device B(config-if-GigabitEthernet 0/0)# ipv6 address 2001:db8::2/32
Device B(config-if-GigabitEthernet 0/0)# exit
```

Configure Device C.

```
Device C> enable
Device C# configure terminal
Device C(config)# interface GigabitEthernet 0/0
Device C(config-if-GigabitEthernet 0/0)# ipv6 address 2001:db8::3/32
Device C(config-if-GigabitEthernet 0/0)# exit
Device C(config)# interface GigabitEthernet 0/1
Device C(config-if-GigabitEthernet 0/1)# ipv6 address 2::1/64
Device C(config-if-GigabitEthernet 0/1)# exit
```

(2) Enable the RIPng routing function on all the devices.

Configure Device A.

```
Device A(config)# ipv6 router rip
Device A(config-router)# exit
Device A(config)# interface GigabitEthernet 0/0
Device A(config-if-GigabitEthernet 0/0)# ipv6 rip enable
```

Configure Device B.

```
Device B(config)# ipv6 router rip
Device B(config-router)# exit
Device B(config)# interface GigabitEthernet 0/0
Device B(config-if-GigabitEthernet 0/0)# ipv6 rip enable
```

Configure Device C.

```
Device C(config)# ipv6 router rip
Device C(config-router)# exit
Device C(config)# interface GigabitEthernet 0/0
Device C(config-if-GigabitEthernet 0/0)# ipv6 rip enable
Device C(config)# interface GigabitEthernet 0/1
Device C(config-if-GigabitEthernet 0/1)# ipv6 rip enable
```

5. Verification

Check the routing tables of Device A, Device B, and Device C. Verify that RIPng has learned the routes to remote networks.

- Check the routing table of Device A.

```
Device A# show ipv6 route
IPv6 routing table name - Default - 6 entries
Codes:  C - Connected, L - Local, S - Static
    R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
    N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
    E1 - OSPF external type 1, E2 - OSPF external type 2
    SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
    IA - Inter area


R      2::/64 [120/2] via FE80::2D0:F8FF:FEFB:D521, GigabitEthernet 0/0
C      2001:DB8::/32 via GigabitEthernet 0/0, directly connected
L      2001:DB8::1/128 via GigabitEthernet 0/0, local host
C      FE80::/10 via ::1, Null0
C      FE80::/64 via GigabitEthernet 0/0, directly connected
L      FE80::2D0:F8FF:FEFB:E7CE/128 via GigabitEthernet 0/0, local host
```

- Check the routing table of Device B.

```
Device B# show ipv6 route

IPv6 routing table name - Default - 6 entries
Codes:  C - Connected, L - Local, S - Static
        R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area

R      2::/64 [120/2] via FE80::2D0:F8FF:FEFB:D521, GigabitEthernet 0/0
C      2001:DB8::/32 via GigabitEthernet 0/0, directly connected
L      2001:DB8::2/128 via GigabitEthernet 0/0, local host
C      FE80::/64 via GigabitEthernet 0/0, directly connected
L      FE80::2D0:F8FF:FEFB:C9BA/128 via GigabitEthernet 0/0, local host
```

- Check the routing table of Device C.

```
Device C# show ipv6 route

IPv6 routing table name - Default - 9 entries
Codes:  C - Connected, L - Local, S - Static
        R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area

C      2::/64 via GigabitEthernet 0/1, directly connected
L      2::2/128 via GigabitEthernet 0/1, local host
C      2001:DB8::/32 via GigabitEthernet 0/0, directly connected
L      2001:DB8::3/128 via GigabitEthernet 0/0, local host
C      FE80::/10 via ::1, Null0
C      FE80::/64 via GigabitEthernet 0/0, directly connected
L      FE80::2D0:F8FF:FEFB:D521/128 via GigabitEthernet 0/0, local host
C      FE80::/64 via GigabitEthernet 0/1, directly connected
L      FE80::2D0:F8FF:FEFB:D521/128 via GigabitEthernet 0/1, local host
```

6. Configuration Files

- Device A configuration file

```
!
ipv6 router rip
!
interface GigabitEthernet 0/0
 ipv6 address 2001:db8::1/32
 ipv6 rip enable
!
```

- Device B configuration file

```
!
ipv6 router rip
!
interface GigabitEthernet 0/0
 ipv6 address 2001:db8::2/32
 ipv6 rip enable
!
```

- Device C configuration file

```
!
ipv6 router rip
!
interface GigabitEthernet 0/0
 ipv6 address 2001:db8::3/32
 ipv6 rip enable
!
interface GigabitEthernet 0/1
 ipv6 address 2::1/64
 ipv6 rip enable
!
```

7. Common Errors

- The IPv6 address is not configured on an interface.
- The interface used for interworking between devices is configured as a passive interface.

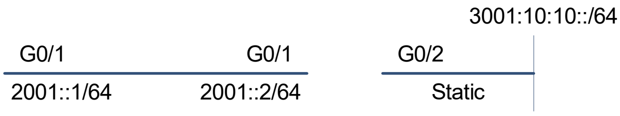
1.11.2 Advertising Default Routes/External Routes

1. Requirements

On a network adopting OSPFv3 networking, Device A and Device B are egress devices on the network, Device A is the default egress used to advertise the default route to Device B, and Device B communicates with the internal network through a static route.

2. Topology

Figure 1-1 Topology for Advertising Default Routes/External Routes



3. Notes

- Configure interface IPv6 addresses for all devices (omitted).
- Configure the RIPng basic functions on all devices (omitted).
- Redistribute the static route on Device B.
- On the GigabitEthernet 0/1 interface of Device A, configure advertisement of the default route.

4. Procedure

(1) Configure redistribution of a static route on Device B.

```
Device B> enable
Device B# configure terminal
Device B(config)# ipv6 router rip
Device B(config-router)# redistribute static
```

(2) Configure redistribution of a default route on Device A.

```
Device A> enable
Device A# configure terminal
Device A(config)# interface GigabitEthernet 0/1
Device A(config-if-GigabitEthernet 0/1)# ipv6 rip default-information
originate
```

5. Verification

Check the routing tables on Device A and Device B, and verify that Device A can learn the route 3001:10:10::/64, and Device B can learn the default route ::/0.

```
Device A# show ipv6 route rip

IPv6 routing table name - Default - 17 entries
Codes:  C - Connected, L - Local, S - Static
        R - RIP, O - OSPF, B - BGP, I - IS-IS
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area
R       3001:10:10::/64 [120/2] via FE80::2D0:F8FF:FE22:334A, GigabitEthernet 0/1
Device B# show ipv6 route rip

IPv6 routing table name - Default - 17 entries
Codes:  C - Connected, L - Local, S - Static
        R - RIP, O - OSPF, B - BGP, I - IS-IS
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area
R       ::/0 [120/2] via FE80::21A:A9FF:FE41:5B06, GigabitEthernet 0/1
```

6. Configuration Files

- Device A configuration file

```
!
interface GigabitEthernet 0/1
 ipv6 rip default-information originate
!
```

- Device B configuration file

```
!
ipv6 router rip
 redistribute static
!
```