Contents

1 IP Routing Overview

This chapter describes IP routing and how it is a basic element of data communication networks.

1.1 Introduction to IP Routing

According to the destination address, routes are classified into one of the following types:

- Network segment route

  The destination is a network segment. In this case, if the destination is an IPv4 address, the subnet mask is less than 32 bits, and if the destination is an IPv6 address, the prefix length is less than 128 bits.

- Host route

  The destination is a host. In this case, if the destination is an IPv4 address, the subnet mask is 32 bits, and if the destination is an IPv6 address, the prefix length is 128 bits.

According to whether the destination directly connects to a router, routes are classified into one of the following types:

- Direct route

  The router directly connects to the network where the destination is located.

- Indirect route

  The router indirectly connects to the network where the destination is located.

According to the destination address type, routes are classified into one of the following types:

- Unicast route

  The destination address is a unicast address.

- Multicast route

  The destination address is a multicast address.

1.2 Principles

1.2.1 Routers and Routing Principles

On the Internet, network connecting devices such as hubs, bridges, switches, and routers control traffic and ensure data transmission quality. Each of these devices serves a different role, but for a common purpose: forming a functioning network. The following describes a router's role in a network, and the purpose and nature of routes.

A router selects routes and forwards packets. Upon receiving a packet, a router selects a proper path, which may have one or multiple hops, to send the packet to the next router according to the destination address in the packet. The last router is responsible for sending the packet to the destination host.

A route is a path along which packets are sent from the source to the destination. When multiple routes are available to send packets from a router to the destination, the router can select the optimal route from an IP routing table. Optimal route selection depends on routing protocol preferences and metrics of routes. When multiple routes have the same routing protocol preference and metric, load balancing can be implemented among these routes to relieve network pressure. When multiple routes have different routing protocol preferences and metrics, route backup can be implemented among these routes to improve network reliability.

1.2.2 Static Routes and Dynamic Routes

Routers support direct, static, and dynamic routes. Dynamic routes include Routing Information Protocol (RIP) routes, Open Shortest Path First (OSPF) routes, Intermediate System-to-Intermediate System (IS-IS) routes, and Border Gateway Protocol (BGP) routes.

Differences Between Static Routes and Dynamic Routes

Routing protocols are the rules used by routers to discover routes, generate routing tables, and guide packet forwarding. Routes are classified into the following types according to their origin:

- Direct routes: are discovered by link layer protocols.
- Static routes: are manually configured by network administrators.
- Dynamic routes: are discovered by dynamic routing protocols.

Static routes are easy to configure, have low system requirements, and apply to simple, stable, and small networks. The disadvantage of static routes is that they require subsequent maintenance as they cannot automatically adapt to network topology changes.

Dynamic routing protocols have routing algorithms. Therefore dynamic routes can automatically adapt to network topology changes and apply to networks on which Layer 3 devices are deployed. The disadvantages of dynamic routes are that they are complex to configure, have higher system requirements than static ones, and consume network and system resources.

Classification of Dynamic Routing Protocols

Dynamic routing protocols are classified into types based on the following two criteria.

According to the application range, dynamic routing protocols are classified into the following types:

- Interior Gateway Protocols (IGPs)

  Run inside an autonomous system (AS), including RIP, OSPF, and IS-IS.
- Exterior Gateway Protocols (EGPs)

  Run between ASs, including BGP.

According to the type of algorithm they use, dynamic routing protocols are classified into the following types:

- Distance-vector routing protocols

  Include RIP and BGP. BGP is also called a path-vector protocol.
- Link-state routing protocols

  Include OSPF and IS-IS.

The preceding algorithms differ mainly in route discovery and calculation methods.

1.2.3 Routing Table and FIB Table

Routers forward packets based on routing tables and forwarding information base (FIB) tables. Each router maintains at least one routing table and one FIB table. Routers select routes based on routing tables and forward packets based on FIB tables.

Routing Table

Each router maintains a local core routing table (namely, an IP routing table), and each routing protocol maintains its own routing table.

- Local core routing table

  A router uses the local core routing table to store preferred routes. The router then sends the preferred routes to the FIB table to guide packet forwarding. The router selects routes according to the priorities of protocols and costs stored in the routing table.

  📖 **NOTE:**

A router that supports Layer 3 Virtual Private Network (L3VPN) maintains a local core routing table for each VPN instance.

- Protocol routing table

  A protocol routing table stores routing information discovered by the protocol.

  A routing protocol can import and advertise routes that are discovered by other routing protocols. For example, if a router running the Open Shortest Path First (OSPF) protocol needs to use OSPF to advertise direct routes, static routes, or Intermediate System-Intermediate System (IS-IS) routes, the router must import the routes into the OSPF routing table.

Routing Table Contents

You can run the **display ip routing-table** command on a router to view basic information about the routing table of the router. The command output is as follows:

```
<Huawei> display ip routing-table
Proto: Protocol        Pre: Preference
Route Flags: R - relay, D - download to fib, T - to vpn-instance
------------------------------------------------------------------------------
Routing Table: _public_
         Destinations : 14       Routes : 14

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        0.0.0.0/0   Static  60   0          RD   10.137.216.1    Vlanif20
     10.10.10.0/24  Direct  0    0           D   10.10.10.10     Vlanif20
    10.10.10.10/32  Direct  0    0           D   127.0.0.1       InLoopBack0
   10.10.10.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
     10.10.11.0/24  Direct  0    0           D   10.10.11.1      LoopBack0
     10.10.11.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
   10.10.11.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
   10.137.216.0/23  Direct  0    0           D   10.137.217.208  Vlanif20
 10.137.217.208/32  Direct  0    0           D   127.0.0.1       InLoopBack0
 10.137.217.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

A routing table contains the following key data for each IP packet:

- Destination: identifies the destination IP address or destination network address of an IP packet.
- Mask: supplements the destination address to specially identify the address of the network segment where the destination host or router resides.

  The network segment address of a destination host or router is obtained through the "AND" operation on the destination address and network mask. For example, if the destination address is 10.1.1.1 and the mask is 255.255.255.0, the address of the network segment where the host or router resides is 10.1.1.0.

  The network mask is composed of several consecutive 1s. These 1s can be expressed in either the dotted decimal notation or the number of consecutive 1s in the mask. For example, the network mask can be expressed either as 255.255.255.0 or 24.
- Proto: indicates the protocol through which routes are learned.
- Pre: indicates the routing protocol preference of a route. There may multiple routes to the same destination, which have different next hops and outbound interfaces. These routes may be discovered by different routing protocols or manually configured. A router selects the route with

the highest preference (the smallest value) as the optimal route. For the routing protocol preference, see 1.2.5 Routing Protocol Preference.

- Cost: indicates the route cost. When multiple routes to the same destination have the same preference, the route with the lowest cost is selected as the optimal route.

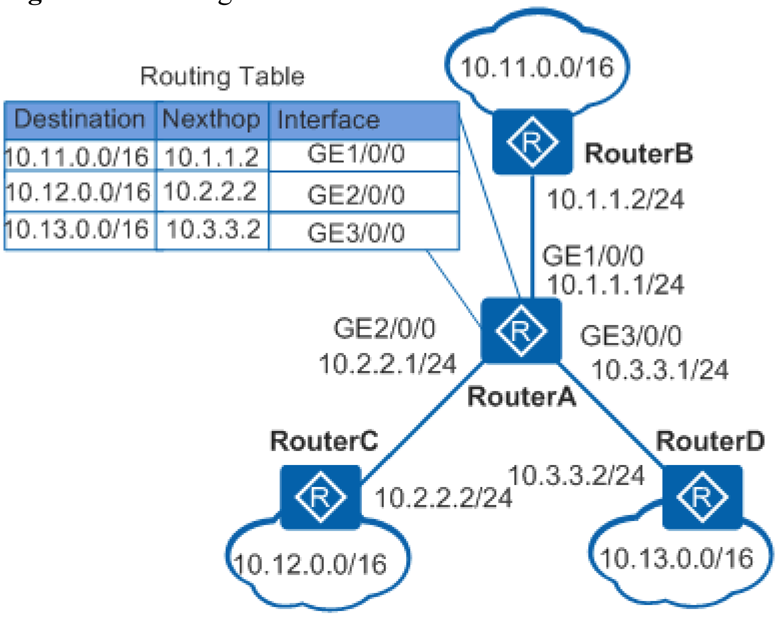
NOTE:

The Preference value is used to compare the preferences of different routing protocols, while the Cost value is used to compare the preferences of different routes of the same routing protocol.

- NextHop: indicates the IP address of the next device that an IP packet passes through.
- Interface: indicates the outbound interface through which an IP packet is forwarded.

In Figure 1-1, the routing table of RouterA shows that it connects to three networks, so it has three IP addresses and three outbound interfaces.

Figure 1-1 Routing table



Routing Table

Destination	Nexthop	Interface
10.11.0.0/16	10.1.1.2	GE1/0/0
10.12.0.0/16	10.2.2.2	GE2/0/0
10.13.0.0/16	10.3.3.2	GE3/0/0

Automatic Restoration After the Number of Routes Exceeds the Upper Limit

A local core routing table stores routes of different routing protocols. If the number of routes in the local core routing table reaches the upper limit, no more route can be added to the table. The local core routing table has the following route limitations:

- System route limit: specifies the maximum number of routes supported by the system.
- System route prefix limit: specifies the range of prefixes for all the routes supported by the system.
- Multicast IGP route limit: specifies the maximum number of multicast IGP routes.
- Multi-topology route limit: specifies the maximum number of multi-topology routes.
- Private network route limit: specifies the maximum number of private network routes supported by the system.
- VPN route limit: specifies the maximum number of VPN routes supported by the system.
- VPN route prefix limit: specifies the range of prefixes for all the VPN routes supported by the system.

If a protocol fails to add routes to the local core routing table due to a specific route limitation, the system records the failure with the protocol name and routing table ID.

After routes of protocols are deleted from the local core routing table, and the number of routes falls below the upper limit, the system prompts all the protocols that failed to add routes to the local core routing table to re-add the routes to the local core routing table. This process restores most of the routes in the local core routing table. The size of released table space determines whether all routes in the local core routing table can be restored.

Matching with FIB Table

After selecting an optimal route from the routing table, a router sends it to the FIB table. When receives a packet, the router compares it against the FIB table to find the optimal route to forward the packet.

Each entry in the FIB table contains the physical or logical interface through which a packet is sent to a network segment or host to reach the next router. An entry can also indicate whether the packet can be sent to a destination host in a directly connected network.

The router performs the "AND" operation on the destination address in the packet and the network mask of each entry in the FIB table. The router then compares the result of the "AND" operation with the entries in the FIB table to find a match and chooses the optimal route to forward packets according to the longest match rule.

For example, assume that a router has the following routing table:

```
Routing Tables:
Destination/Mask    Proto  Pre  Cost     Flags NextHop         Interface
 0.0.0.0/0      Static   60   0       D   192.168.0.2      GigabitEthernet1/0/0
 10.8.0.0/16    Static   60   3       D   192.168.0.2      GigabitEthernet1/0/0
 10.9.0.0/16    Static   60   50      D   172.16.0.2       GigabitEthernet3/0/0
 10.9.1.0/24    Static   60   4       D   192.168.0.2      GigabitEthernet2/0/0
 10.20.0.0/16   Direct   0    0       D   172.16.0.1       GigabitEthernet4/0/0
```

After receiving a packet carrying the destination address 10.9.1.2, the router searches the following FIB table:

```
 FIB Table:
 Total number of Routes : 5
Destination/Mask   Nexthop         Flag TimeStamp     Interface              TunnelID
0.0.0.0/0            192.168.0.2       SU   t[37]         GigabitEthernet1/0/0  0x0
10.8.0.0/16          192.168.0.2       DU   t[37]         GigabitEthernet1/0/0  0x0
10.9.0.0/16          172.16.0.2        DU   t[9992]       GigabitEthernet3/0/0  0x0
10.9.1.0/24          192.168.0.2       DU   t[9992]       GigabitEthernet2/0/0  0x0
10.20.0.0/16         172.16.0.1        U    t[9992]       GigabitEthernet4/0/0  0x0
```

The router performs the "AND" operation on the destination address 19.9.1.2 and the masks 0, 16, and 24 to obtain the network segment addresses: 0.0.0.0/0, 10.9.0.0/16, and 10.9.1.0/24. The three addresses match three entries in the FIB table. The router chooses the entry 10.9.1.0/24 according to the longest match rule, and forwards the packet through GigabitEthernet2/0/0.

1.2.4 Route Iteration

Routes can be used to forward traffic only when they have directly connected next hops. However, this condition may not be met when routes are generated. The system then needs to search for directly connected next hops and corresponding outbound interfaces. This process is called route iteration. In most cases, BGP routes, static routes, and user network routes (UNRs) do not have directly connected next hops, and route iteration is required. The following examples demonstrate how route iteration generates an FIB entry.

A next-hop IP address of a BGP route is often the IP address of an indirectly connected peer's loopback interface, and therefore the BGP route needs to be iterated. The system searches the IP routing table for a direct route (an IGP route in most cases) that is destined for the next-hop IP address of the BGP route and then adds the next-hop IP address and outbound interface of the IGP route to the IP routing table. This generates a FIB entry.

A next-hop IP address of a BGP VPN route is often the IP address of an indirectly connected PE's loopback interface, and the BGP route needs to be iterated to a tunnel. The system searches the tunnel list for a tunnel that is destined for this loopback IP address and then adds the tunnel information to the routing table. This generates a FIB entry.

1.2.5 Routing Protocol Preference

Routing protocols (including static routing) may discover different routes to the same destination, but not all routes are optimal. Only one routing protocol at a time determines the optimal route to a destination. To select the optimal route, each routing protocol (including static routing) is assigned a preference (a smaller value indicates a higher preference). When multiple routing information sources coexist, the route discovered by the routing protocol with the highest preference is selected as the optimal route and added to the local routing table.

Routers define external preference and internal preference. External preference is manually configured for each routing protocol. Table 1-1 lists the default external preferences of routing protocols.

Table 1-1 Routing protocols and their default external preferences

Routing Protocol or Route Type	Default External Preference
Direct	0
OSPF	10
IS-IS	15
Static	60
RIP	100
OSPF ASE	150
OSPF NSSA	150
IBGP	255
EBGP	255

NOTE:

In Table 1-1, the value 0 indicates direct routes and the value 255 indicates routes learned from unreliable sources. A smaller value indicates a higher preference.

You can manually configure the external preference of all routing protocols except direct routes. The preference for each static route varies.

Internal preferences of routing protocols cannot be manually configured. Table 1-2 lists the internal preferences of routing protocols.

Table 1-2 Internal preferences of routing protocols

Routing Protocol or Route Type	Internal Preference

Routing Protocol or Route Type	Internal Preference
Direct	0
OSPF	10
IS-IS Level-1	15
IS-IS Level-2	18
Static	60
RIP	100
OSPF ASE	150
OSPF NSSA	150
IBGP	200
EBGP	20

During route selection, a router first compares the external preferences of routes. When the same external preference is set for different routing protocols, the router selects the optimal route based on the internal preference. For example, assume that there are two routes to 10.1.1.0/24: a static route and an OSPF route. Both routes have the same external preference: 5. In this case, the router determines the optimal route based on the internal preference listed in Table 1-2. An OSPF route has an internal preference of 10, and a static route has an internal preference of 60. This indicates that the OSPF route has a higher preference than the static route, so the router selects the OSPF route as the optimal route.

1.2.6 Route Metric

A route metric specifies the cost of a route to a specified destination address. The following factors often affect the route metric:

- Path length

  Path length is the most common factor that affects the route metric. Link-state routing protocols allow you to assign a link cost for each link to identify the path length of a link. In this case, the path length is the sum of the link costs of all the links that packets pass through. Distance-vector routing protocols use the hop count to identify the path length. The hop count is the number of devices that packets pass through from the source to the destination. For example, the hop count from a router to its directly connected network is 0, and the hop count from a router to a network that can be reached through just one other router is 1. Other lengths can be deduced in the same manner.

- Network bandwidth

  Network bandwidth is the transmission capability of a link. For example, a 10-Gigabit link has a higher transmission capability than a 1-Gigabit link. Although bandwidth defines the maximum transmission rate of a link, routes over high-bandwidth links are not necessarily better than routes over low-bandwidth links. For example, when a high-bandwidth link is congested, forwarding packets over this link will require more time.

- Load

  The load is the degree to which a network resource is busy. You can calculate the load by calculating the CPU usage and packets processed per second. Continually monitoring the CPU usage and packets processed per second helps you learn more about network usage.

- Communication cost

  The communication cost is the operating cost of a route over a link. The communication cost is another important indicator, especially if you do not care about network performance but are concerned about the operating expenditure.

1.2.7 Load Balancing and Route Backup

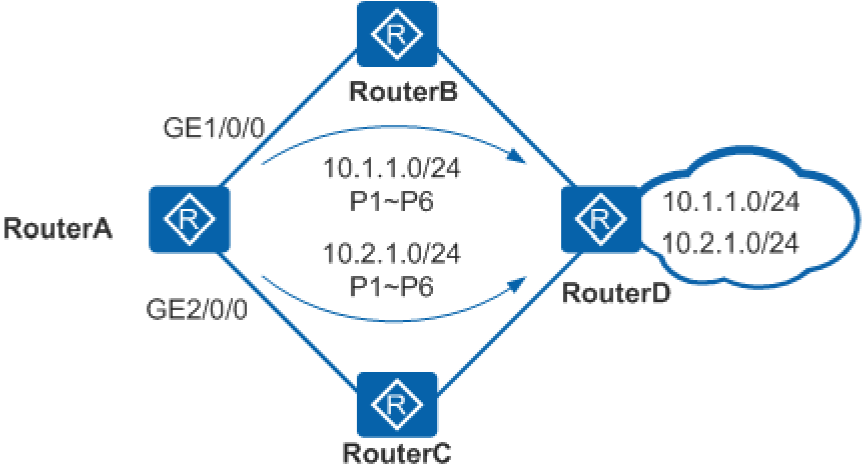
When multiple routes have the same routing protocol preference and metric, these routes are called equal-cost routes, among which load balancing can be implemented. When multiple routes have different routing protocol preferences and metrics, route backup can be implemented among these routes.

Load Balancing

Routers support the multi-route mode, which allows you to configure multiple routes with the same destination and preference. If the destinations and costs of multiple routes discovered by the same routing protocol are the same, load balancing can be performed among the routes.

During load balancing, a router forwards packets based on the packets' 5-tuple (source IP address, destination IP address, source port, destination port, and transport protocol). When the 5-tuple information is the same, the router always chooses the next-hop address that is the same as the last one to send packets. When the 5-tuple information is different, the router forwards packets over idle paths.

Figure 1-2 Networking diagram of load balancing



In the example shown in Figure 1-2, RouterA forwards the first packet P1 to 10.1.1.0/24 through GE1/0/0 and needs to forward subsequent packets to 10.1.1.0/24 and 10.2.1.0/24 respectively. The forwarding process is as follows:

- If RouterA finds that 5-tuple information of P2 destined for 10.1.1.0/24 is the same as that of P1 destined for 10.1.1.0/24, it forwards P2 and subsequent packets destined for 10.1.1.0/24 through GE1/0/0.
- If RouterA finds that 5-tuple information of P1 destined for 10.2.1.0/24 is different from that of P1 destined for 10.1.1.0/24, it forwards P1 and subsequent packets destined for 10.2.1.0/24 through GE2/0/0.

NOTE:

The number of equal-cost routes for load balancing varies with products.

Route Backup

Route backup can improve network reliability. You can configure multiple routes to the same destination as required. The route with the highest preference functions as the primary route, and other routes with lower preferences function as backup routes.

A router generally uses the primary route to forward data. When the primary link fails, the primary route becomes inactive. The router selects a backup route with the highest preference to forward data. In this manner, data is switched from the primary route to a backup route. When the primary link recovers, the router selects the primary route to forward data again because the primary route has the highest preference. Data is then switched back from the backup route to the primary route.

1.2.8 IP FRR

Definition

When a router detects a fault at the physical or data link layer, IP fast reroute (FRR) enables the router to report the fault to the upper-layer routing system, and to immediately use a backup link to forward packets. IP FRR is a method that implements fast route backup.

Purpose

On traditional IP networks, when a fault occurs at the lower layer of the forwarding link, the physical interface on the router becomes Down. After the router detects the fault, it informs the upper-layer routing system to recalculate routes and then update routing information. Usually, it takes the routing system several seconds to re-select an available route.

Second-level convergence is intolerable to services that are sensitive to delay and packet loss because it may lead to service interruption. For example, Voice over Internet Protocol (VoIP) services are only tolerant of millisecond-level interruption.

IP FRR resolves this by ensuring that the forwarding system rapidly detects a link fault and then uses a backup route to restore services as soon as possible.

IP FRR Classification and Implementation

IP FRR, which is designed for routes on IP networks, is classified into IP FRR on public networks and IP FRR on private networks.

- IP FRR on public networks protects routers on public networks.
- IP FRR on private networks protects Customer Edges (CEs).

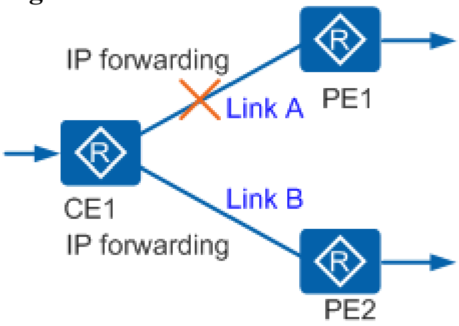
IP FRR is implemented as follows:

1. If the primary link is available, you can configure an IP FRR policy to provide the forwarding information of the backup route to the forwarding engine.
2. If the forwarding engine detects a link fault, the engine uses the backup link to forward traffic before the routes on the control plane converge.

IP FRR Typical Applications

In the example shown in Figure 1-3, IP FRR is configured to improve network reliability. CE1 is dual-homed to PE1 and PE2 and has two outbound interfaces and two next hops configured. That is, link B functions as the backup of link A. When link A fails, traffic can be rapidly switched to link B.

Figure 1-3 IP FRR



1.2.9 Route Convergence

Definition

Route convergence is the action of recalculating routes to replace existing routes in the case of network topology changes. The integration of multiple network services urgently requires differentiated services. Routes for key services, such as Voice over IP (VoIP), video conferences, and multicast services, need to be converged rapidly, while routes for common services can be converged relatively slowly. In this case, the system needs to converge routes based on their convergence priorities to improve network reliability.

Priority-based convergence is a mechanism that allows the system to converge routes based on the convergence priority. You can set different convergence priorities for routes: critical, high, medium, and low (in descending order of priority). The system then converges routes according to the assigned scheduling weight to guide service forwarding.

Principles

Routing protocols first compute and deliver routes of high convergence priority to the system. You can reconfigure the scheduling weight values as required. Table 1-3 lists the default convergence priorities of public routes.

Table 1-3 Default convergence priorities of public routes

Routing Protocol or Route Type	Convergence Priority
Direct	high
Static	medium
32-bit host routes of OSPF and IS-IS	medium
OSPF routes (excluding 32-bit host routes)	low
IS-IS routes (excluding 32-bit host routes)	low
RIP	low
BGP	low

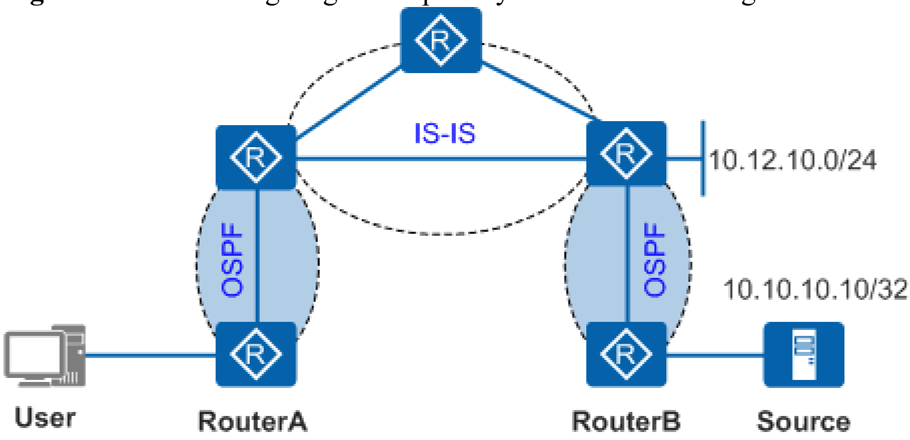
NOTE:

For private routes, only the convergence priorities of 32-bit OSPF and IS-IS host routes are identified as medium, and the convergence priorities of the other routes are identified as low.

Priority-based Route Convergence

Figure 1-4 shows a networking arrangement for multicast services. OSPF and IS-IS run on the network. The receiver connects to RouterA, and the multicast source server 10.10.10.10/32 connects to RouterB. The route to the multicast source server must be converged faster than other routes such as 10.12.10.0/24. You can set the convergence priority of route 10.10.10.10/32 to be higher than that of route 10.12.10.0/24. When routes are converged on the network, the route to the multicast source server 10.10.10.10/32 is converged first. This ensures the transmission of multicast services.

Figure 1-4 Networking diagram of priority-based route convergence



1.2.10 Default Routes

Default routes are special routes used only when packets to be forwarded do not match any routing entry in a routing table. If the destination address of a packet does not match any entry in the routing table, the packet is sent through a default route. If no default route exists and the destination address of the packet does not match any entry in the routing table, the packet is discarded. An Internet Control Message Protocol (ICMP) packet is then sent, informing the originating host that the destination host or network is unreachable.

In a routing table, a default route is the route to network 0.0.0.0 (with the mask 0.0.0.0). You can run the **display ip routing-table** command to check whether a default route is configured. Generally, administrators can manually configure default static routes. Default routes can also be generated through dynamic routing protocols such as OSPF and IS-IS.

1.2.11 Route Importing

Different routing protocols using different algorithms may discover different routes. If multiple routing protocols run on a large network, the routing protocols need to re-advertise the routes they discover.

Each routing protocol can import routes discovered by other routing protocols, direct routes, and static routes.

1.2.12 Autonomous System

An Autonomous System (AS) is a set of IP networks and routers under one administration entity and with common routing policies.

Each AS supports multiple IGPs. All the networks in an AS are assigned the same AS number and managed by the same administration group. Two types of AS numbers are available: a 2-byte AS number (with a number range from 1 to 65535) and a 4-byte AS number (with a number range from 1 to 4294967295). Available AS numbers can become exhausted thereby 2-byte AS numbers need to be extended to 4-byte AS numbers. A 4-byte AS number is shown in the X.Y format, where X ranges from 1 to 65535 and Y ranges from 0 to 65535.

Based on the network where they are used, AS numbers are classified into two types. Table 1-4 lists the two types of AS numbers and their ranges.

Table 1-4 AS number types and ranges

AS Number Type	2-Byte AS Number	4-Byte AS Number
Public AS number	1 to 64511	1 to 64511, 65536 to 4294967295
Private AS number	64512 to 65535	64512 to 65535

1.2.13 Indirect Next Hop

Definition

Indirect next hop is a technique that speeds up route convergence. It can change the direct association between route prefixes and next hops into an indirect association. Then next-hop information can be refreshed independently, and the prefixes of the same next hop do not need to be refreshed one by one. This speeds up route convergence.

Purpose

In the scenario requiring route iteration, when IGP routes or tunnels are switched, FIB entries are quickly refreshed. This implements fast traffic convergence and reduces the impact on services.

Mapping Between the Route Prefix and Next Hop

The mapping between the route prefix and next hop is the basis of indirect next hop. To meet the requirements of route iteration and tunnel iteration in different scenarios, next-hop information involves the address family, original next-hop address, and tunnel policy. The system assigns an index to information about each next hop, performs route iteration, notifies the iteration result to the routing protocols, and distributes FIB entries.

On-Demand Route Iteration

In on-demand route iteration, when a dependent route is changed, only the next hop related to the dependent route is re-iterated. If the destination address of a route is the original next-hop address or network segment address of next-hop information, route changes affect the iteration result of next-hop information. Otherwise, route changes do not affect next hop-information. Therefore, when a route changes, you can re-iterate only the related next hop according to the destination address of the route.

In tunnel iteration, when a tunnel alternates between Up and Down, you just need to re-iterate the next-hop information whose original next-hop address is the same as the destination address of the tunnel.

Iteration Policy

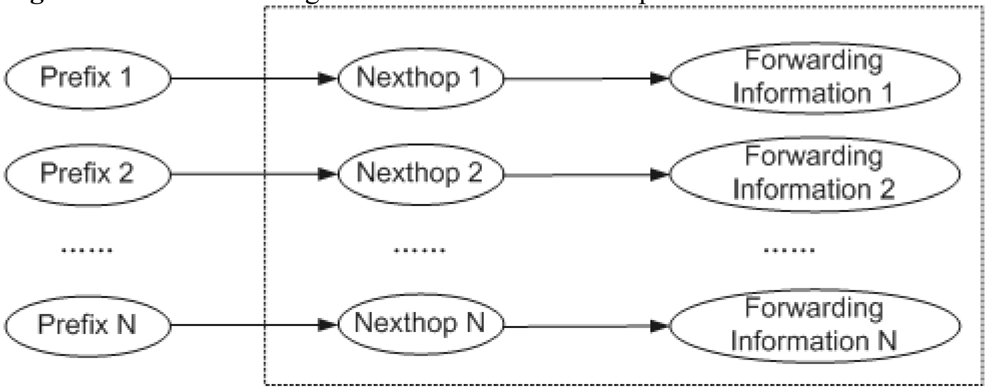
An iteration policy controls the next-hop iteration result to meet the requirements of different application scenarios. In route iteration, iteration behaviors do not need to be controlled by the iteration policy. Instead, iteration behaviors only need to comply with the longest matching rule. The iteration policy needs to be used only when VPN routes are iterated to tunnels.

By default, the system selects LSPs for a VPN without performing load balancing. If load balancing or other types of tunnels are required, you need to configure a tunnel policy and bind the tunnel policy to a tunnel. After a tunnel policy is applied, the system uses the tunnel bound in the tunnel policy or selects a tunnel according to the priorities of different types of tunnels.

Refreshment of Indirect Next Hop

On the forwarding plane, public network routes are forwarded based on the next hop and outbound interface while VPN routes are forwarded based on the public network tunnel in addition to the next hop and outbound interface. Before indirect next hop is used, forwarding information, including the next hop, outbound interface, and tunnel token, needs to be added into the FIB entry using the route prefix. In this case, the route convergence speed is relevant to the number of route prefixes. After indirect next hop is used, many route prefixes correspond to a shared next hop. Forwarding information is added into the FIB entry using the next hop, and the traffic with the relevant route prefixes can be switched simultaneously. Therefore, the route convergence speed becomes faster.

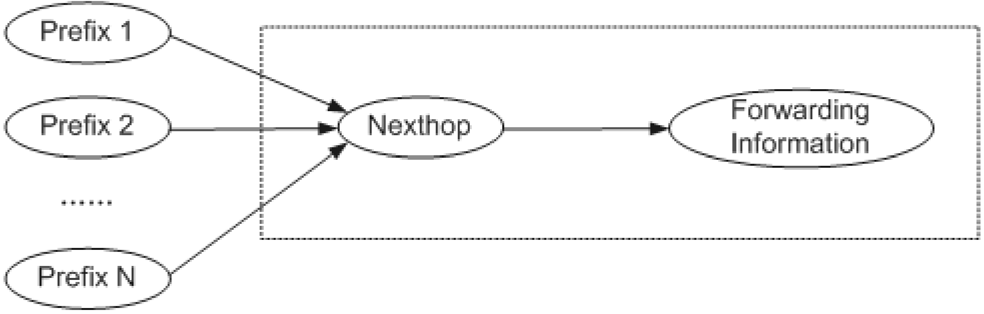
Figure 1-5 Schematic diagram before indirect next hop is used



As shown in Figure 1-5, before indirect next hop is used, prefixes are independent of each other, each corresponding to its next hop and forwarding information. When a dependent route changes, the next hop corresponding to each prefix is iterated and forwarding information is updated based on the prefix. In this case, the convergence speed is related to the number of prefixes.

Actually, prefixes of a BGP neighbor have the same next hop, forwarding information, and refreshed forwarding information.

Figure 1-6 Schematic diagram after indirect next hop is used



As shown in Figure 1-6, after indirect next hop is used, prefixes of a BGP neighbor share a next hop. When a dependent route changes, only the shared next hop is iterated and forwarding information is updated based on the next hop. In this case, traffic of all prefixes can be converged simultaneously. The convergence speed is irrelevant to the number of prefixes.

Comparison Between Route Iteration and Tunnel Iteration

Comparison between route iteration and tunnel iteration is shown in the following table.

Table 1-5 Comparison between route iteration and tunnel iteration

Iteration Type	Description
Route iteration	• Iterates BGP public routes. • Triggered by route changes. • Supports next-hop iteration based on the specified routing policy.

Iteration Type	Description
Tunnel iteration	• Iterates BGP VPN routes. • Triggered by tunnel changes or tunnel policy changes. • Controls iteration behaviors through the tunnel policy to meet the requirements of different application scenarios.

1.3 References

None