## Contents

### Configuring basic IP routing

- Routing table
- Dynamic routing protocols
- Route preference
- Load sharing
- Route backup
- Route recursion
- Route redistribution
- Extension attribute redistribution
- Setting the maximum lifetime for routes and labels in the RIB
- Setting the maximum lifetime for routes in the FIB
- Configuring RIP NSR
  - Configuring IPv4 RIP NSR
  - Configuring IPv6 RIP NSR
- Configuring inter-protocol FRR
  - Configuring IPv4 RIP inter-protocol FRR
  - Configuring IPv6 RIP inter-protocol FRR
- Displaying and maintaining a routing table

### Configuring static routing

- Configuring a static route
- Configuring BFD for static routes
  - Bidirectional control mode
  - Single-hop echo mode
- Configuring static route FRR
  - Configuration guidelines
  - Configuration procedure
- Displaying and maintaining static routes
- Static route configuration examples
  - Basic static route configuration example
  - BFD for static routes configuration example (direct next hop)
  - BFD for static routes configuration example (indirect next hop)
  - Static route FRR configuration example

### Configuring a default route

### Configuring RIP

- Overview
- RIP route entries
- Routing loop prevention
- RIP operation
- RIP versions
- TRIP
- Protocols and standards
- RIP configuration task list
- Configuring basic RIP
  - Enabling RIP
  - Controlling RIP reception and advertisement on interfaces
  - Configuring a RIP version
- Configuring RIP route control
  - Configuring an additional routing metric
  - Configuring RIPv2 route summarization
  - Disabling host route reception
  - Advertising a default route
  - Configuring received/redistributed route filtering
  - Setting a preference for RIP
- Configuring RIP route redistribution
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tuning and optimizing RIP networks</td>
<td>33</td>
</tr>
<tr>
<td>Configuration prerequisites</td>
<td>33</td>
</tr>
<tr>
<td>Setting RIP timers</td>
<td>33</td>
</tr>
<tr>
<td>Enabling split horizon and poison reverse</td>
<td>34</td>
</tr>
<tr>
<td>Setting the maximum number of ECMP routes</td>
<td>35</td>
</tr>
<tr>
<td>Enabling zero field check on incoming RIPv1 messages</td>
<td>35</td>
</tr>
<tr>
<td>Enabling source IP address check on incoming RIP updates</td>
<td>35</td>
</tr>
<tr>
<td>Configuring RIPv2 message authentication</td>
<td>36</td>
</tr>
<tr>
<td>Setting the RIP triggered update interval</td>
<td>36</td>
</tr>
<tr>
<td>Specifying a RIP neighbor</td>
<td>37</td>
</tr>
<tr>
<td>Configuring TRIP</td>
<td>37</td>
</tr>
<tr>
<td>Configuring RIP network management</td>
<td>38</td>
</tr>
<tr>
<td>Configuring the RIP packet sending rate</td>
<td>38</td>
</tr>
<tr>
<td>Setting the maximum length of RIP packets</td>
<td>39</td>
</tr>
<tr>
<td>Configuring RIP GR</td>
<td>39</td>
</tr>
<tr>
<td>Enabling RIP NSR</td>
<td>40</td>
</tr>
<tr>
<td>Configuring BFD for RIP</td>
<td>41</td>
</tr>
<tr>
<td>Configuring single-hop echo detection (for a directly connected RIP neighbor)</td>
<td>41</td>
</tr>
<tr>
<td>Configuring single-hop echo detection (for a specific destination)</td>
<td>41</td>
</tr>
<tr>
<td>Configuring bidirectional control detection</td>
<td>42</td>
</tr>
<tr>
<td>Configuring RIP FRR</td>
<td>42</td>
</tr>
<tr>
<td>Configuration restrictions and guidelines</td>
<td>43</td>
</tr>
<tr>
<td>Configuration prerequisites</td>
<td>43</td>
</tr>
<tr>
<td>Configuration procedure</td>
<td>43</td>
</tr>
<tr>
<td>Displaying and maintaining RIP</td>
<td>44</td>
</tr>
<tr>
<td>RIP configuration examples</td>
<td>44</td>
</tr>
<tr>
<td>Configuring basic RIP</td>
<td>44</td>
</tr>
<tr>
<td>Configuring RIPv2 route redistribution</td>
<td>47</td>
</tr>
<tr>
<td>Configuring an additional metric for a RIP interface</td>
<td>49</td>
</tr>
<tr>
<td>Configuring RIP to advertise a summary route</td>
<td>51</td>
</tr>
<tr>
<td>Configuring RIP GR</td>
<td>51</td>
</tr>
<tr>
<td>Configuring RIP NSR</td>
<td>54</td>
</tr>
<tr>
<td>Configuring BFD for RIPv2 (single-hop echo detection for a directly connected neighbor)</td>
<td>56</td>
</tr>
<tr>
<td>Configuring BFD for RIPv2 (single-hop echo detection for a specific destination)</td>
<td>58</td>
</tr>
<tr>
<td>Configuring BFD for RIPv2 (bidirectional control detection)</td>
<td>60</td>
</tr>
<tr>
<td>Configuring RIP FRR</td>
<td>64</td>
</tr>
<tr>
<td>Configuring OSPF</td>
<td>67</td>
</tr>
<tr>
<td>Overview</td>
<td>67</td>
</tr>
<tr>
<td>OSPF packets</td>
<td>67</td>
</tr>
<tr>
<td>LSA types</td>
<td>67</td>
</tr>
<tr>
<td>OSPF areas</td>
<td>67</td>
</tr>
<tr>
<td>Router types</td>
<td>68</td>
</tr>
<tr>
<td>Route types</td>
<td>70</td>
</tr>
<tr>
<td>Route calculation</td>
<td>71</td>
</tr>
<tr>
<td>OSPF network types</td>
<td>71</td>
</tr>
<tr>
<td>DR and BDR</td>
<td>72</td>
</tr>
<tr>
<td>Protocols and standards</td>
<td>73</td>
</tr>
<tr>
<td>OSPF configuration task list</td>
<td>73</td>
</tr>
<tr>
<td>Enabling OSPF</td>
<td>75</td>
</tr>
<tr>
<td>Configuration prerequisites</td>
<td>75</td>
</tr>
<tr>
<td>Configuration guidelines</td>
<td>75</td>
</tr>
<tr>
<td>Enabling OSPF on a network</td>
<td>75</td>
</tr>
<tr>
<td>Enabling OSPF on an interface</td>
<td>76</td>
</tr>
<tr>
<td>Configuring OSPF areas</td>
<td>76</td>
</tr>
<tr>
<td>Configuring a stub area</td>
<td>77</td>
</tr>
<tr>
<td>Configuring an NSSSA area</td>
<td>77</td>
</tr>
<tr>
<td>Configuring a virtual link</td>
<td>78</td>
</tr>
<tr>
<td>Configuring OSPF network types</td>
<td>78</td>
</tr>
<tr>
<td>Configuration prerequisites</td>
<td>78</td>
</tr>
<tr>
<td>Configuring the broadcast network type for an interface</td>
<td>79</td>
</tr>
<tr>
<td>Configuring the NBMA network type for an interface</td>
<td>79</td>
</tr>
</tbody>
</table>
Configuring basic IP routing

IP routing directs IP packet forwarding on routers based on a routing table. This chapter focuses on unicast routing protocols. For more information about multicast routing protocols, see IP Multicast Configuration Guide.

Routing table

A RIB contains the global routing information and related information, including route recursion, route redistribution, and route extension information. The router selects optimal routes from the routing table and puts them into the FIB table. It uses the FIB table to forward packets. For more information about the FIB table, see Layer 3—IP Services Configuration Guide.

Table 1 categorizes routes by different criteria.

Table 1 Route categories

<table>
<thead>
<tr>
<th>Criterion</th>
<th>Categories</th>
</tr>
</thead>
</table>
| Destination                    | • Network route—The destination is a network. The subnet mask is less than 32 bits.  
                                    |   • Host route—The destination is a host. The subnet mask is 32 bits.               |
| Whether the destination is directly connected | • Direct route—The destination is directly connected.                           |
|                                 | • Indirect route—The destination is indirectly connected.                    |
| Origin                         | • Direct route—A direct route is discovered by the data link protocol on an interface, and is also called an interface route. |
|                                 | • Static route—A static route is manually configured by an administrator.     |
|                                 | • Dynamic route—A dynamic route is dynamically discovered by a routing protocol. |

To view brief information about a routing table, use the display ip routing-table command.

<sysname> display ip routing-table

Destinations : 19 Routes : 19

<table>
<thead>
<tr>
<th>Destination/Mask</th>
<th>Proto</th>
<th>Pre</th>
<th>Cost</th>
<th>NextHop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>1.1.1.0/24</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>1.1.1.1</td>
<td>Eth1/1</td>
</tr>
<tr>
<td>1.1.1.0/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>1.1.1.1</td>
<td>Eth1/1</td>
</tr>
<tr>
<td>1.1.1.1/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>1.1.1.255/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>1.1.1.1</td>
<td>Eth1/1</td>
</tr>
<tr>
<td>2.2.2.0/24</td>
<td>Static</td>
<td>60</td>
<td>0</td>
<td>12.2.2.2</td>
<td>Eth1/2</td>
</tr>
<tr>
<td>80.1.1.0/24</td>
<td>OSPF</td>
<td>10</td>
<td>2</td>
<td>80.1.1.1</td>
<td>Eth1/3</td>
</tr>
</tbody>
</table>

A route entry includes the following key items:

- **Destination**—IP address of the destination host or network.
- **Mask**—Mask length of the IP address.
- **Proto**—Protocol that installed the route.
- **Pre**—Preference of the route. Among routes to the same destination, the route with the highest preference is optimal.
- **Cost**—If multiple routes to a destination have the same preference, the one with the smallest cost is the optimal route.
- **NextHop**—Next hop.
- **Interface**—Output interface.

### Dynamic routing protocols

Static routes work well in small, stable networks. They are easy to configure and require fewer system resources. However, in networks where topology changes occur frequently, a typical practice is to configure a dynamic routing protocol. Compared with static routing, a dynamic routing protocol is complicated to configure, requires more router resources, and consumes more network resources.

Dynamic routing protocols dynamically collect and report reachability information to adapt to topology changes. They are suitable for large networks.

Dynamic routing protocols can be classified by different criteria, as shown in **Table 2**.

**Table 2 Categories of dynamic routing protocols**

<table>
<thead>
<tr>
<th>Criterion</th>
<th>Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation scope</td>
<td>• <strong>IGPs</strong>—Work within an AS. Examples include RIP, OSPF, and IS-IS.</td>
</tr>
<tr>
<td></td>
<td>• <strong>EGPs</strong>—Work between ASs. The most popular EGP is BGP.</td>
</tr>
<tr>
<td>Routing algorithm</td>
<td>• <strong>Distance-vector protocols</strong>—Examples include RIP and BGP. BGP is also</td>
</tr>
<tr>
<td></td>
<td>considered a path-vector protocol.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Link-state protocols</strong>—Examples include OSPF and IS-IS.</td>
</tr>
<tr>
<td>Destination address type</td>
<td>• <strong>Unicast routing protocols</strong>—Examples include RIP, OSPF, BGP, and IS-IS.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Multicast routing protocols</strong>—Examples include PIM-SM and PIM-DM.</td>
</tr>
<tr>
<td>IP version</td>
<td>• <strong>IPv4 routing protocols</strong>—Examples include RIP, OSPF, BGP, and IS-IS.</td>
</tr>
<tr>
<td></td>
<td>• <strong>IPv6 routing protocols</strong>—Examples include RIPng, OSPFv3, IPv6 BGP, and</td>
</tr>
<tr>
<td></td>
<td>IPv6 IS-IS.</td>
</tr>
</tbody>
</table>

An AS refers to a group of routers that use the same routing policy and work under the same administration.

### Route preference

Routing protocols, including static and direct routing, each by default have a preference. If they find multiple routes to the same destination, the router selects the route with the highest preference as the optimal route.

The preference of a direct route is always 0 and cannot be changed. You can configure a preference for each static route and each dynamic routing protocol. The following table lists the route types and default preferences. The smaller the value, the higher the preference.

**Table 3 Route types and default route preferences**

<table>
<thead>
<tr>
<th>Route type</th>
<th>Preference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct route</td>
<td>0</td>
</tr>
<tr>
<td>Multicast static route</td>
<td>1</td>
</tr>
<tr>
<td>OSPF</td>
<td>10</td>
</tr>
<tr>
<td>Route type</td>
<td>Preference</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>IS-IS</td>
<td>15</td>
</tr>
<tr>
<td>Unicast static route</td>
<td>60</td>
</tr>
<tr>
<td>RIP</td>
<td>100</td>
</tr>
<tr>
<td>OSPF ASE</td>
<td>150</td>
</tr>
<tr>
<td>OSPF NSSA</td>
<td>150</td>
</tr>
<tr>
<td>IBGP</td>
<td>255</td>
</tr>
<tr>
<td>EBGP</td>
<td>255</td>
</tr>
<tr>
<td>Unknown (route from an untrusted source)</td>
<td>256</td>
</tr>
</tbody>
</table>
Extension attribute redistribution

Extension attribute redistribution enables routing protocols to learn route extension attributes from each other, including BGP extended community attributes, OSPF area IDs, route types, and router IDs.

The RIB records extended attributes of each routing protocol and redistribution relationships of different routing protocol extended attributes.

Setting the maximum lifetime for routes and labels in the RIB

Perform this task to prevent routes of a certain protocol from being aged out due to slow protocol convergence resulting from a large number of route entries or long GR period.

The configuration takes effect at the next protocol or RIB process switchover.

To set the maximum lifetime for routes and labels in the RIB (IPv4):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter RIB view.</td>
<td>rib</td>
</tr>
<tr>
<td>3.</td>
<td>Create a RIB IPv4 address family and enter its view.</td>
<td>address-family ipv4</td>
</tr>
<tr>
<td>4.</td>
<td>Set the maximum lifetime for IPv4 routes and labels in the RIB.</td>
<td>protocol protocol [ instance instance-name ] lifetime seconds</td>
</tr>
</tbody>
</table>

By default, the maximum lifetime for routes and labels in the RIB is 480 seconds.

To set the maximum lifetime for routes and labels in the RIB (IPv6):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>6.</td>
<td>Enter RIB view.</td>
<td>rib</td>
</tr>
<tr>
<td>7.</td>
<td>Create a RIB IPv6 address family and enter its view.</td>
<td>address-family ipv6</td>
</tr>
<tr>
<td>8.</td>
<td>Set the maximum lifetime for IPv6 routes and labels in the RIB.</td>
<td>protocol protocol [ instance instance-name ] lifetime seconds</td>
</tr>
</tbody>
</table>

By default, the maximum lifetime for routes and labels in the RIB is 480 seconds.

Setting the maximum lifetime for routes in the FIB

When GR or NSR is disabled, FIB entries must be retained for some time after a protocol process switchover or RIB process switchover. When GR or NSR is enabled, FIB entries must be removed immediately after a protocol or RIB process switchover to avoid routing issues. Perform this task to meet such requirements.

To set the maximum lifetime for routes in the FIB (IPv4):
Step Command Remarks
1. Enter system view. system-view N/A
2. Enter RIB view. rib N/A
3. Create a RIB IPv4 address family and enter its view. address-family ipv4 By default, no RIB IPv4 address family exists.
4. Set the maximum lifetime for IPv4 routes in the FIB. fib lifetime seconds By default, the maximum lifetime for routes in the FIB is 600 seconds.

To set the maximum lifetime for routes in the FIB (IPv6):

Step Command Remarks
1. Enter system view. system-view N/A
2. Enter RIB view. rib N/A
3. Create a RIB IPv6 address family and enter its view. address-family ipv6 By default, no RIB IPv6 address family exists.
4. Set the maximum lifetime for IPv6 routes in the FIB. fib lifetime seconds By default, the maximum lifetime for routes in the FIB is 600 seconds.

Configuring RIB NSR

IMPORTANT:
Use this feature with protocol GR or NSR to avoid route timeouts and traffic interruption.

When an active/standby switchover occurs, nonstop routing (NSR) backs up routing information from the active process to the standby process to avoid routing flapping and ensure forwarding continuity.

RIB NSR provides faster route convergence than protocol NSR during an active/standby switchover.

Configuring IPv4 RIB NSR

The following matrix shows the feature and hardware compatibility:

<table>
<thead>
<tr>
<th>Hardware</th>
<th>IPv4 RIB NSR compatibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSR954(JH296A/JH297A/JH298A/JH299A/JH373A)</td>
<td>No</td>
</tr>
<tr>
<td>MSR958(JH300A/JH301A)</td>
<td>No</td>
</tr>
<tr>
<td>MSR1002-4/1003-8S</td>
<td>No</td>
</tr>
<tr>
<td>MSR2003</td>
<td>Yes</td>
</tr>
<tr>
<td>MSR2004-24/2004-48</td>
<td>No</td>
</tr>
<tr>
<td>MSR3012/3024/3044/3064</td>
<td>No</td>
</tr>
<tr>
<td>MSR4060/4080</td>
<td>Yes</td>
</tr>
</tbody>
</table>

To configure IPv4 RIB NSR:
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter RIB view.</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>Create a RIB IPv4 address family and enter its view.</td>
<td>By default, no RIB IPv4 address family exists.</td>
</tr>
<tr>
<td>4.</td>
<td>Enable IPv4 RIB NSR.</td>
<td>By default, RIB NSR is disabled.</td>
</tr>
</tbody>
</table>

Configuring IPv6 RIB NSR

The following matrix shows the feature and hardware compatibility:

<table>
<thead>
<tr>
<th>Hardware</th>
<th>IPv6 RIB NSR compatibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSR954(JH296A/JH297A/JH298A/JH299A/JH373A)</td>
<td>No</td>
</tr>
<tr>
<td>MSR958(JH300A/JH301A)</td>
<td>No</td>
</tr>
<tr>
<td>MSR1002-4/1003-8S</td>
<td>No</td>
</tr>
<tr>
<td>MSR2003</td>
<td>Yes</td>
</tr>
<tr>
<td>MSR2004-24/2004-48</td>
<td>No</td>
</tr>
<tr>
<td>MSR3012/3024/3044/3064</td>
<td>No</td>
</tr>
<tr>
<td>MSR4060/4080</td>
<td>Yes</td>
</tr>
</tbody>
</table>

To configure IPv6 RIB NSR:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter RIB view.</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>Create a RIB IPv6 address family and enter its view.</td>
<td>By default, no RIB IPv6 address family exists.</td>
</tr>
<tr>
<td>4.</td>
<td>Enable IPv6 RIB NSR.</td>
<td>By default, RIB NSR is disabled.</td>
</tr>
</tbody>
</table>

Configuring inter-protocol FRR

⚠️ CAUTION:
This feature uses the next hop of a route from a different protocol as the backup next hop for the faulty route, which might cause loops.

Inter-protocol fast reroute (FRR) enables fast rerouting between routes of different protocols to reduce the service interruption time caused by unreachable next hops.

Among the routes to the same destination in the RIB, a router adds the route with the highest preference to the FIB table. For example, if a static route and an OSPF route in the RIB have the same destination, the router adds the OSPF route to the FIB table by default. The next hop of the static route is selected as the backup next hop for the OSPF route. When the next hop of the OSPF route is unreachable, the backup next hop is used.
Configuring IPv4 RIB inter-protocol FRR

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter RIB view.</td>
<td>rib</td>
</tr>
<tr>
<td>3.</td>
<td>Create a RIB IPv4 address family and enter its view.</td>
<td>address-family ipv4</td>
</tr>
<tr>
<td>4.</td>
<td>Enable IPv4 RIB inter-protocol FRR.</td>
<td>inter-protocol fast-reroute [ vpn-instance vpn-instance-name ]</td>
</tr>
</tbody>
</table>

Configuring IPv6 RIB inter-protocol FRR

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter RIB view.</td>
<td>rib</td>
</tr>
<tr>
<td>3.</td>
<td>Create a RIB IPv6 address family and enter its view.</td>
<td>address-family ipv6</td>
</tr>
<tr>
<td>4.</td>
<td>Enable IPv6 RIB inter-protocol FRR.</td>
<td>inter-protocol fast-reroute [ vpn-instance vpn-instance-name ]</td>
</tr>
</tbody>
</table>

Displaying and maintaining a routing table

Execute **display** commands in any view and **reset** commands in user view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display routing table information.</td>
<td>display ip routing-table [ topology topo-name ] [ vpn-instance vpn-instance-name ] [ verbose ]</td>
</tr>
<tr>
<td>Display information about routes permitted by an IPv4 basic ACL.</td>
<td>display ip routing-table [ topology topo-name ] [ vpn-instance vpn-instance-name ] acl ipv4-acl-number [ verbose ]</td>
</tr>
<tr>
<td>Display information about routes to a specific destination address.</td>
<td>display ip routing-table [ topology topo-name ] [ vpn-instance vpn-instance-name ] ip-address [ mask</td>
</tr>
<tr>
<td>Display information about routes to a range of destination addresses.</td>
<td>display ip routing-table [ topology topo-name ] [ vpn-instance vpn-instance-name ] ip-address1 to ip-address2 [ verbose ]</td>
</tr>
<tr>
<td>Display information about routes permitted by an IP prefix list.</td>
<td>display ip routing-table [ topology topo-name ] [ vpn-instance vpn-instance-name ] prefix-list prefix-list-name [ verbose ]</td>
</tr>
<tr>
<td>Display information about routes installed by a protocol.</td>
<td>display ip routing-table [ topology topo-name ] [ vpn-instance vpn-instance-name ] protocol protocol [ inactive</td>
</tr>
<tr>
<td>Task</td>
<td>Command</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Display IPv4 route statistics.</td>
<td><code>display ip routing-table topology topo-name [vpn-instance vpn-instance-name] statistics</code></td>
</tr>
<tr>
<td>Display brief IPv4 routing table information.</td>
<td><code>display ip routing-table topology topo-name [vpn-instance vpn-instance-name] summary</code></td>
</tr>
<tr>
<td>Display route attribute information in the RIB.</td>
<td><code>display rib attribute [attribute-id]</code></td>
</tr>
<tr>
<td>Display RIB GR state information.</td>
<td><code>display rib graceful-restart</code></td>
</tr>
<tr>
<td>Display next hop information in the RIB.</td>
<td><code>display rib nib [self-originated] [nib-id] [verbose]</code></td>
</tr>
<tr>
<td>Display next hop information for direct routes.</td>
<td><code>display rib nib protocol protocol [verbose]</code></td>
</tr>
<tr>
<td>Clear IPv4 route statistics.</td>
<td><code>reset ip routing-table statistics protocol {topology topo-name [vpn-instance vpn-instance-name] all}</code></td>
</tr>
<tr>
<td>Display IPv6 routing table information.</td>
<td><code>display ipv6 routing-table [vpn-instance vpn-instance-name] [verbose]</code></td>
</tr>
<tr>
<td>Display information about routes to an IPv6 destination address.</td>
<td><code>display ipv6 routing-table [vpn-instance vpn-instance-name] ipv6-address [prefix-length] [longer-match] [verbose]</code></td>
</tr>
<tr>
<td>Display information about routes permitted by an IPv6 basic ACL.</td>
<td><code>display ipv6 routing-table [vpn-instance vpn-instance-name] acl ipv6-acl-number [verbose]</code></td>
</tr>
<tr>
<td>Display information about routes to a range of IPv6 destination addresses.</td>
<td><code>display ipv6 routing-table [vpn-instance vpn-instance-name] ipv6-address1 to ipv6-address2 [verbose]</code></td>
</tr>
<tr>
<td>Display information about routes permitted by an IPv6 prefix list.</td>
<td><code>display ipv6 routing-table [vpn-instance vpn-instance-name] prefix-list prefix-list-name [verbose]</code></td>
</tr>
<tr>
<td>Display information about routes installed by an IPv6 protocol.</td>
<td><code>display ipv6 routing-table [vpn-instance vpn-instance-name] protocol protocol [inactive] [verbose]</code></td>
</tr>
<tr>
<td>Display IPv6 route statistics.</td>
<td><code>display ipv6 routing-table [vpn-instance vpn-instance-name] statistics</code></td>
</tr>
<tr>
<td>Display brief IPv6 routing table information.</td>
<td><code>display ipv6 routing-table [vpn-instance vpn-instance-name] summary</code></td>
</tr>
<tr>
<td>Display route attribute information in the IPv6 RIB.</td>
<td><code>display ipv6 rib attribute [attribute-id]</code></td>
</tr>
<tr>
<td>Display IPv6 RIB GR state information.</td>
<td><code>display ipv6 rib graceful-restart</code></td>
</tr>
<tr>
<td>Display next hop information in the IPv6 RIB.</td>
<td><code>display ipv6 rib nib [self-originated] [nib-id] [verbose]</code></td>
</tr>
<tr>
<td>Display next hop information for IPv6 direct routes.</td>
<td><code>display ipv6 rib nib protocol protocol [verbose]</code></td>
</tr>
<tr>
<td>Clear IPv6 route statistics.</td>
<td>`reset ipv6 routing-table statistics protocol {vpn-instance vpn-instance-name} {protocol</td>
</tr>
</tbody>
</table>
Configuring static routing

Static routes are manually configured. If a network's topology is simple, you only need to configure static routes for the network to work correctly.

Static routes cannot adapt to network topology changes. If a fault or a topological change occurs in the network, the network administrator must modify the static routes manually.

Configuring a static route

Before you configure a static route, complete the following tasks:

- Configure the physical parameters for related interfaces.
- Configure the link-layer attributes for related interfaces.
- Configure the IP addresses for related interfaces.

You can associate Track with a static route to monitor the reachability of the next hops. For more information about Track, see *High Availability Configuration Guide*.

To configure a static route:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2. (Optional.) Create a static route group and enter its view.</td>
<td>ip route-static-group group-name</td>
<td>By default, no static route group is configured.</td>
</tr>
<tr>
<td>3. (Optional.) Configure a static route prefix.</td>
<td>prefix dest-address { mask-length</td>
<td>mask }</td>
</tr>
<tr>
<td>4. (Optional.) Return to system view.</td>
<td>quit</td>
<td>N/A</td>
</tr>
</tbody>
</table>
| 5. Configure a static route. | • Method 1: ip route-static { dest-address { mask-length | mask } | group group-name } { interface-type interface-number | next-hop-address | next-hop-address | vpn-instance d-vpn-instance-name next-hop-address } [ permanent | track track-entry-number ] [ preference preference ] [ tag tag-value ] [ description text ]
  
  • Method 2: ip route-static vpn-instance s-vpn-instance-name { dest-address { mask-length | mask } | group group-name } { interface-type interface-number | next-hop-address | next-hop-address | public | vpn-instance d-vpn-instance-name next-hop-address } [ permanent | track track-entry-number ] [ preference preference ] [ tag tag-value ] [ description text ]
  
  • Method 3: ip route-static topology topo-name { dest-address { mask | mask-length } | group group-name } { next-hop-address | interface-type interface-number } | By default, no static route is configured. |
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.</td>
<td>ip route-static default-preference default-preference</td>
<td>The default setting is 60.</td>
</tr>
<tr>
<td>7.</td>
<td>delete [ topology topo-name</td>
<td>vpn-instance vpn-instance-name ] static-routes all</td>
</tr>
</tbody>
</table>

### Configuring BFD for static routes

**IMPORTANT:**
Enabling BFD for a flapping route could worsen the situation.

BFD provides a general-purpose, standard, medium-, and protocol-independent fast failure detection mechanism. It can uniformly and quickly detect the failures of the bidirectional forwarding paths between two routers for protocols, such as routing protocols and MPLS.

For more information about BFD, see *High Availability Configuration Guide*.

### Bidirectional control mode

To use BFD bidirectional control detection between two devices, enable BFD control mode for each device’s static route destined to the peer.

To configure a static route and enable BFD control mode, use one of the following methods:
- Specify an output interface and a direct next hop.
- Specify an indirect next hop and a specific BFD packet source address for the static route.

To configure BFD control mode for a static route (direct next hop):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
</tbody>
</table>
### Step 2. Configure BFD control mode for a static route.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Method 1:</td>
<td>By default, BFD control mode for a static route is not configured.</td>
</tr>
<tr>
<td></td>
<td>ip route-static dest-address { mask-length</td>
<td>mask } interface-type interface-number next-hop-address bfd control-packet [ preference preference ] [ tag tag-value ] [ description text ]</td>
</tr>
<tr>
<td></td>
<td>bfd-source ip-address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Method 2:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ip route-static vpn-instance d-vpn-instance-name dest-address { mask-length</td>
<td>mask } interface-type interface-number next-hop-address bfd control-packet bfd-source ip-address [ preference preference ] [ tag tag-value ] [ description text ]</td>
</tr>
</tbody>
</table>

To configure BFD control mode for a static route (indirect next hop):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Method 1:</td>
<td>By default, BFD control mode for a static route is not configured.</td>
</tr>
<tr>
<td></td>
<td>ip route-static dest-address { mask-length</td>
<td>mask } { next-hop-address bfd control-packet bfd-source ip-address</td>
</tr>
<tr>
<td></td>
<td>• Method 2:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ip route-static vpn-instance d-vpn-instance-name dest-address { mask-length</td>
<td>mask } { next-hop-address bfd control-packet bfd-source ip-address</td>
</tr>
</tbody>
</table>

### Single-hop echo mode

With BFD echo mode enabled for a static route, the output interface sends BFD echo packets to the destination device, which loops the packets back to test the link reachability.

**IMPORTANT:**

Do not use BFD for a static route with the output interface in spoofing state.

To configure BFD echo mode for a static route:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Enter system view.</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Configure the source address of echo packets.</td>
<td>By default, the source address of echo packets is not configured. For more information about this command, see High</td>
</tr>
</tbody>
</table>
### Configuring static route FRR

A link or router failure on a path can cause packet loss and even routing loop. Static route fast reroute (FRR) enables fast rerouting to minimize the impact of link or node failures.

**Figure 1 Network diagram**

As shown in Figure 1, upon a link failure, packets are directed to the backup next hop to avoid traffic interruption. You can either specify a backup next hop for FRR or enable FRR to automatically select a backup next hop (which must be configured in advance).

**Configuration guidelines**

- Do not use static route FRR and BFD (for a static route) at the same time.
- Static route does not take effect when the backup output interface is unavailable.
- Equal-cost routes do not support static route FRR.
- The backup output interface and next hop cannot be modified, and cannot be the same as the primary output interface and next hop.
- Static route FRR is available only when the state of primary link (with Layer 3 interfaces staying up) changes from bidirectional to unidirectional or down.
## Configuration procedure

### Configuring static route FRR by specifying a backup next hop

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure static route FRR.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Method 1:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>ip route-static dest-address</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>`{ mask-length</td>
<td>mask } interface-type interface-number [ next-hop-address [ backup-interface interface-type interface-number [ backup-nexthop backup-nexthop-address ] ] ] [ permanent ] [ preference preference ] [ tag tag-value ] [ description text ]`</td>
</tr>
<tr>
<td></td>
<td>Method 2:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>ip route-static vpn-instance s-vpn-instance-name dest-address</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>`{ mask-length</td>
<td>mask } interface-type interface-number [ next-hop-address [ backup-interface interface-type interface-number [ backup-nexthop backup-nexthop-address ] ] ] [ permanent ] [ preference preference ] [ tag tag-value ] [ description text ]`</td>
</tr>
<tr>
<td></td>
<td>Method 3:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>ip route-static topology topo-name dest-address</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>`{ mask-length</td>
<td>mask } interface-type interface-number [ next-hop-address [ backup-interface interface-type interface-number [ backup-nexthop backup-nexthop-address ] ] ] [ preference preference ] [ tag tag-value ] [ description text ]`</td>
</tr>
</tbody>
</table>

### Configuring static route FRR to automatically select a backup next hop

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure static route FRR to automatically select a backup next hop.</td>
<td><code>ip route-static fast-reroute auto</code></td>
</tr>
</tbody>
</table>

### Enabling BFD echo packet mode for static route FRR

By default, static route FRR uses ARP to detect primary link failures. Perform this task to enable static route FRR to use BFD echo packet mode for fast failure detection on the primary link.

To enable BFD echo packet mode for static route FRR:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure the source IP address of BFD echo packets.</td>
<td><code>bfd echo-source-ip ip-address</code></td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td>on the same network segment as any local interface’s IP address. For more information about this command, see High Availability Command Reference.</td>
<td></td>
</tr>
<tr>
<td>3. Enable BFD echo packet mode for static route FRR.</td>
<td>ip route-static primary-path-detect bfd echo</td>
<td>By default, BFD echo mode for static route FRR is disabled.</td>
</tr>
</tbody>
</table>

**Displaying and maintaining static routes**

Execute `display` commands in any view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display static route information.</td>
<td>`display ip routing-table protocol static [ inactive</td>
</tr>
<tr>
<td>Display static route next hop information.</td>
<td><code>display route-static nib [ nib-id ] [ verbose ]</code></td>
</tr>
<tr>
<td>Display static routing table information.</td>
<td>`display route-static routing-table [ topology topo-name</td>
</tr>
</tbody>
</table>

**Static route configuration examples**

**Basic static route configuration example**

**Network requirements**

As shown in Figure 2, configure static routes on the routers for interconnections between any two hosts.

**Figure 2 Network diagram**

![Network diagram](image)

**Configuration procedure**

1. Configure IP addresses for interfaces. (Details not shown.)
2. Configure static routes:
   - # Configure a default route on Router A.
     ```
     # Configure a default route on Router A.
     ```
<RouterA> system-view
[RouterA] ip route-static 0.0.0.0 0.0.0.0 1.1.4.2
# Configure two static routes on Router B.
<RouterB> system-view
[RouterB] ip route-static 1.1.2.0 255.255.255.0 1.1.4.1
[RouterB] ip route-static 1.1.3.0 255.255.255.0 1.1.5.6
# Configure a default route on Router C.
<RouterC> system-view
[RouterC] ip route-static 0.0.0.0 0.0.0.0 1.1.5.5

3. Configure the default gateways of Host A, Host B, and Host C as 1.1.2.3, 1.1.6.1, and 1.1.3.1. (Details not shown.)

Verifying the configuration

# Display the static route information on Router A.
[RouterA] display ip routing-table protocol static

Summary Count : 1

Static Routing table Status : <Active>
Summary Count : 1

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/0           Static 60   0            1.1.4.2         GE1/0/2

Static Routing table Status : <Inactive>
Summary Count : 0

# Display the static route information on Router B.
[RouterB] display ip routing-table protocol static

Summary Count : 2

Static Routing table Status : <Active>
Summary Count : 2

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
1.1.2.0/24          Static 60   0            1.1.4.1         GE1/0/1
1.1.3.0/24          Static 60   0            1.1.5.6         GE1/0/2

Static Routing table Status : <Inactive>
Summary Count : 0

# Use the ping command on Host B to test the reachability of Host A (Windows XP runs on the two hosts).
C:\Documents and Settings\Administrator>ping 1.1.2.2

Pinging 1.1.2.2 with 32 bytes of data:

Reply from 1.1.2.2: bytes=32 time=1ms TTL=126
Reply from 1.1.2.2: bytes=32 time=1ms TTL=126
Reply from 1.1.2.2: bytes=32 time=1ms TTL=126
Reply from 1.1.2.2: bytes=32 time=1ms TTL=126

Ping statistics for 1.1.2.2:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 1ms, Maximum = 1ms, Average = 1ms

# Use the tracert command on Host B to test the reachability of Host A.
C:\Documents and Settings\Administrator>tracert 1.1.2.2

Tracing route to 1.1.2.2 over a maximum of 30 hops

1  <1 ms  <1 ms  <1 ms  1.1.6.1
2  <1 ms  <1 ms  <1 ms  1.1.4.1
3    1 ms <1 ms  <1 ms  1.1.2.2

Trace complete.

BFD for static routes configuration example (direct next hop)

Network requirements

Configure the following, as shown in Figure 3:
  • Configure a static route to subnet 120.1.1.0/24 on Router A.
  • Configure a static route to subnet 121.1.1.0/24 on Router B.
  • Enable BFD for both routes.
  • Configure a static route to subnet 120.1.1.0/24 and a static route to subnet 121.1.1.0/24 on Router C.

When the link between Router A and Router B through the Layer 2 switch fails, BFD can detect the failure immediately. Router A then communicates with Router B through Router C.

Figure 3 Network diagram

Table 4 Interface and IP address assignment

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router A</td>
<td>GigabitEthernet 1/0/1</td>
<td>12.1.1.1/24</td>
</tr>
<tr>
<td>Router A</td>
<td>GigabitEthernet 1/0/2</td>
<td>10.1.1.102/24</td>
</tr>
<tr>
<td>Router B</td>
<td>GigabitEthernet 1/0/1</td>
<td>12.1.1.2/24</td>
</tr>
</tbody>
</table>
### Device Interface IP address

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router B</td>
<td>GigabitEthernet 1/0/2</td>
<td>13.1.1.1/24</td>
</tr>
<tr>
<td>Router C</td>
<td>GigabitEthernet 1/0/1</td>
<td>10.1.1.100/24</td>
</tr>
<tr>
<td>Router C</td>
<td>GigabitEthernet 1/0/2</td>
<td>13.1.1.2/24</td>
</tr>
</tbody>
</table>

### Configuration procedure

1. Configure IP addresses for interfaces. (Details not shown.)
2. Configure static routes and BFD:

   # Configure static routes on Route A and enable BFD control mode for the static route that traverses the Layer 2 switch.

```
<RouterA> system-view
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] bfd min-transmit-interval 500
[RouterA-GigabitEthernet1/0/1] bfd min-receive-interval 500
[RouterA-GigabitEthernet1/0/1] bfd detect-multiplier 9
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] ip route-static 120.1.1.0 24 gigabitethernet 1/0/1 12.1.1.2 bfd control-packet
[RouterA] ip route-static 120.1.1.0 24 gigabitethernet 1/0/2 10.1.1.100 preference 65
[RouterA] quit
```

# Configure static routes on Router B and enable BFD control mode for the static route that traverses the Layer 2 switch.

```
<RouterB> system-view
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] bfd min-transmit-interval 500
[RouterB-GigabitEthernet1/0/1] bfd min-receive-interval 500
[RouterB-GigabitEthernet1/0/1] bfd detect-multiplier 9
[RouterB-GigabitEthernet1/0/1] quit
[RouterB] ip route-static 121.1.1.0 24 gigabitethernet 1/0/1 12.1.1.1 bfd control-packet
[RouterB] ip route-static 121.1.1.0 24 gigabitethernet 1/0/2 13.1.1.2 preference 65
[RouterB] quit
```

# Configure static routes on Router C.

```
<RouterC> system-view
[RouterC] ip route-static 120.1.1.0 24 13.1.1.1
[RouterC] ip route-static 121.1.1.0 24 10.1.1.102
```

### Verifying the configuration

# Display BFD sessions on Router A.

```
<RouterA> display bfd session

Total Session Num: 1     Up Session Num: 1     Init Mode: Active

IPv4 Session Working Under **Ctrl Mode**:

<table>
<thead>
<tr>
<th>LD/RD</th>
<th>SourceAddr</th>
<th>DestAddr</th>
<th>State</th>
<th>Holdtime</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/7</td>
<td>12.1.1.1</td>
<td>12.1.1.2</td>
<td>Up</td>
<td>2000ms</td>
<td>GE1/0/1</td>
</tr>
</tbody>
</table>
```
The output shows that the BFD session has been created.

# Display static routes on Router A.
<RouterA> display ip routing-table protocol static

Summary Count : 1

<table>
<thead>
<tr>
<th>Destination/Mask</th>
<th>Proto</th>
<th>Pre</th>
<th>Cost</th>
<th>NextHop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>120.1.1.0/24</td>
<td>Static</td>
<td>60</td>
<td>0</td>
<td>12.1.1.2</td>
<td>GE1/0/1</td>
</tr>
</tbody>
</table>

Static Routing table Status : <Inactive>
Summary Count : 0

The output shows that Router A communicates with Router B through GigabitEthernet 1/0/1. Then the link over GigabitEthernet 1/0/1 fails.

# Display static routes on Router A.
<RouterA> display ip routing-table protocol static

Summary Count : 1

<table>
<thead>
<tr>
<th>Destination/Mask</th>
<th>Proto</th>
<th>Pre</th>
<th>Cost</th>
<th>NextHop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>120.1.1.0/24</td>
<td>Static</td>
<td>65</td>
<td>0</td>
<td>10.1.1.100</td>
<td>GE1/0/2</td>
</tr>
</tbody>
</table>

Static Routing table Status : <Inactive>
Summary Count : 0

The output shows that Router A communicates with Router B through GigabitEthernet 1/0/2.

**BFD for static routes configuration example (indirect next hop)**

**Network requirements**

*Figure 4* shows the network topology as follows:

- Router A has a route to interface Loopback 1 (2.2.2.9/32) on Router B, with the output interface GigabitEthernet 1/0/1.
- Router B has a route to interface Loopback 1 (1.1.1.9/32) on Router A, with the output interface GigabitEthernet 1/0/1.
- Router D has a route to 1.1.1.9/32, with the output interface GigabitEthernet 1/0/1, and a route to 2.2.2.9/32, with the output interface GigabitEthernet 1/0/2.

Configure the following:

- Configure a static route to subnet 120.1.1.0/24 on Router A.
- Configure a static route to subnet 121.1.1.0/24 on Router B.
- Enable BFD for both routes.
- Configure a static route to subnet 120.1.1.0/24 and a static route to subnet 121.1.1.0/24 on both Router C and Router D.

When the link between Router A and Router B through Router D fails, BFD can detect the failure immediately. Router A then communicates with Router B through Router C.

**Figure 4 Network diagram**

**Table 5 Interface and IP address assignment**

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router A</td>
<td>GigabitEthernet 1/0/1</td>
<td>12.1.1.1/24</td>
</tr>
<tr>
<td>Router A</td>
<td>GigabitEthernet 1/0/2</td>
<td>10.1.1.102/24</td>
</tr>
<tr>
<td>Router A</td>
<td>Loopback 1</td>
<td>1.1.1.9/32</td>
</tr>
<tr>
<td>Router B</td>
<td>GigabitEthernet 1/0/1</td>
<td>11.1.1.2/24</td>
</tr>
<tr>
<td>Router B</td>
<td>GigabitEthernet 1/0/2</td>
<td>13.1.1.1/24</td>
</tr>
<tr>
<td>Router B</td>
<td>Loopback 1</td>
<td>2.2.2.9/32</td>
</tr>
<tr>
<td>Router C</td>
<td>GigabitEthernet 1/0/1</td>
<td>10.1.1.100/24</td>
</tr>
<tr>
<td>Router C</td>
<td>GigabitEthernet 1/0/2</td>
<td>13.1.1.2/24</td>
</tr>
<tr>
<td>Router D</td>
<td>GigabitEthernet 1/0/1</td>
<td>12.1.1.2/24</td>
</tr>
<tr>
<td>Router D</td>
<td>GigabitEthernet 1/0/2</td>
<td>11.1.1.2/24</td>
</tr>
</tbody>
</table>

**Configuration procedure**

1. Configure IP addresses for interfaces. (Details not shown.)
2. Configure static routes and BFD:
   
   # Configure static routes on Router A and enable BFD control mode for the static route that traverses Router D.

   ```
   <RouterA> system-view
   [RouterA] bfd multi-hop min-transmit-interval 500
   [RouterA] bfd multi-hop min-receive-interval 500
   [RouterA] bfd multi-hop detect-multiplier 9
   [RouterA] ip route-static 120.1.1.0 24 2.2.2.9 bfd control-packet bfd-source 1.1.1.9
   [RouterA] ip route-static 120.1.1.0 24 gigabitethernet 1/0/2 10.1.1.100 preference 65
   [RouterA] quit
   # Configure static routes on Router B and enable BFD control mode for the static route that traverses Router D.
   ```
<RouterB> system-view
[RouterB] bfd multi-hop min-transmit-interval 500
[RouterB] bfd multi-hop min-receive-interval 500
[RouterB] bfd multi-hop detect-multiplier 9
[RouterB] ip route-static 121.1.1.0 24 1.1.1.9 bfd control-packet bfd-source 2.2.2.9
[RouterB] ip route-static 121.1.1.0 24 gigabitethernet 1/0/2 13.1.1.2 preference 65
[RouterB] quit

# Configure static routes on Router C.
<RouterC> system-view
[RouterC] ip route-static 120.1.1.0 24 13.1.1.1
[RouterC] ip route-static 121.1.1.0 24 10.1.1.102

# Configure static routes on Router D.
<RouterD> system-view
[RouterD] ip route-static 120.1.1.0 24 11.1.1.2
[RouterD] ip route-static 121.1.1.0 24 12.1.1.1

Verifying the configuration

# Display the BFD session information on Router A.
<RouterA> display bfd session

Total Session Num: 1     Up Session Num: 1     Init Mode: Active

IPv4 Session Working Under Ctrl Mode:

LD/RD          SourceAddr      DestAddr        State    Holdtime    Interface
4/7            1.1.1.9         2.2.2.9         Up       2000ms      N/A

The output shows that the BFD session has been created.

# Display static routes on Router A.
<RouterA> display ip routing-table protocol static

Summary Count : 1

Static Routing table Status : <Active>
Summary Count : 1

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
120.1.1.0/24        Static 60   0            12.1.1.2        GE1/0/1

Static Routing table Status : <Inactive>
Summary Count : 0

The output shows that Router A communicates with Router B through GigabitEthernet 1/0/1. Then the link over GigabitEthernet 1/0/1 fails.

# Display static routes on Router A.
<RouterA> display ip routing-table protocol static

Summary Count : 1

Static Routing table Status : <Active>
Summary Count : 1

<table>
<thead>
<tr>
<th>Destination/Mask</th>
<th>Proto</th>
<th>Pre</th>
<th>Cost</th>
<th>NextHop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>120.1.1.0/24</td>
<td>Static</td>
<td>65</td>
<td>0</td>
<td>10.1.1.100</td>
<td>GE1/0/2</td>
</tr>
</tbody>
</table>

Static Routing table Status : <Inactive>
Summary Count : 0

The output shows that Router A communicates with Router B through GigabitEthernet 1/0/2.

Static route FRR configuration example

Network requirements

As shown in Figure 5, configure static routes on Router A, Router B, and Router C, and configure static route FRR. When Link A becomes unidirectional, traffic can be switched to Link B immediately.

Figure 5 Network diagram

Table 6 Interface and IP address assignment

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router A</td>
<td>GigabitEthernet 1/0/1</td>
<td>12.12.12.1/24</td>
</tr>
<tr>
<td>Router A</td>
<td>GigabitEthernet 1/0/2</td>
<td>13.13.13.1/24</td>
</tr>
<tr>
<td>Router A</td>
<td>Loopback 0</td>
<td>1.1.1.1/32</td>
</tr>
<tr>
<td>Router B</td>
<td>GigabitEthernet 1/0/1</td>
<td>24.24.24.4/24</td>
</tr>
<tr>
<td>Router B</td>
<td>GigabitEthernet 1/0/2</td>
<td>13.13.13.2/24</td>
</tr>
<tr>
<td>Router B</td>
<td>Loopback 0</td>
<td>4.4.4.4/32</td>
</tr>
<tr>
<td>Router C</td>
<td>GigabitEthernet 1/0/1</td>
<td>12.12.12.2/24</td>
</tr>
<tr>
<td>Router C</td>
<td>GigabitEthernet 1/0/2</td>
<td>24.24.24.2/24</td>
</tr>
</tbody>
</table>

Configuration procedure

1. Configure IP addresses for interfaces. (Details not shown.)
2. Configure static route FRR on link A by using one of the following methods:
   o (Method 1.) Specify a backup next hop for static route FRR:
     # Configure a static route on Router A, and specify GigabitEthernet 1/0/1 as the backup output interface and 12.12.12.2 as the backup next hop.
     <RouterA> system-view
# Configure a static route on Router B, and specify GigabitEthernet 1/0/1 as the backup output interface and 24.24.24.2 as the backup next hop.

```plaintext
<RouterB> system-view
[RouterB] ip route-static 1.1.1.1 32 gigabitethernet 1/0/2 13.13.13.1
backup-interface gigabitethernet 1/0/1 backup-nexthop 24.24.24.2
```

- **Method 2.** Configure static route FRR to automatically select a backup next hop:

  # Configure static routes on Router A, and enable static route FRR.

```plaintext
<RouterA> system-view
[RouterA] ip route-static 4.4.4.4 32 gigabitethernet 1/0/2 13.13.13.2
[RouterA] ip route-static 4.4.4.4 32 gigabitethernet 1/0/1 12.12.12.2 preference 70
[RouterA] ip route-static fast-reroute auto
```

# Configure static routes on Router B, and enable static route FRR.

```plaintext
<RouterB> system-view
[RouterB] ip route-static 1.1.1.1 32 gigabitethernet 1/0/2 13.13.13.1
[RouterB] ip route-static 1.1.1.1 32 gigabitethernet 1/0/1 24.24.24.2 preference 70
[RouterB] ip route-static fast-reroute auto
```

3. Configure static routes on Router C.

```plaintext
<RouterC> system-view
[RouterC] ip route-static 4.4.4.4 32 gigabitethernet 1/0/2 24.24.24.4
[RouterC] ip route-static 1.1.1.1 32 gigabitethernet 1/0/1 12.12.12.1
```

### Verifying the configuration

# Display route 4.4.4.4/32 on Router A to view the backup next hop information.

```plaintext
[RouterA] display ip routing-table 4.4.4.4 verbose
```

Summary Count : 1

**Destination**: 4.4.4.4/32  
**Protocol**: Static  
**Process ID**: 0  
**SubProtID**: 0x0  
**Cost**: 0  
**IpPre**: N/A  
**Tag**: 0  
**OrigTblID**: 0x0  
**TableID**: 0x2  
**NibID**: 0x26000002  
**AttrID**: 0xffffffff  
**Flags**: 0x1008c  
**Label**: NULL  
**BkLabel**: NULL  
**Tunnel ID**: Invalid  
**BkTunnel ID**: Invalid  
**FtnIndex**: 0x0  
**Connector**: N/A  
**RealNextHop**: 13.13.13.2  
**OrigNextHop**: 13.13.13.2  
**BkNextHop**: 12.12.12.2  
**Interface**: GigabitEthernet1/0/2
```

# Display route 1.1.1.1/32 on Router B to view the backup next hop information.

```plaintext
[RouterB] display ip routing-table 1.1.1.1 verbose
```

# Display route 1.1.1.1/32 on Router B to view the backup next hop information.

```plaintext
[RouterB] display ip routing-table 1.1.1.1 verbose
```
Summary Count : 1

Destination: 1.1.1.1/32
Protocol: Static
Process ID: 0
SubProtID: 0x0                      Age: 04h20m37s
Cost: 0                             Preference: 10
IpPre: N/A                          QosLocalID: N/A
Tag: 0                              State: Active Adv
OrigTblID: 0x0                       OrigVrf: default-vrf
TableID: 0x2                         OrigAs: 0
NibID: 0x26000002                    LastAs: 0
AttrID: 0xffffffff                   Neighbor: 0.0.0.0
Flags: 0x1008c                      OrigNextHop: 13.13.13.1
Label: NULL                         RealNextHop: 13.13.13.1
BkLabel: NULL                       BkNextHop: 24.24.24.2
Tunnel ID: Invalid                   Interface: GigabitEthernet1/0/2
BkTunnel ID: Invalid                 BkInterface: GigabitEthernet1/0/1
FtnIndex: 0x0                        TrafficIndex: N/A
Connector: N/A
Configuring a default route

A default route is used to forward packets that do not match any specific routing entry in the routing table. Without a default route, packets that do not match any routing entries are discarded and an ICMP destination-unreachable packet is sent to the source.

A default route can be configured in either of the following ways:

- The network administrator can configure a default route with both destination and mask being 0.0.0.0. For more information, see "Configuring a static route."
- Some dynamic routing protocols, such as OSPF, RIP, and IS-IS, can generate a default route. For example, an upstream router running OSPF can generate a default route and advertise it to other routers. These routers install the default route with the next hop being the upstream router. For more information, see the respective chapters on these routing protocols in this configuration guide.
Configuring RIP

Overview

Routing Information Protocol (RIP) is a distance-vector IGP suited to small-sized networks. It employs UDP to exchange route information through port 520.

RIP uses a hop count to measure the distance to a destination. The hop count from a router to a directly connected network is 0. The hop count from a router to a directly connected router is 1. To limit convergence time, RIP restricts the value range of the metric from 0 to 15. A destination with a metric value of 16 (or greater) is considered unreachable. For this reason, RIP is not suitable for large-sized networks.

RIP route entries

RIP stores routing entries in a database. Each routing entry contains the following elements:

- **Destination address**—IP address of a destination host or a network.
- **Next hop**—IP address of the next hop.
- **Egress interface**—Egress interface of the route.
- **Metric**—Cost from the local router to the destination.
- **Route time**—Time elapsed since the last update. The time is reset to 0 when the routing entry is updated.
- **Route tag**—Used for route control. For more information, see "Configuring routing policies."

Routing loop prevention

RIP uses the following mechanisms to prevent routing loops:

- **Counting to infinity**—A destination with a metric value of 16 is considered unreachable. When a routing loop occurs, the metric value of a route will increment to 16 to avoid endless looping.
- **Triggered updates**—RIP immediately advertises triggered updates for topology changes to reduce the possibility of routing loops and to speed up convergence.
- **Split horizon**—Disables RIP from sending routes through the interface where the routes were learned to prevent routing loops and save bandwidth.
- **Poison reverse**—Enables RIP to set the metric of routes received from a neighbor to 16 and sends these routes back to the neighbor. The neighbor can delete such information from its routing table to prevent routing loops.

RIP operation

RIP works as follows:

1. RIP sends request messages to neighboring routers. Neighboring routers return response messages that contain their routing tables.
2. RIP uses the received responses to update the local routing table and sends triggered update messages to its neighbors. All RIP routers on the network do this to learn latest routing information.
3. RIP periodically sends the local routing table to its neighbors. After a RIP neighbor receives the message, it updates its routing table, selects optimal routes, and sends an update to other neighbors. RIP ages routes to keep only valid routes.
RIP versions

There are two RIP versions, RIPv1 and RIPv2.

RIPv1 is a classful routing protocol. It advertises messages only through broadcast. RIPv1 messages do not carry mask information, so RIPv1 can only recognize natural networks such as Class A, B, and C. For this reason, RIPv1 does not support discontiguous subnets.

RIPv2 is a classless routing protocol. It has the following advantages over RIPv1:
- Supports route tags to implement flexible route control through routing policies.
- Supports masks, route summarization, and CIDR.
- Supports designated next hops to select the best ones on broadcast networks.
- Supports multicasting route updates so only RIPv2 routers can receive these updates to reduce resource consumption.
- Supports plain text authentication and MD5 authentication to enhance security.

RIPv2 supports two transmission modes: broadcast and multicast. Multicast is the default mode using 224.0.0.9 as the multicast address. An interface operating in RIPv2 broadcast mode can also receive RIPv1 messages.

TRIP

Triggered RIP (TRIP), as an extension of RIP for Wide Area Network (WAN), is typically used for reducing the management cost of dial-up networks.

TRIP enables the router to send a routing update message only when a route entry in the routing table is updated or a next hop becomes unreachable. This avoids overhead caused by periodic routing updates through RIP broadcasts. TRIP uses an acknowledgment and retransmission mechanism to ensure successful transmission of routing updates.

TRIP introduces the following types of packets, which are identified by the Command field values in the RIP packet header:

<table>
<thead>
<tr>
<th>Type</th>
<th>Command value</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update Request</td>
<td>9</td>
<td>Requests for needed routes from the neighbor.</td>
</tr>
<tr>
<td>Update Response</td>
<td>10</td>
<td>Contains the routes requested by the neighbor.</td>
</tr>
<tr>
<td>Update Acknowledge</td>
<td>11</td>
<td>Acknowledges every received response.</td>
</tr>
</tbody>
</table>

A TRIP-enabled router retransmits an Update Request to the neighboring device at periodic intervals until an Update Response is received.

After receiving the Update Request, the neighbor returns an Update Response. The router keeps retransmitting the Update Response at periodic intervals until one of the following events occurs:
- An Update Acknowledge is received.
- The number of the retransmission times reaches the upper limit. In this case, the neighbor considers that the request sender is unreachable.

Protocols and standards

- RFC 1058, *Routing Information Protocol*
- RFC 1723, *RIP Version 2 - Carrying Additional Information*
- RFC 1721, *RIP Version 2 Protocol Analysis*
- RFC 1722, *RIP Version 2 Protocol Applicability Statement*
RIP configuration task list

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring basic RIP:</td>
</tr>
<tr>
<td>• (Required.) Enabling RIP</td>
</tr>
<tr>
<td>• (Optional.) Controlling RIP reception and advertisement on interfaces</td>
</tr>
<tr>
<td>• (Optional.) Configuring a RIP version</td>
</tr>
<tr>
<td>(Optional.) Configuring RIP route control:</td>
</tr>
<tr>
<td>• Configuring an additional routing metric</td>
</tr>
<tr>
<td>• Configuring RIPv2 route summarization</td>
</tr>
<tr>
<td>• Disabling host route reception</td>
</tr>
<tr>
<td>• Advertising a default route</td>
</tr>
<tr>
<td>• Configuring received/redistributed route filtering</td>
</tr>
<tr>
<td>• Setting a preference for RIP</td>
</tr>
<tr>
<td>• Configuring RIP route redistribution</td>
</tr>
<tr>
<td>(Optional.) Tuning and optimizing RIP networks:</td>
</tr>
<tr>
<td>• Setting RIP timers</td>
</tr>
<tr>
<td>• Enabling split horizon and poison reverse</td>
</tr>
<tr>
<td>• Setting the maximum number of ECMP routes</td>
</tr>
<tr>
<td>• Enabling zero field check on incoming RIPv1 messages</td>
</tr>
<tr>
<td>• Enabling source IP address check on incoming RIP updates</td>
</tr>
<tr>
<td>• Configuring RIPv2 message authentication</td>
</tr>
<tr>
<td>• Setting the RIP triggered update interval</td>
</tr>
<tr>
<td>• Specifying a RIP neighbor</td>
</tr>
<tr>
<td>• Configuring TRIP</td>
</tr>
<tr>
<td>• Configuring RIP network management</td>
</tr>
<tr>
<td>• Configuring the RIP packet sending rate</td>
</tr>
<tr>
<td>• Setting the maximum length of RIP packets</td>
</tr>
<tr>
<td>(Optional.) Configuring RIP GR</td>
</tr>
<tr>
<td>(Optional.) Enabling RIP NSR</td>
</tr>
<tr>
<td>(Optional.) Configuring BFD for RIP</td>
</tr>
<tr>
<td>(Optional.) Configuring RIP FRR</td>
</tr>
</tbody>
</table>

Configuring basic RIP

Before you configure basic RIP settings, complete the following tasks:

• Configure the link layer protocol.
• Configure IP addresses for interfaces to ensure IP connectivity between neighboring routers.
Enabling RIP

Follow these guidelines when you enable RIP:

- To enable multiple RIP processes on a router, you must specify an ID for each process. A RIP process ID has only local significance. Two RIP routers having different process IDs can also exchange RIP packets.
- If you configure RIP settings in interface view before enabling RIP, the settings do not take effect until RIP is enabled.
- If a physical interface is attached to multiple networks, you cannot advertise these networks in different RIP processes.
- You cannot enable multiple RIP processes on a physical interface.
- The `rip enable` command takes precedence over the `network` command.

Enabling RIP on a network

You can enable RIP on a network and specify a wildcard mask for the network. After that, only the interface attached to the network runs RIP.

To enable RIP on a network:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td><code>rip [ process-id ] [ vpn-instance vpn-instance-name ]</code></td>
<td>By default, RIP is disabled.</td>
</tr>
<tr>
<td>3.</td>
<td><code>network network-address [ wildcard-mask ]</code></td>
<td>By default, RIP is disabled on a network. The <code>network 0.0.0.0</code> command can enable RIP on all interfaces in a single process, but does not apply to multiple RIP processes.</td>
</tr>
</tbody>
</table>

Enabling RIP on an interface

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td><code>rip [ process-id ] [ vpn-instance vpn-instance-name ]</code></td>
<td>By default, RIP is disabled.</td>
</tr>
<tr>
<td>3.</td>
<td><code>quit</code></td>
<td>N/A</td>
</tr>
<tr>
<td>4.</td>
<td><code>interface interface-type interface-number</code></td>
<td>N/A</td>
</tr>
<tr>
<td>5.</td>
<td><code>rip process-id enable [ exclude-subip ]</code></td>
<td>By default, RIP is disabled on an interface.</td>
</tr>
</tbody>
</table>

Controlling RIP reception and advertisement on interfaces

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td><code>rip [ process-id ] [ vpn-instance vpn-instance-name ]</code></td>
<td>N/A</td>
</tr>
</tbody>
</table>
Configuring a RIP version

You can configure a global RIP version in RIP view or an interface-specific RIP version in interface view.

An interface preferentially uses the interface-specific RIP version. If no interface-specific version is specified, the interface uses the global RIP version. If neither a global nor interface-specific RIP version is configured, the interface sends RIPv1 broadcasts and can receive the following:

- RIPv1 broadcasts and unicasts.
- RIPv2 broadcasts, multicasts, and unicasts.

To configure a RIP version:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>rip [ process-id ] [ vpn-instance vpn-instance-name ]</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>version { 1</td>
<td>2 }</td>
</tr>
<tr>
<td>4.</td>
<td>quit</td>
<td>N/A</td>
</tr>
<tr>
<td>5.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>6.</td>
<td>rip version { 1</td>
<td>2 [ broadcast</td>
</tr>
</tbody>
</table>
Configuring RIP route control

Before you configure RIP route control, complete the following tasks:

- Configure IP addresses for interfaces to ensure IP connectivity between neighboring routers.
- Configure basic RIP.

Configuring an additional routing metric

An additional routing metric (hop count) can be added to the metric of an inbound or outbound RIP route.

An outbound additional metric is added to the metric of a sent route, and it does not change the route's metric in the routing table.

An inbound additional metric is added to the metric of a received route before the route is added into the routing table, and the route's metric is changed. If the sum of the additional metric and the original metric is greater than 16, the metric of the route is 16.

To configure additional routing metrics:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>rip metricin [ route-policy route-policy-name ] value</td>
<td>The default setting is 0.</td>
</tr>
<tr>
<td>4.</td>
<td>rip metricout [ route-policy route-policy-name ] value</td>
<td>The default setting is 1.</td>
</tr>
</tbody>
</table>

Configuring RIPv2 route summarization

Perform this task to summarize contiguous subnets into a summary network and sends the network to neighbors. The smallest metric among all summarized routes is used as the metric of the summary route.

Enabling RIPv2 automatic route summarization

Automatic summarization enables RIPv2 to generate a natural network for contiguous subnets. For example, suppose there are three subnet routes 10.1.1.0/24, 10.1.2.0/24, and 10.1.3.0/24. Automatic summarization automatically creates and advertises a summary route 10.0.0.0/8 instead of the more specific routes.

To enable RIPv2 automatic route summarization:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>rip [ process-id ] [ vpn-instance vpn-instance-name ]</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>summary</td>
<td>By default, RIPv2 automatic route summarization is enabled. If subnets in the routing table are not contiguous, disable automatic route summarization to advertise</td>
</tr>
</tbody>
</table>
Advertising a summary route

Perform this task to manually configure a summary route.

For example, suppose contiguous subnets routes 10.1.1.0/24, 10.1.2.0/24, and 10.1.3.0/24 exist in the routing table. You can create a summary route 10.1.0.0/16 on GigabitEthernet 1/0/1 to advertise the summary route instead of the more specific routes.

To configure a summary route:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter RIP view.</td>
<td>rip [ process-id ] [ vpn-instance vpn-instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Disable RIPv2 automatic route summarization.</td>
<td>undo summary</td>
</tr>
<tr>
<td>4.</td>
<td>Return to system view.</td>
<td>quit</td>
</tr>
<tr>
<td>5.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>6.</td>
<td>Configure a summary route.</td>
<td>rip summary-address ip-address { mask-length</td>
</tr>
</tbody>
</table>

Disabling host route reception

Perform this task to disable RIPv2 from receiving host routes from the same network to save network resources. This feature does not apply to RIPv1.

To disable RIP from receiving host routes:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter RIP view.</td>
<td>rip [ process-id ] [ vpn-instance vpn-instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Disable RIP from receiving host routes.</td>
<td>undo host-route</td>
</tr>
</tbody>
</table>

Advertising a default route

You can advertise a default route on all RIP interfaces in RIP view or on a specific RIP interface in interface view. The interface view setting takes precedence over the RIP view settings.

To disable an interface from advertising a default route, use the rip default-route no-originate command on the interface.

To configure RIP to advertise a default route:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
### Configuring received/redistributed route filtering

Perform this task to filter received and redistributed routes by using a filtering policy.

To configure route filtering:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter RIP view.</td>
<td>rip [ process-id ] [ vpn-instance vpn-instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the filtering of received routes.</td>
<td>filter-policy { ipv4-acl-number }</td>
</tr>
<tr>
<td></td>
<td></td>
<td>gateway prefix-list-name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>prefix-list prefix-list-name { gateway prefix-list-name }</td>
</tr>
<tr>
<td></td>
<td></td>
<td>import { interface-type interface-number }</td>
</tr>
<tr>
<td>4.</td>
<td>Configure the filtering of redistributed routes.</td>
<td>filter-policy { ipv4-acl-number }</td>
</tr>
<tr>
<td></td>
<td></td>
<td>prefix-list prefix-list-name export { protocol [ process-id ] }</td>
</tr>
<tr>
<td></td>
<td></td>
<td>{ interface-type interface-number }</td>
</tr>
</tbody>
</table>

### Setting a preference for RIP

If multiple IGPs find routes to the same destination, the route found by the IGP that has the highest priority is selected as the optimal route. Perform this task to assign a preference to RIP. The smaller the preference value, the higher the priority.

To set a preference for RIP:
### Configuring RIP route redistribution

Perform this task to configure RIP to redistribute routes from other routing protocols, including OSPF, IS-IS, BGP, static, and direct.

To configure RIP route redistribution:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter RIP view.</td>
<td>rip [ process-id ] [ vpn-instance vpn-instance-name ] N/A</td>
</tr>
<tr>
<td>3.</td>
<td>Set a preference for RIP.</td>
<td>preference { preference</td>
</tr>
<tr>
<td>4.</td>
<td>(Optional.) Set a default cost for redistributed routes.</td>
<td>default cost cost-value The default setting is 0.</td>
</tr>
</tbody>
</table>

### Tuning and optimizing RIP networks

#### Configuration prerequisites

Before you tune and optimize RIP networks, complete the following tasks:

- Configure IP addresses for interfaces to ensure IP connectivity between neighboring nodes.
- Configure basic RIP.

#### Setting RIP timers

You can change the RIP network convergence speed by adjusting the following RIP timers:

- **Update timer**—Specifies the interval between route updates.
- **Timeout timer**—Specifies the route aging time. If no update for a route is received within the aging time, the metric of the route is set to 16.
- **Suppress timer**—Specifies how long a RIP route stays in suppressed state. When the metric of a route is 16, the route enters the suppressed state. A suppressed route can be replaced by an updated route that is received from the same neighbor before the suppress timer expires and has a metric less than 16.
• **Garbage-collect timer**—Specifies the interval from when the metric of a route becomes 16 to when it is deleted from the routing table. RIP advertises the route with a metric of 16. If no update is announced for that route before the garbage-collect timer expires, the route is deleted from the routing table.

**IMPORTANT:**
To avoid unnecessary traffic or route flapping, configure identical RIP timer settings on RIP routers.

To set RIP timers:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter RIP view.</td>
<td>rip [ process-id ] [ vpn-instance vpn-instance-name ]</td>
<td>N/A</td>
</tr>
</tbody>
</table>
| 3. Set RIP timers. | timers { garbage-collect garbage-collect-value | suppress suppress-value | timeout timeout-value | update update-value } * | By default:  
  • The garbage-collect timer is 120 seconds.  
  • The suppress timer is 120 seconds.  
  • The timeout timer is 180 seconds.  
  • The update timer is 30 seconds. |

### Enabling split horizon and poison reverse

The split horizon and poison reverse functions can prevent routing loops.

If both split horizon and poison reverse are configured, only the poison reverse function takes effect.

#### Enabling split horizon

Split horizon disables RIP from sending routes through the interface where the routes were learned to prevent routing loops between adjacent routers.

To enable split horizon:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter interface view.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3. Enable split horizon.</td>
<td>rip split-horizon</td>
<td>By default, split horizon is enabled.</td>
</tr>
</tbody>
</table>

#### Enabling poison reverse

Poison reverse allows RIP to send routes through the interface where the routes were learned. The metric of these routes is always set to 16 (unreachable) to avoid routing loops between neighbors.

To enable poison reverse:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter interface view.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
</tbody>
</table>
### Setting the maximum number of ECMP routes

Perform this task to implement load sharing over ECMP routes.

To set the maximum number of ECMP routes:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>rip process-id [ vpn-instance-name ]</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>maximum load-balancing number</td>
<td>By default, the maximum number of RIP ECMP routes equals the maximum number of ECMP routes supported by the system.</td>
</tr>
</tbody>
</table>

### Enabling zero field check on incoming RIPv1 messages

Some fields in the RIPv1 message must be set to zero. These fields are called "zero fields." You can enable zero field check on incoming RIPv1 messages. If a zero field of a message contains a non-zero value, RIP does not process the message. If you are certain that all messages are trustworthy, disable zero field check to save CPU resources.

This feature does not apply to RIPv2 packets, because they have no zero fields.

To enable zero field check on incoming RIPv1 messages:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>rip process-id [ vpn-instance-name ]</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>checkzero</td>
<td>The default setting is enabled.</td>
</tr>
</tbody>
</table>

### Enabling source IP address check on incoming RIP updates

Perform this task to enable source IP address check on incoming RIP updates.

Upon receiving a message on an Ethernet interface, RIP compares the source IP address of the message with the IP address of the interface. If they are not in the same network segment, RIP discards the message.

Upon receiving a message on a PPP interface, RIP checks whether the source address of the message is the IP address of the peer interface. If not, RIP discards the message.

To enable source IP address check on incoming RIP updates:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Configuring RIPv2 message authentication

Perform this task to enable authentication on RIPv2 messages. This feature does not apply to RIPv1 because RIPv1 does not support authentication. Although you can specify an authentication mode for RIPv1 in interface view, the configuration does not take effect.

RIPv2 supports two authentication modes: simple authentication and MD5 authentication.

To configure RIPv2 message authentication:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>rip authentication-mode { md5 { rfc2082 { cipher</td>
<td>plain } string key-id } rfc2453 { cipher</td>
</tr>
</tbody>
</table>

Setting the RIP triggered update interval

Perform this task to avoid network overhead and reduce system resource consumption caused by frequent RIP triggered updates.

You can use the `timer triggered` command to set the maximum interval, minimum interval, and incremental interval for sending RIP triggered updates.

- For a stable network, the `minimum-interval` is used.
- If network changes become frequent, the triggered update sending interval is incremented by `$incremental-interval \times 2^{n-2}$` for each triggered update until the `maximum-interval` is reached. The value `n` is the number of triggered update times.

To set the triggered update interval:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>rip [ process-id ] [ vpn-instance vpn-instance-name ]</td>
<td>N/A</td>
</tr>
</tbody>
</table>
| 3.   | timer triggered maximum-interval [ minimum-interval [ incremental-interval ] ] | By default:  
  - The maximum interval is 5 seconds.
  - The minimum interval is 50 milliseconds.
  - The incremental interval is 200 milliseconds. |
Specifying a RIP neighbor

Typically RIP messages are sent in broadcast or multicast. To enable RIP on a link that does not support broadcast or multicast, you must manually specify RIP neighbors.

Follow these guidelines when you specify a RIP neighbor:

- Do not use the `peer ip-address` command when the neighbor is directly connected. Otherwise, the neighbor might receive both unicast and multicast (or broadcast) messages of the same routing information.
- If the specified neighbor is not directly connected, disable source address check on incoming updates.

To specify a RIP neighbor:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td><code>rip [ process-id ] [ vpn-instance vpn-instance-name ]</code></td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td><code>peer ip-address</code></td>
<td>By default, RIP does not unicast updates to any peer.</td>
</tr>
<tr>
<td>4.</td>
<td><code>undo validate-source-address</code></td>
<td>By default, source IP address check on inbound RIP updates is enabled.</td>
</tr>
</tbody>
</table>

Configuring TRIP

TRIP helps avoid network overhead caused by periodic routing updates through RIP broadcasts.

Enabling TRIP

Perform this task to enable TRIP. TRIP enables the router to send a routing update message only when a route entry in the routing table is updated or a next hop becomes unreachable.

To enable TRIP:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td><code>rip [ process-id ] [ vpn-instance vpn-instance-name ]</code></td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td><code>quit</code></td>
<td>N/A</td>
</tr>
<tr>
<td>4.</td>
<td><code>interface interface-type interface-number</code></td>
<td>N/A</td>
</tr>
<tr>
<td>5.</td>
<td><code>rip triggered</code></td>
<td>By default, TRIP is disabled. TRIP also is disabled when RIP is disabled.</td>
</tr>
</tbody>
</table>

Setting TRIP retransmission parameters

Perform this task to configure the following parameters:

- Interval at which a TRIP-enabled device retransmits an Update Request or Update Response.
- Maximum times for retransmitting an Update Response.
For two routers on an analog dial-up link, the difference between the retransmission intervals on the two ends must be greater than 50 seconds. Otherwise, they cannot become TRIP neighbors.

The formula for calculating the total TRIP Update Response retransmission time is retransmission interval × maximum retransmission times. To avoid continuous Update Response retransmission when the neighbor becomes unreachable, make sure the value of the total time is no greater than 180 seconds (TRIP timeout time).

To set TRIP retransmission parameters:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter RIP view.</td>
<td>rip [ process-id ] [ vpn-instance vpn-instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Set TRIP update retransmission interval.</td>
<td>trip retransmit timer retransmit-time-value</td>
</tr>
<tr>
<td>4.</td>
<td>Set the maximum TRIP update retransmission times.</td>
<td>trip retransmit count retransmit-count-value</td>
</tr>
</tbody>
</table>

By default, the device retransmits an Update Request or Update Response every 5 seconds.

By default, the device can retransmit an Update Response to a maximum of 36 times. No count limit is required for retransmitting an Update Request.

Configuring RIP network management

You can use network management software to manage the RIP process to which MIB is bound. To configure RIP network management:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Bind MIB to a RIP process.</td>
<td>rip mib-binding process-id</td>
</tr>
</tbody>
</table>

By default, MIB is bound to the RIP process with the smallest process ID.

Configuring the RIP packet sending rate

Perform this task to set the interval for sending RIP packets and the maximum number of RIP packets that can be sent at each interval. This feature can avoid excessive RIP packets from affecting system performance and consuming too much bandwidth.

To configure the RIP packet sending rate:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter RIP view.</td>
<td>rip [ process-id ] [ vpn-instance vpn-instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Set the interval for sending RIP packets and the maximum number of RIP packets that can be sent at each interval.</td>
<td>output-delay time count count</td>
</tr>
</tbody>
</table>

By default, an interface sends up to three RIP packets every 20 milliseconds.
### Setting the maximum length of RIP packets

**NOTE:**
The supported maximum length of RIP packets varies by vendor. Use this feature with caution to avoid compatibility issues.

The packet length of RIP packets determines how many routes can be carried in a RIP packet. Set the maximum length of RIP packets to make good use of link bandwidth.

When authentication is enabled, follow these guidelines to ensure packet forwarding:

- For simple authentication, the maximum length of RIP packets must be no less than 52 bytes.
- For MD5 authentication (with packet format defined in RFC 2453), the maximum length of RIP packets must be no less than 56 bytes.
- For MD5 authentication (with packet format defined in RFC 2082), the maximum length of RIP packets must be no less than 72 bytes.

To set the maximum length of RIP packets:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td><code>interface interface-type interface-number</code></td>
</tr>
<tr>
<td>3.</td>
<td>Set the maximum length of RIP packets.</td>
<td><code>rip max-packet-length value</code></td>
</tr>
</tbody>
</table>

### Configuring RIP GR

GR ensures forwarding continuity when a routing protocol restarts or an active/standby switchover occurs.

Two routers are required to complete a GR process. The following are router roles in a GR process:

- **GR restarter**—Graceful restarting router. It must have GR capability.
- **GR helper**—A neighbor of the GR restarter. It helps the GR restarter to complete the GR process.

After RIP restarts on a router, the router must learn RIP routes again and update its FIB table, which causes network disconnections and route reconvergence.

With the GR feature, the restarting router (known as the GR restarter) can notify the event to its GR capable neighbors. GR capable neighbors (known as GR helpers) maintain their adjacencies with...
the router within a GR interval. During this process, the FIB table of the router does not change. After
the restart, the router contacts its neighbors to retrieve its FIB.
By default, a RIP-enabled device acts as the GR helper. Perform this task on the GR restarter.

**IMPORTANT:**
You cannot enable RIP NSR on a device that acts as GR restarter.

To configure GR on the GR restarter:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter RIP view.</td>
<td>rip [ process-id ] [ vpn-instance vpn-instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Enable GR for RIP.</td>
<td>graceful-restart</td>
</tr>
<tr>
<td>4.</td>
<td>(Optional.) Set the GR interval.</td>
<td>graceful-restart interval interval</td>
</tr>
</tbody>
</table>

### Enabling RIP NSR

The following matrix shows the feature and hardware compatibility:

<table>
<thead>
<tr>
<th>Hardware</th>
<th>RIP NSR compatibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSR954(JH296A/JH297A/JH298A/JH299A/JH373A)</td>
<td>No</td>
</tr>
<tr>
<td>MSR958(JH300A/JH301A)</td>
<td>No</td>
</tr>
<tr>
<td>MSR1002-4/1003-8S</td>
<td>No</td>
</tr>
<tr>
<td>MSR2003</td>
<td>Yes</td>
</tr>
<tr>
<td>MSR2004-24/2004-48</td>
<td>Yes</td>
</tr>
<tr>
<td>MSR3012/3024/3044/3064</td>
<td>Yes</td>
</tr>
<tr>
<td>MSR4060/4080</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Nonstop Routing (NSR) allows the device to back up the routing information from the active RIP process to the standby RIP process. After an active/standby switchover, NSR can complete route regeneration without tearing down adjacencies or impacting forwarding services.

NSR does not require the cooperation of neighboring devices to recover routing information, and it is typically used more often than GR.

**IMPORTANT:**
A device that has RIP NSR enabled cannot act as GR restarter.

To enable RIP NSR:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter RIP view.</td>
<td>rip [ process-id ] [ vpn-instance ]</td>
</tr>
</tbody>
</table>
### Step Command Remarks

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td>Enable RIP NSR.</td>
<td>non-stop-routing</td>
</tr>
</tbody>
</table>

By default, RIP NSR is disabled. RIP NSR enabled for a RIP process takes effect only on that process. As a best practice, enable RIP NSR for each process if multiple RIP processes exist.

### Configuring BFD for RIP

RIP detects route failures by periodically sending requests. If it receives no response for a route within a certain time, RIP considers the route unreachable. To speed up convergence, perform this task to enable BFD for RIP. For more information about BFD, see *High Availability Configuration Guide*.

RIP supports the following BFD detection modes:

- **Single-hop echo detection**—Detection mode for a direct neighbor. In this mode, a BFD session is established only when the directly connected neighbor has route information to send.

- **Single-hop echo detection for a specific destination**—In this mode, a BFD session is established to the specified RIP neighbor when RIP is enabled on the local interface.

- **Bidirectional control detection**—Detection mode for an indirect neighbor. In this mode, a BFD session is established only when both ends have routes to send and BFD is enabled on the receiving interface.

### Configuring single-hop echo detection (for a directly connected RIP neighbor)

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure the source IP address of BFD echo packets.</td>
<td>bfd echo-source-ip ip-address</td>
</tr>
<tr>
<td>3.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>4.</td>
<td>Enable BFD for RIP.</td>
<td>rip bfd enable</td>
</tr>
</tbody>
</table>

### Configuring single-hop echo detection (for a specific destination)

When a unidirectional link occurs between the local device and a specific neighbor, BFD can detect the failure. The local device will not receive or send any RIP packets through the interface connected to the neighbor to improve convergence speed. When the link recovers, the interface can send RIP packets again.

This feature applies to RIP neighbors that are directly connected.

To configure BFD for RIP (single hop echo detection for a specific destination):
**Configuring bidirectional control detection**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure the source IP address of BFD echo packets.</td>
<td>bfd echo-source-ip ip-address</td>
</tr>
<tr>
<td>3.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>4.</td>
<td>Enable BFD for RIP.</td>
<td>rip bfd enable destination ip-address</td>
</tr>
</tbody>
</table>

**Configuring RIP FRR**

A link or router failure on a path can cause packet loss and even routing loop until RIP completes routing convergence based on the new network topology. FRR enables fast rerouting to minimize the impact of link or node failures.

**Figure 6 Network diagram for RIP FRR**

As shown in Figure 6, configure FRR on Router B by using a routing policy to specify a backup next hop. When the primary link fails, RIP directs packets to the backup next hop. At the same time, RIP
calculates the shortest path based on the new network topology, and forwards packets over that path after network convergence.

Configuration restrictions and guidelines

- RIP FRR takes effect only for RIP routes learned from directly connected neighbors.
- RIP FRR is available only when the state of primary link (with Layer 3 interfaces staying up) changes from bidirectional to unidirectional or down.
- Equal-cost routes do not support RIP FRR.

Configuration prerequisites

You must specify a next hop by using the `apply fast-reroute backup-interface` command in a routing policy and reference the routing policy for FRR. For more information about routing policy configuration, see "Configuring routing policies."

Configuration procedure

**Configuring RIP FRR**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>2.</td>
<td>Enter RIP view.</td>
<td><code>rip [ process-id ] [ vpn-instance vpn-instance-name ]</code></td>
</tr>
<tr>
<td>3.</td>
<td>Configure RIP FRR.</td>
<td><code>fast-reroute route-policy route-policy-name</code></td>
</tr>
</tbody>
</table>

**Enabling BFD for RIP FRR**

By default, RIP FRR does not use BFD to detect primary link failures. To speed up RIP convergence, enable BFD single-hop echo detection for RIP FRR to detect primary link failures.

To configure BFD for RIP FRR:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
</tbody>
</table>
| 2.   | Configure the source IP address of BFD echo packets. | `bfd echo-source-ip ip-address` | By default, the source IP address of BFD echo packets is not configured.  
The source IP address cannot be on the same network segment as any local interface's IP address.  
For more information about this command, see High Availability Command Reference. |
| 3.   | Enter interface view. | `interface interface-type interface-number` | N/A |
| 4.   | Enable BFD for RIP FRR. | `rip primary-path-detect bfd echo` | By default, BFD for RIP FRR is disabled. |
Displaying and maintaining RIP

Execute **display** commands in any view and execute **reset** commands in user view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display RIP current status and configuration information.</td>
<td><strong>display rip</strong> [process-id]</td>
</tr>
<tr>
<td>Display active routes in the RIP database.</td>
<td><strong>display rip</strong> process-id database [ip-address {mask-length</td>
</tr>
<tr>
<td>Display RIP GR information.</td>
<td><strong>display rip</strong> [process-id] graceful-restart</td>
</tr>
<tr>
<td>Display RIP interface information.</td>
<td><strong>display rip</strong> process-id interface [interface-type interface-number]</td>
</tr>
<tr>
<td>Display neighbor information for a RIP process.</td>
<td><strong>display rip</strong> process-id neighbor [interface-type interface-number]</td>
</tr>
<tr>
<td>Display RIP NSR information.</td>
<td><strong>display rip</strong> [process-id] non-stop-routing</td>
</tr>
<tr>
<td>Display routing information for a RIP process.</td>
<td><strong>display rip</strong> process-id route [ip-address {mask-length</td>
</tr>
<tr>
<td>Reset a RIP process.</td>
<td><strong>reset rip</strong> process-id process</td>
</tr>
<tr>
<td>Clear the statistics for a RIP process.</td>
<td><strong>reset rip</strong> process-id statistics</td>
</tr>
</tbody>
</table>

RIP configuration examples

Configuring basic RIP

Network requirements

As shown in Figure 7, enable RIPv2 on all interfaces on Router A and Router B. Configure Router B to not advertise route 10.2.1.0/24 to Router A, and to accept only route 2.1.1.0/24 from Router A.

**Figure 7 Network diagram**

![Network Diagram](image)

Configuration procedure

1. Configure IP addresses for interfaces. (Details not shown.)
2. Configure basic RIP by using either of the following methods:
   (Method 1) # Enable RIP on the specified networks on Router A.
   ```
   <RouterA> system-view
   [RouterA] rip
   [RouterA-rip-1] network 1.0.0.0
   [RouterA-rip-1] network 2.0.0.0
   [RouterA-rip-1] network 3.0.0.0
   ```
(Method 2) # Enable RIP on the specified interfaces on Router B.

<i>RouterB</i> system-view
[RouterB] rip
[RouterB-rip-1] quit
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] rip 1 enable
[RouterB-GigabitEthernet1/0/1] quit
[RouterB] interface gigabitethernet 1/0/2
[RouterB-GigabitEthernet1/0/2] rip 1 enable
[RouterB-GigabitEthernet1/0/2] quit
[RouterB] interface gigabitethernet 1/0/3
[RouterB-GigabitEthernet1/0/3] rip 1 enable
[RouterB-GigabitEthernet1/0/3] quit

# Display the RIP routing table on Router A.

[RouterA] display rip 1 route
Route Flags: R - RIP, T - TRIP
            P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
            D - Direct, O - Optimal, F - Flush to RIB

-------------------------------------------------------------------------------
Peer 1.1.1.2 on GigabitEthernet1/0/1
Destination/Mask  Nexthop  Cost  Tag  Flags  Sec
10.0.0.0/8  1.1.1.2  1  0  RAOF  9
Local route
Destination/Mask  Nexthop  Cost  Tag  Flags  Sec
1.1.1.0/24  0.0.0.0  0  0  RDOF  -
2.1.1.0/24  0.0.0.0  0  0  RDOF  -
3.1.1.0/24  0.0.0.0  0  0  RDOF  -

The output shows that RIPv1 uses natural masks to advertise routing information.

3. Configure a RIP version:

# Configure RIPv2 on Router A.

[RouterA] rip
[RouterA-rip-1] version 2
[RouterA-rip-1] undo summary
[RouterA-rip-1] quit

# Configure RIPv2 on Router B.

[RouterB] rip
[RouterB-rip-1] version 2
[RouterB-rip-1] undo summary
[RouterB-rip-1] quit

# Display the RIP routing table on Router A.

[RouterA] display rip 1 route
Route Flags: R - RIP, T - TRIP
            P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
            D - Direct, O - Optimal, F - Flush to RIB

-------------------------------------------------------------------------------
Peer 1.1.1.2 on GigabitEthernet1/0/1
Destination/Mask  Nexthop  Cost  Tag  Flags  Sec
10.0.0.0/8  1.1.1.2  1  0  RAOF  9
The output shows that RIPv2 uses classless subnet masks.

NOTE:
After RIPv2 is configured, RIPv1 routes might still exist in the routing table until they are aged out.

# Display the RIP routing table on Router B.
[RouterB] display rip 1 route
Route Flags: R - RIP, T - TRIP
    P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
    D - Direct, O - Optimal, F - Flush to RIB
----------------------------------------------------------------------------
Peer 1.1.1.1 on GigabitEthernet1/0/1
Destination/Mask            Nexthop           Cost    Tag     Flags   Sec
2.1.1.0/24                  1.1.1.1           1       0       RAOF    19
3.1.1.0/24                  1.1.1.1           1       0       RAOF    19
Local route
Destination/Mask            Nexthop           Cost    Tag     Flags   Sec
1.1.1.0/24                  0.0.0.0           0       0       RDOF    -
10.1.1.0/24                 0.0.0.0           0       0       RDOF    -
10.2.1.0/24                 0.0.0.0           0       0       RDOF    -

4. Configure RIP route filtering:
   # Use IP prefix lists on Router B to filter received and redistributed routes.
[RouterB] ip prefix-list aaa index 10 permit 2.1.1.0 24
[RouterB] ip prefix-list bbb index 10 deny 10.2.1.0 24
[RouterB] ip prefix-list bbb index 11 permit 0.0.0.0 0 less-equal 32
[RouterB] rip 1
[RouterB-rip-1] filter-policy prefix-list aaa import
[RouterB-rip-1] filter-policy prefix-list bbb export
[RouterB-rip-1] quit

# Display the RIP routing table on Router A.
[RouterA] display rip 1 route
Route Flags: R - RIP, T - TRIP
    P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
    D - Direct, O - Optimal, F - Flush to RIB
----------------------------------------------------------------------------
Peer 1.1.1.2 on GigabitEthernet1/0/1
Destination/Mask            Nexthop           Cost    Tag     Flags   Sec
10.1.1.0/24                 1.1.1.2           1       0       RAOF    19
Local route
Destination/Mask            Nexthop           Cost    Tag     Flags   Sec
1.1.1.0/24 0.0.0.0 0 0 RDOF -
2.1.1.0/24 0.0.0.0 0 0 RDOF -
3.1.1.0/24 0.0.0.0 0 0 RDOF -

# Display the RIP routing table on Router B.

[RouterB] display rip 1 route
Route Flags: R - RIP, T - TRIP
    P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
    D - Direct, O - Optimal, F - Flush to RIB

Peer 1.1.1.1 on GigabitEthernet1/0/1
Destination/Mask        Nexthop           Cost    Tag     Flags   Sec
2.1.1.0/24              1.1.1.1           1       0       RAOF    19
Local route
Destination/Mask        Nexthop           Cost    Tag     Flags   Sec
1.1.1.0/24              0.0.0.0           0       0       RDOF    -
10.1.1.0/24              0.0.0.0           0       0       RDOF    -
10.2.1.0/24              0.0.0.0           0       0       RDOF    -

Configuring RIP route redistribution

Network requirements

As shown in Figure 8, Router B communicates with Router A through RIP 100 and with Router C through RIP 200.

Configure RIP 200 to redistribute direct routes and routes from RIP 100 on Router B so Router C can learn routes destined for 10.2.1.0/24 and 11.1.1.0/24. Router A cannot learn routes destined for 12.3.1.0/24 and 16.4.1.0/24.

Figure 8 Network diagram

Configuration procedure

1. Configure IP addresses for interfaces. (Details not shown.)
2. Configure basic RIP:

   # Enable RIP 100, and configure RIPv2 on Router A.
   <RouterA> system-view
   [RouterA] rip 100
   [RouterA-rip-100] network 10.0.0.0
   [RouterA-rip-100] version 2
   [RouterA-rip-100] undo summary
   [RouterA-rip-100] quit

   # Enable RIP 100 and RIP 200, and configure RIPv2 on Router B.
   <RouterB> system-view
[RouterB] rip 100
[RouterB-rip-100] network 11.0.0.0
[RouterB-rip-100] version 2
[RouterB-rip-100] undo summary
[RouterB-rip-100] quit
[RouterB] rip 200
[RouterB-rip-200] network 12.0.0.0
[RouterB-rip-200] version 2
[RouterB-rip-200] undo summary
[RouterB-rip-200] quit
# Enable RIP 200, and configure RIPv2 on Router C.
<RouterC> system-view
[RouterC] rip 200
[RouterC-rip-200] network 12.0.0.0
[RouterC-rip-200] network 16.0.0.0
[RouterC-rip-200] version 2
[RouterC-rip-200] undo summary
[RouterC-rip-200] quit
# Display the IP routing table on Router C.
[RouterC] display ip routing-table

Destinations : 16        Routes : 16

<table>
<thead>
<tr>
<th>Destination/Mask</th>
<th>Proto</th>
<th>Pre</th>
<th>Cost</th>
<th>NextHop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>12.3.1.0/24</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>12.3.1.2</td>
<td>GE1/0/1</td>
</tr>
<tr>
<td>12.3.1.2/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>12.3.1.255/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>12.3.1.2</td>
<td>GE1/0/1</td>
</tr>
<tr>
<td>16.4.1.0/24</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>16.4.1.1</td>
<td>GE1/0/2</td>
</tr>
<tr>
<td>16.4.1.255/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>16.4.1.1</td>
<td>GE1/0/2</td>
</tr>
<tr>
<td>127.0.0.0/8</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>127.0.0.0/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>127.0.0.1/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>127.255.255.255/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>224.0.0.0/4</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0</td>
<td>NULL0</td>
</tr>
<tr>
<td>224.0.0.0/24</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0</td>
<td>NULL0</td>
</tr>
<tr>
<td>255.255.255.255/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
</tbody>
</table>

3. Configure RIP route redistribution:

# Configure RIP 200 to redistribute direct routes and routes from RIP 100 on Router B.
[RouterB] rip 200
[RouterB-rip-200] import-route rip 100
[RouterB-rip-200] import-route direct
[RouterB-rip-200] quit
# Display the IP routing table on Router C.
[RouterC] display ip routing-table
Network requirements

As shown in Figure 9, run RIPv2 on all the interfaces of Router A, Router B, Router C, Router D, and Router E.

Router A has two links to Router D. The link from Router B to Router D is more stable than that from Router C to Router D. Configure an additional metric for RIP routes received from GigabitEthernet 1/0/2 on Router A so Router A prefers route 1.1.5.0/24 learned from Router B.

Figure 9 Network diagram

Configuration procedure

1. Configure IP addresses for the interfaces. (Details not shown.)
2. Configure basic RIP:
   # Configure Router A.
   <RouterA> system-view
   [RouterA] rip
   [RouterA-rip-1] network 1.0.0.0
   [RouterA-rip-1] version 2

Configuring an additional metric for a RIP interface
# Configure Router B.
<RouterB> system-view
[RouterB] rip
[RouterB-rip-1] network 1.0.0.0
[RouterB-rip-1] version 2
[RouterB-rip-1] undo summary

# Configure Router C.
<RouterC> system-view
[RouterC] rip
[RouterC-rip-1] network 1.0.0.0
[RouterC-rip-1] version 2
[RouterC-rip-1] undo summary

# Configure Router D.
<RouterD> system-view
[RouterD] rip
[RouterD-rip-1] network 1.0.0.0
[RouterD-rip-1] version 2
[RouterD-rip-1] undo summary

# Configure Router E.
<RouterE> system-view
[RouterE] rip
[RouterE-rip-1] network 1.0.0.0
[RouterE-rip-1] version 2
[RouterE-rip-1] undo summary

# Display all active routes in the RIP database on Router A.
[RouterA] display rip 1 database
  1.0.0.0/8, auto-summary
  1.1.1.0/24, cost 0, nexthop 1.1.1.1, RIP-interface
  1.1.2.0/24, cost 0, nexthop 1.1.2.1, RIP-interface
  1.1.3.0/24, cost 1, nexthop 1.1.1.2
  1.1.4.0/24, cost 1, nexthop 1.1.2.2
  1.1.5.0/24, cost 2, nexthop 1.1.1.2
  1.1.5.0/24, cost 2, nexthop 1.1.2.2

The output shows two RIP routes destined for network 1.1.5.0/24. The next hops of the routes are Router B (1.1.1.2) and Router C (1.1.2.2). The cost of the routes is 2.

3. Configure an additional metric for a RIP interface:

# Configure an inbound additional metric of 3 for RIP-enabled interface GigabitEthernet 1/0/2.
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] rip metricin 3

# Display all active routes in the RIP database on Router A.
[RouterA-GigabitEthernet1/0/2] display rip 1 database
  1.0.0.0/8, auto-summary
  1.1.1.0/24, cost 0, nexthop 1.1.1.1, RIP-interface
  1.1.2.0/24, cost 0, nexthop 1.1.2.1, RIP-interface
  1.1.3.0/24, cost 1, nexthop 1.1.1.2
  1.1.4.0/24, cost 2, nexthop 1.1.1.2
The output shows that only one RIP route reaches network 1.1.5.0/24, with the next hop as Router B (1.1.1.2) and a cost of 2.

Configuring RIP to advertise a summary route

Network requirements

As shown in Figure 10, Router A and Router B run OSPF, Router D runs RIP, and Router C runs OSPF and RIP.

- Configure RIP to redistribute OSPF routes on Router C so Router D can learn routes destined for networks 10.1.1.0/24, 10.2.1.0/24, 10.5.1.0/24, and 10.6.1.0/24.
- To reduce the routing table size of Router D, configure route summarization on Router C to advertise only the summary route 10.0.0.0/8 to Router D.

Figure 10 Network diagram

Configuration procedure

1. Configure IP addresses for interfaces. (Details not shown.)
2. Configure basic OSPF:

   # Configure Router A.
   <RouterA> system-view
   [RouterA] ospf
   [RouterA-ospf-1] area 0
   [RouterA-ospf-1-area-0.0.0.0] network 10.5.1.0 0.0.0.255
   [RouterA-ospf-1-area-0.0.0.0] network 10.2.1.0 0.0.0.255
   [RouterA-ospf-1-area-0.0.0.0] quit

   # Configure Router B.
   <RouterB> system-view
   [RouterB] ospf
   [RouterB-ospf-1] area 0
   [RouterB-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
   [RouterB-ospf-1-area-0.0.0.0] network 10.6.1.0 0.0.0.255
   [RouterB-ospf-1-area-0.0.0.0] quit

   # Configure Router C.
   <RouterC> system-view
   [RouterC] ospf
   [RouterC-ospf-1] area 0
3. Configure basic RIP:
   # Configure Router C.
   [RouterC] rip 1
   [RouterC-rip-1] network 11.3.1.0
   [RouterC-rip-1] version 2
   [RouterC-rip-1] undo summary

   # Configure Router D.
   <RouterD> system-view
   [RouterD] rip 1
   [RouterD-rip-1] network 11.0.0.0
   [RouterD-rip-1] version 2
   [RouterD-rip-1] undo summary
   [RouterD-rip-1] quit

   # Configure RIP to redistribute routes from OSPF process 1 and direct routes on Router C.
   [RouterC-rip-1] import-route direct
   [RouterC-rip-1] import-route ospf 1
   [RouterC-rip-1] quit

   # Display the IP routing table on Router D.
   [RouterD] display ip routing-table

   Destinations : 15 Routes : 15

<table>
<thead>
<tr>
<th>Destination/Mask</th>
<th>Proto</th>
<th>Pre</th>
<th>Cost</th>
<th>NextHop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>10.1.1.0/24</td>
<td>RIP</td>
<td>100</td>
<td>1</td>
<td>11.3.1.1</td>
<td>GE1/0/1</td>
</tr>
<tr>
<td>10.2.1.0/24</td>
<td>RIP</td>
<td>100</td>
<td>1</td>
<td>11.3.1.1</td>
<td>GE1/0/1</td>
</tr>
<tr>
<td>10.5.1.0/24</td>
<td>RIP</td>
<td>100</td>
<td>1</td>
<td>11.3.1.1</td>
<td>GE1/0/1</td>
</tr>
<tr>
<td>10.6.1.0/24</td>
<td>RIP</td>
<td>100</td>
<td>1</td>
<td>11.3.1.1</td>
<td>GE1/0/1</td>
</tr>
<tr>
<td>11.3.1.0/24</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>11.3.1.2</td>
<td>GE1/0/1</td>
</tr>
<tr>
<td>11.3.1.0/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>11.3.1.2</td>
<td>GE1/0/1</td>
</tr>
<tr>
<td>11.3.1.2/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>11.4.1.0/24</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>11.4.1.2</td>
<td>GE1/0/2</td>
</tr>
<tr>
<td>11.4.1.0/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>11.4.1.2</td>
<td>GE1/0/2</td>
</tr>
<tr>
<td>11.4.1.2/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>127.0.0.0/8</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>127.0.0.0/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>127.0.0.1/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>127.255.255.255/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
</tbody>
</table>

4. Configure route summarization:
   # Configure route summarization on Router C to advertise only the summary route 10.0.0.0/8.
   [RouterC] interface gigabitethernet 1/0/2
   [RouterC-GigabitEthernet1/0/2] rip summary-address 10.0.0.0 8

   # Display the IP routing table on Router D.
   [RouterD] display ip routing-table
### Configuring RIP GR

#### Network requirements

As shown in Figure 11, Router A, Router B, and Router C run RIPv2.

- Enable GR on Router A. Router A acts as the GR restarter.
- Router B and Router C act as GR helpers to synchronize their routing tables with Router A by using GR.

#### Figure 11 Network diagram

![Network diagram](image)

#### Configuration procedure

1. Configure IP addresses and subnet masks for interfaces on the routers. (Details not shown.)
2. Configure RIPv2 on the routers to ensure the following: (Details not shown.)
   - Router A, Router B, and Router C can communicate with each other at Layer 3.
   - Dynamic route update can be implemented among them with RIPv2.
3. Enable RIP GR on Router A.

```
<RouterA> system-view
[RouterA] rip
```
Verifying the configuration

# Restart RIP process 1 on Router A.
[RouterA-rip-1] return
<RouterA> reset rip 1 process
Reset RIP process? [Y/N]:y

# Display GR status on Router A.
<RouterA> display rip graceful-restart
RIP process: 1
Graceful Restart capability : Enabled
Current GR state             : Normal
Graceful Restart period      : 60 seconds
Graceful Restart remaining time : 0 seconds

Configuring RIP NSR

Network requirements

As shown in Figure 12, Router A, Router B, and Router S all run RIPv2.
Enable RIP NSR on Router S to ensure correct routing when an active/standby switchover occurs on Router S.

Figure 12 Network diagram

Configuration procedure

1. Configure IP addresses and subnet masks for interfaces on the routers. (Details not shown.)
2. Configure RIPv2 on the routers to ensure the following: (Details not shown.)
   a. Router A, Router B, and Router S can communicate with each other at Layer 3.
   b. Dynamic route update can be implemented among them with RIPv2.
3. Enable RIP NSR on Router S.
   <RouterS> system-view
   [RouterS] rip 100
   [RouterS-rip-100] non-stop-routing
   [RouterS-rip-100] quit

Verifying the configuration

# Perform an active/standby switchover on Router S.
[RouterS] placement reoptimize

Predicted changes to the placement

<table>
<thead>
<tr>
<th>Program</th>
<th>Current location</th>
<th>New location</th>
</tr>
</thead>
<tbody>
<tr>
<td>lb</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>lsm</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>slsp</td>
<td>0/0</td>
<td>0/0</td>
</tr>
</tbody>
</table>
rib6 0/0 0/0
routepolicy 0/0 0/0
rib 0/0 0/0
staticroute6 0/0 0/0
staticroute 0/0 0/0
eviisis 0/0 0/0
ospf 0/0 1/0
Continue? [y/n]: y
Re-optimization of the placement start. You will be notified on completion
Re-optimization of the placement complete. Use 'display placement' to view the new placement

# Display neighbor information and route information on Router A.
[RouterA] display rip 1 neighbor
Neighbor Address: 12.12.12.2
Interface : GigabitEthernet1/0/1
Version : RIPv2     Last update: 00h00m13s
Relay nbr : No        BFD session: None
Bad packets: 0         Bad routes : 0
[RouterA] display rip 1 route
Route Flags: R - RIP, T - TRIP
        P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
        D - Direct, O - Optimal, F - Flush to RIB
----------------------------------------------------------------------------
Peer 12.12.12.2 on GigabitEthernet1/0/1
Destination/Mask        Nexthop           Cost    Tag     Flags   Sec
14.0.0.0/8              12.12.12.2        1       0       RAOF    16
44.0.0.0/8              12.12.12.2        2       0       RAOF    16
Local route

# Display neighbor information and route information on Router B.
[RouterB] display rip 1 neighbor
Interface : GigabitEthernet1/0/1
Version : RIPv2     Last update: 00h00m32s
Relay nbr : No        BFD session: None
Bad packets: 0         Bad routes : 0
[RouterB] display rip 1 route
Route Flags: R - RIP, T - TRIP
        P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
        D - Direct, O - Optimal, F - Flush to RIB
----------------------------------------------------------------------------
Peer 14.14.14.2 on GigabitEthernet1/0/1
Destination/Mask        Nexthop           Cost    Tag     Flags   Sec
12.0.0.0/8              14.14.14.2        1       0       RAOF    1
22.0.0.0/8              14.14.14.2        2       0       RAOF    1
Local route
The output shows that the neighbor and route information on Router A and Router B keep unchanged during the active/standby switchover on Router S. The traffic from Router A to Router B has not been impacted.

Configuring BFD for RIP (single-hop echo detection for a directly connected neighbor)

Network requirements

As shown in Figure 13, GigabitEthernet 1/0/1 of Router A and Router C runs RIP process 1. GigabitEthernet 1/0/2 of Router A runs RIP process 2. GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 of Router B run RIP process 1.

- Configure a static route destined for 100.1.1.1/24 and enable static route redistribution into RIP on Router C. This allows Router A to learn two routes destined for 100.1.1.1/24 through GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 respectively, and uses the one through GigabitEthernet 1/0/1.
- Enable BFD for RIP on GigabitEthernet 1/0/1 of Router A. When the link over GigabitEthernet 1/0/1 fails, BFD can quickly detect the failure and notify RIP. RIP deletes the neighbor relationship and route information learned on GigabitEthernet 1/0/1, and uses the route destined for 100.1.1.124 through GigabitEthernet 1/0/2.

Figure 13 Network diagram

Configuration procedure

1. Configure basic RIP and enable BFD on the interfaces:
   
   # Configure Router A.

   <RouterA> system-view
   [RouterA] rip 1
   [RouterA-rip-1] version 2
   [RouterA-rip-1] undo summary
   [RouterA-rip-1] network 192.168.1.0
   [RouterA-rip-1] quit
   [RouterA] interface gigabitethernet 1/0/1
   [RouterA-GigabitEthernet1/0/1] rip bfd enable
   [RouterA-GigabitEthernet1/0/1] rip bfd neighbor 192.168.2.224
   [RouterA-GigabitEthernet1/0/1] rip bfd neighbor 192.168.3.224
   [RouterA-GigabitEthernet1/0/1] quit
   [RouterA] rip 2
# Configure Router B.
<RouterB> system-view
[RouterB] rip 1
[RouterB-rip-1] version 2
[RouterB-rip-1] undo summary
[RouterB-rip-1] network 192.168.2.0
[RouterB-rip-1] network 192.168.3.0
[RouterB-rip-1] quit

# Configure Router C.
<RouterC> system-view
[RouterC] rip 1
[RouterC-rip-1] version 2
[RouterC-rip-1] undo summary
[RouterC-rip-1] network 192.168.1.0
[RouterC-rip-1] network 192.168.3.0
[RouterC-rip-1] import-route static
[RouterC-rip-1] quit

2. Configure the BFD parameters on GigabitEthernet 1/0/1 of Router A.
[RouterA] bfd echo-source-ip 11.11.11.11
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] bfd min-transmit-interval 500
[RouterA-GigabitEthernet1/0/1] bfd min-receive-interval 500
[RouterA-GigabitEthernet1/0/1] bfd detect-multiplier 7
[RouterA-GigabitEthernet1/0/1] return

3. Configure a static route on Router C.
[RouterC] ip route-static 120.1.1.1 24 null 0

Verifying the configuration

# Display the BFD session information on Router A.
<RouterA> display bfd session

Total Session Num: 1 Up Session Num: 1 Init Mode: Active

IPv4 Session Working Under Echo Mode:

<table>
<thead>
<tr>
<th>LD</th>
<th>SourceAddr</th>
<th>DestAddr</th>
<th>State</th>
<th>Holdtime</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>192.168.1.1</td>
<td>192.168.1.2</td>
<td>Up</td>
<td>2000ms</td>
<td>GE1/0/1</td>
</tr>
</tbody>
</table>

# Display RIP routes destined for 120.1.1.0/24 on Router A.
<RouterA> display ip routing-table 120.1.1.0 24

Summary count : 1

<table>
<thead>
<tr>
<th>Destination/Mask</th>
<th>Proto</th>
<th>Pre Cost</th>
<th>NextHop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>120.1.1.0/24</td>
<td>RIP</td>
<td>100</td>
<td>192.168.1.2</td>
<td>GE1/0/1</td>
</tr>
</tbody>
</table>

The output shows that Router A communicates with Router C through GigabitEthernet 1/0/1. Then the link over GigabitEthernet 1/0/1 fails.
## Display RIP routes destined for 120.1.1.0/24 on Router A.

```
<RouterA> display ip routing-table 120.1.1.0 24
```

Summary count : 1

<table>
<thead>
<tr>
<th>Destination/Mask</th>
<th>Proto</th>
<th>Pre</th>
<th>Cost</th>
<th>NextHop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>120.1.1.0/24</td>
<td>RIP</td>
<td>100</td>
<td>2</td>
<td>192.168.2.2</td>
<td>GE1/0/2</td>
</tr>
</tbody>
</table>

The output shows that Router A communicates with Router C through GigabitEthernet 1/0/2.

### Configuring BFD for RIP (single-hop echo detection for a specific destination)

#### Network requirements

As shown in Figure 14, GigabitEthernet 1/0/2 of Router A and GigabitEthernet 1/0/1 of Router B run RIP process 1. GigabitEthernet 1/0/2 of Router B and Router C runs RIP process 1.

- Configure a static route destined for 100.1.1.0/24 and enable static route redistribution into RIP on both Router A and Router C. This allows Router B to learn two routes destined for 100.1.1.0/24 through GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2. The route redistributed from Router A has a smaller cost than that redistributed from Router C, so Router B uses the route through GigabitEthernet 1/0/1.
- Enable BFD for RIP on GigabitEthernet 1/0/2 of Router A, and specify GigabitEthernet 1/0/1 of Router B as the destination. When a unidirectional link occurs between Router A and Router B, BFD can quickly detect the link failure and notify RIP. RIP then deletes the neighbor relationship and the route information learned on GigabitEthernet 1/0/2. It does not receive or send any packets on GigabitEthernet 1/0/2. When the route learned from Router A ages out, Router B uses the route destined for 100.1.1.1/24 through GigabitEthernet 1/0/2.

**Figure 14 Network diagram**

### Configuration procedure

1. Configure IP addresses for interfaces. (Details not shown.)
2. Configure basic RIP and enable BFD on the interfaces:

   ```
   # Configure Router A.
   <RouterA> system-view
   [RouterA] rip 1
   [RouterA-rip-1] network 192.168.2.0
   [RouterA-rip-1] import-route static
   ```
3. Configure BFD parameters on GigabitEthernet 1/0/2 of Router A.
   [RouterA] bfd echo-source-ip 11.11.11.11
   [RouterA] interface gigabitethernet 1/0/2
   [RouterA-GigabitEthernet1/0/2] bfd min-echo-receive-interval 500
   [RouterA-GigabitEthernet1/0/2] quit

4. Configure static routes:
   # Configure a static route on Router A.
   [RouterA] ip route-static 100.1.1.0 24 null 0
   # Configure a static route on Router C.
   [RouterC] ip route-static 100.1.1.0 24 null 0

Verifying the configuration

# Display the BFD session information on Router A.
<RouterA> display bfd session

  Total Session Num: 1   Up Session Num: 1   Init Mode: Active

  IPv4 session working under Echo mode:

<table>
<thead>
<tr>
<th>LD</th>
<th>SourceAddr</th>
<th>DestAddr</th>
<th>State</th>
<th>Holdtime</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>192.168.2.1</td>
<td>192.168.2.2</td>
<td>Up</td>
<td>2000ms</td>
<td>GE1/0/2</td>
</tr>
</tbody>
</table>

# Display routes destined for 100.1.1.0/24 on Router B.
<RouterB> display ip routing-table 100.1.1.0 24 verbose

  Summary Count : 1

  Destination: 100.1.1.0/24
  Protocol: RIP
  Process ID: 1
  SubProtID: 0x1  Age: 00h02m47s
  Cost: 1  Preference: 100
  IpPre: N/A  QosLocalID: N/A
# Display routes destined for 100.1.1.0/24 on Router B when the link between Router A and Router B fails.

```
<RouterB> display ip routing-table 100.1.1.0 24 verbose
```

Summary Count : 1

Destination: 100.1.1.0/24
 Protocol: RIP
 Process ID: 1
 SubProtID: 0x1  Age: 00h21m23s
 Cost: 4  Preference: 100
 IpPre: N/A  QosLocalID: N/A
 Tag: 0  State: Active Adv
OrigTblID: 0x0  OrigVrf: default-vrf
TableID: 0x2  OrigAs: 0
NibID: 0x12000003  LastAs: 0
AttrID: 0xffffffff  Neighbor: 192.168.3.2
Flags: 0x1008c  OrigNextHop: 192.168.3.2
Label: NULL  RealNextHop: 192.168.3.2
BkLabel: NULL  BkNextHop: N/A
Tunnel ID: Invalid  Interface: GigabitEthernet1/0/1
BkTunnel ID: Invalid  BkInterface: N/A
FtnIndex: 0x0  TrafficIndex: N/A
Connector: N/A

Configuring BFD for RIP (bidirectional control detection)

### Network requirements

As shown in Figure 15, GigabitEthernet 1/0/2 of Router A and GigabitEthernet 1/0/1 of Router C run RIP process 1. GigabitEthernet 1/0/1 on Router A runs RIP process 2. GigabitEthernet 1/0/2 on Router C, and GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 on Router D run RIP process 1.

- Configure a static route destined for 100.1.1.0/24 on Router A.
- Configure a static route destined for 101.1.1.0/24 on Router C.
- Enable static route redistribution into RIP on Router A and Router C. This allows Router A to learn two routes destined for 100.1.1.0/24 through GigabitEthernet 1/0/2 and GigabitEthernet 1/0/1. It uses the route through GigabitEthernet 1/0/2.
• Enable BFD for RIP on GigabitEthernet 1/0/2 of Router A and GigabitEthernet 1/0/1 of Router C.

When the link over GigabitEthernet 1/0/2 fails, BFD can quickly detect the link failure and notify RIP. RIP deletes the neighbor relationship and the route information learned on GigabitEthernet 1/0/2, and uses the route destined for 100.1.1.0/24 through GigabitEthernet 1/0/1.

Figure 15 Network diagram

Table 7 Interface and IP address assignment

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router A</td>
<td>GigabitEthernet 1/0/1</td>
<td>192.168.3.1/24</td>
</tr>
<tr>
<td>Router A</td>
<td>GigabitEthernet 1/0/2</td>
<td>192.168.1.1/24</td>
</tr>
<tr>
<td>Router B</td>
<td>GigabitEthernet 1/0/1</td>
<td>192.168.2.1/24</td>
</tr>
<tr>
<td>Router B</td>
<td>GigabitEthernet 1/0/2</td>
<td>192.168.1.2/24</td>
</tr>
<tr>
<td>Router C</td>
<td>GigabitEthernet 1/0/1</td>
<td>192.168.2.2/24</td>
</tr>
<tr>
<td>Router C</td>
<td>GigabitEthernet 1/0/2</td>
<td>192.168.4.2/24</td>
</tr>
<tr>
<td>Router D</td>
<td>GigabitEthernet 1/0/1</td>
<td>192.168.3.2/24</td>
</tr>
<tr>
<td>Router D</td>
<td>GigabitEthernet 1/0/2</td>
<td>192.168.4.1/24</td>
</tr>
</tbody>
</table>

Configuration procedure

1. Configure IP addresses for interfaces. (Details not shown.)
2. Configure basic RIP and enable static route redistribution into RIP so Router A and Router C have routes to send to each other:

   # Configure Router A.

   <RouterA> system-view
   [RouterA] rip 1
   [RouterA-rip-1] version 2
   [RouterA-rip-1] undo summary
   [RouterA-rip-1] network 192.168.1.0
   [RouterA-rip-1] network 101.1.1.0
   [RouterA-rip-1] peer 192.168.2.2
   [RouterA-rip-1] undo validate-source-address
   [RouterA-rip-1] import-route static
# Configure Router A.

[RouterA-rip-1] quit
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] rip bfd enable
[RouterA-GigabitEthernet1/0/2] quit
[RouterA] rip 2
[RouterA-rip-2] version 2
[RouterA-rip-2] undo summary
[RouterA-rip-2] network 192.168.3.0
[RouterA-rip-2] quit

# Configure Router B.

[RouterB] system-view

[RouterB] interface gigabitethernet 1/0/2

# Configure Router C.

<RouterC> system-view

[RouterC] rip 1
[RouterC-rip-1] version 2
[RouterC-rip-1] undo summary
[RouterC-rip-1] network 192.168.2.0
[RouterC-rip-1] network 192.168.4.0
[RouterC-rip-1] network 100.1.1.0
[RouterC-rip-1] peer 192.168.1.1
[RouterC-rip-1] undo validate-source-address
[RouterC-rip-1] import-route static
[RouterC-rip-1] quit
[RouterC] interface gigabitethernet 1/0/1
[RouterC-GigabitEthernet1/0/1] rip bfd enable
[RouterC-GigabitEthernet1/0/1] quit

# Configure Router D.

<RouterD> system-view

[RouterD] rip 1
[RouterD-rip-1] version 2
[RouterD-rip-1] undo summary
[RouterD-rip-1] network 192.168.3.0
[RouterD-rip-1] network 192.168.4.0
[RouterD-rip-1] quit

3. Configure BFD parameters for the interfaces:

# Configure Router A.

[RouterA] bfd session init-mode active
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] ip address 192.168.3.1 24
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] ip address 192.168.1.1 24
[RouterA-GigabitEthernet1/0/2] bfd min-transmit-interval 500
[RouterA-GigabitEthernet1/0/2] bfd min-receive-interval 500
[RouterA-GigabitEthernet1/0/2] bfd detect-multiplier 7
[RouterA-GigabitEthernet1/0/2] quit

# Configure Router B.

<RouterB> system-view

[RouterB] interface gigabitethernet 1/0/2
[RouterB-GigabitEthernet1/0/2] ip address 192.168.1.2 24
Verify the configuration

4. Configure static routes:

# Configure a static route to Router C on Router A.
<RouterA> ip route-static 192.168.2.0 24 gigabitethernet 1/0/2 192.168.1.2
<RouterA> quit

# Configure a static route to Router A on Router C.
<RouterC> ip route-static 192.168.1.0 24 gigabitethernet 1/0/1 192.168.2.1

The output shows that Router A communicates with Router C through GigabitEthernet 1/0/2. Then the link over GigabitEthernet 1/0/2 fails.

# Display RIP routes destined for 100.1.1.0/24 on Router A.
<RouterA> display ip routing-table 100.1.1.0 24

Summary count : 1

Destination/Mask Proto Pre Cost NextHop  Interface
100.1.1.0/24 RIP 100 1 192.168.2.2 GE1/0/2
<RouterA> display ip routing-table 100.1.1.0

Summary count : 1

<table>
<thead>
<tr>
<th>Destination/Mask</th>
<th>Proto</th>
<th>Pre</th>
<th>Cost</th>
<th>NextHop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>100.1.1.0/24</td>
<td>RIP</td>
<td>100</td>
<td>2</td>
<td>192.168.3.2</td>
<td>GE1/0/1</td>
</tr>
</tbody>
</table>

The output shows that Router A communicates with Router C through GigabitEthernet 1/0/1.

Configuring RIP FRR

Network requirements

As shown in Figure 16, Router A, Router B, and Router C run RIPv2. Configure RIP FRR so that when Link A becomes unidirectional, traffic can be switched to Link B immediately.

Figure 16 Network diagram

Table 8 Interface and IP address assignment

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router A</td>
<td>GigabitEthernet 1/0/1</td>
<td>12.12.12.1/24</td>
</tr>
<tr>
<td>Router A</td>
<td>GigabitEthernet 1/0/2</td>
<td>13.13.13.1/24</td>
</tr>
<tr>
<td>Router A</td>
<td>Loopback 0</td>
<td>1.1.1.1/32</td>
</tr>
<tr>
<td>Router B</td>
<td>GigabitEthernet 1/0/1</td>
<td>24.24.24.4/24</td>
</tr>
<tr>
<td>Router B</td>
<td>GigabitEthernet 1/0/2</td>
<td>13.13.13.2/24</td>
</tr>
<tr>
<td>Router B</td>
<td>Loopback 0</td>
<td>4.4.4.4/32</td>
</tr>
<tr>
<td>Router C</td>
<td>GigabitEthernet 1/0/1</td>
<td>12.12.12.2/24</td>
</tr>
<tr>
<td>Router C</td>
<td>GigabitEthernet 1/0/2</td>
<td>24.24.24.2/24</td>
</tr>
</tbody>
</table>

Configuration procedure

1. Configure IP addresses and subnet masks for interfaces on the routers. (Details not shown.)
2. Configure RIPv2 on the routers to make sure Router A, Router B, and Router C can communicate with each other at the network layer. (Details not shown.)
3. Configure RIP FRR:
   # Configure Router A.
   <RouterA> system-view
   [RouterA] ip prefix-list abc index 10 permit 4.4.4.4 32
   [RouterA] route-policy frr permit node 10
   [RouterA-route-policy-frr-10] if-match ip address prefix-list abc
[RouterA-route-policy-frr-10] quit
[RouterA] rip 1
[RouterA-rip-1] fast-reroute route-policy frr
[RouterA-rip-1] quit

# Configure Router B.
<RouterB> system-view
[RouterB] ip prefix-list abc index 10 permit 1.1.1.1 32
[RouterB] route-policy frr permit node 10
[RouterB-route-policy-frr-10] if-match ip address prefix-list abc
[RouterB-route-policy-frr-10] apply fast-reroute backup-interface gigabitethernet 1/0/1 backup-nexthop 24.24.24.2
[RouterB-route-policy-frr-10] quit
[RouterB] rip 1
[RouterB-rip-1] fast-reroute route-policy frr
[RouterB-rip-1] quit

Verifying the configuration

# Display route 4.4.4.4/32 on Router A to view the backup next hop information.
[RouterA] display ip routing-table 4.4.4.4 verbose

Destination: 4.4.4.4/32
Protocol: RIP
Process ID: 1
SubProtID: 0x1                  Age: 04h20m37s
  Cost: 1              Preference: 100
  IpPre: N/A           QosLocalID: N/A
  Tag: 0                State: Active Adv
  OrigTblID: 0x0         OrigVrf: default-vrf
  TableID: 0x2          OrigAs: 0
  NibID: 0x26000002     LastAs: 0
  AttrID: 0xffffffff    Neighbor: 13.13.13.2
  Flags: 0x1008c        OrigNextHop: 13.13.13.2
  Label: NULL           RealNextHop: 13.13.13.2
  BkLabel: NULL         BkNextHop: 12.12.12.2
  Tunnel ID: Invalid    Interface: GigabitEthernet1/0/2
  BkTunnel ID: Invalid  BkInterface: GigabitEthernet1/0/1
  FtnIndex: 0x0         TrafficIndex: N/A
  Connector: N/A

# Display route 1.1.1.1/32 on Router B to view the backup next hop information.
[RouterB] display ip routing-table 1.1.1.1 verbose

Summary Count : 1

Destination: 1.1.1.1/32
Protocol: RIP
Process ID: 1
SubProtID: 0x1                  Age: 04h20m37s
Cost: 1                Preference: 100
IpPre: N/A              QosLocalID: N/A
Tag: 0                  State: Active Adv
OrigTblID: 0x0          OrigVrf: default-vrf
TableID: 0x2            OrigAs: 0
NibID: 0x26000002       LastAs: 0
AttrID: 0xffffffff      Neighbor: 13.13.13.1
Flags: 0x1008c          OrigNextHop: 13.13.13.1
Label: NULL             RealNextHop: 13.13.13.1
BkLabel: NULL           BkNextHop: 24.24.24.2
Tunnel ID: Invalid      Interface: GigabitEthernet1/0/2
BkTunnel ID: Invalid    BkInterface: GigabitEthernet1/0/1
FtnIndex: 0x0           TrafficIndex: N/A
Connector: N/A
Configuring OSPF

Overview

Open Shortest Path First (OSPF) is a link-state IGP developed by the OSPF working group of the IETF. OSPF version 2 is used for IPv4. OSPF refers to OSPFv2 throughout this chapter.

OSPF has the following features:

- **Wide scope**—Supports multiple network sizes and several hundred routers in an OSPF routing domain.
- **Fast convergence**—Advertises routing updates instantly upon network topology changes.
- **Loop free**—Computes routes with the SPF algorithm to avoid routing loops.
- **Area-based network partition**—Splits an AS into multiple areas to facilitate management. This feature reduces the LSDB size on routers to save memory and CPU resources, and reduces route updates transmitted between areas to save bandwidth.
- **ECMP routing**—Supports multiple equal-cost routes to a destination.
- **Routing hierarchy**—Supports a 4-level routing hierarchy that prioritizes routes into intra-area, inter-area, external Type-1, and external Type-2 routes.
- **Authentication**—Supports area- and interface-based packet authentication to ensure secure packet exchange.
- **Support for multicasting**—Multicasts protocol packets on some types of links to avoid impacting other devices.

OSPF packets

OSPF messages are carried directly over IP. The protocol number is 89.

OSPF uses the following packet types:

- **Hello**—Periodically sent to find and maintain neighbors, containing timer values, information about the DR, BDR, and known neighbors.
- **Database description (DD)**—Describes the digest of each LSA in the LSDB, exchanged between two routers for data synchronization.
- **Link state request (LSR)**—Requests needed LSAs from a neighbor. After exchanging the DD packets, the two routers know which LSAs of the neighbor are missing from their LSDBs. They then exchange LSR packets requesting the missing LSAs. LSR packets contain the digest of the missing LSAs.
- **Link state update (LSU)**—Transmits the requested LSAs to the neighbor.
- **Link state acknowledgment (LSAck)**—Acknowledges received LSU packets. It contains the headers of received LSAs (an LSAck packet can acknowledge multiple LSAs).

LSA types

OSPF advertises routing information in Link State Advertisements (LSAs). The following LSAs are commonly used:

- **Router LSA**—Type-1 LSA, originated by all routers and flooded throughout a single area only. This LSA describes the collected states of the router’s interfaces to an area.
Network LSA—Type-2 LSA, originated for broadcast and NBMA networks by the designated router, and flooded throughout a single area only. This LSA contains the list of routers connected to the network.

Network Summary LSA—Type-3 LSA, originated by Area Border Routers (ABRs), and flooded throughout the LSA’s associated area. Each summary-LSA describes a route to a destination outside the area, yet still inside the AS (an inter-area route).

ASBR Summary LSA—Type-4 LSA, originated by ABRs and flooded throughout the LSA’s associated area. Type 4 summary-LSAs describe routes to Autonomous System Boundary Router (ASBR).

AS External LSA—Type-5 LSA, originated by ASBRs, and flooded throughout the AS (except stub and NSSA areas). Each AS-external-LSA describes a route to another AS.

NSSA LSA—Type-7 LSA, as defined in RFC 1587, originated by ASBRs in NSSAs and flooded throughout a single NSSA. NSSA LSAs describe routes to other ASs.

Opaque LSA—A proposed type of LSA. Its format consists of a standard LSA header and application specific information. Opaque LSAs are used by the OSPF protocol or by some applications to distribute information into the OSPF routing domain. The opaque LSA includes Type 9, Type 10, and Type 11. The Type 9 opaque LSA is flooded into the local subnet, the Type 10 is flooded into the local area, and the Type 11 is flooded throughout the AS.

**OSPF areas**

In large OSPF routing domains, SPF route computations consume too many storage and CPU resources, and enormous OSPF packets generated for route synchronization occupy excessive bandwidth.

To resolve these issues, OSPF splits an AS into multiple areas. Each area is identified by an area ID. The boundaries between areas are routers rather than links. A network segment (or a link) can only reside in one area as shown in Figure 17.

You can configure route summarization on ABRs to reduce the number of LSAs advertised to other areas and minimize the effect of topology changes.

**Figure 17 Area-based OSPF network partition**
Backbone area and virtual links

Each AS has a backbone area that distributes routing information between non-backbone areas. Routing information between non-backbone areas must be forwarded by the backbone area. OSPF has the following requirements:

- All non-backbone areas must maintain connectivity to the backbone area.
- The backbone area must maintain connectivity within itself.

In practice, these requirements might not be met due to lack of physical links. OSPF virtual links can solve this issue.

A virtual link is established between two ABRs through a non-backbone area. It must be configured on both ABRs to take effect. The non-backbone area is called a transit area.

As shown in Figure 18, Area 2 has no direct physical link to the backbone Area 0. You can configure a virtual link between the two ABRs to connect Area 2 to the backbone area.

Figure 18 Virtual link application 1

Virtual links can also be used as redundant links. If a physical link failure breaks the internal connectivity of the backbone area, you can configure a virtual link to replace the failed physical link, as shown in Figure 19.

Figure 19 Virtual link application 2

The virtual link between the two ABRs acts as a point-to-point connection. You can configure interface parameters, such as hello interval, on the virtual link as they are configured on a physical interface.

The two ABRs on the virtual link unicast OSPF packets to each other, and the OSPF routers in between convey these OSPF packets as normal IP packets.

Stub area and totally stub area

A stub area does not distribute Type-5 LSAs to reduce the routing table size and LSAs advertised within the area. The ABR of the stub area advertises a default route in a Type-3 LSA so that the routers in the area can reach external networks through the default route.

To further reduce the routing table size and advertised LSAs, you can configure the stub area as a totally stub area. The ABR of a totally stub area does not advertise inter-area routes or external
routes. It advertises a default route in a Type-3 LSA so that the routers in the area can reach external networks through the default route.

**NSSA area and totally NSSA area**

An NSSA area does not import AS external LSAs (Type-5 LSAs) but can import Type-7 LSAs generated by the NSSA ASBR. The NSSA ABR translates Type-7 LSAs into Type-5 LSAs and advertises the Type-5 LSAs to other areas.

As shown in Figure 20, the OSPF AS contains Area 1, Area 2, and Area 0. The other two ASs run RIP. Area 1 is an NSSA area where the ASBR redistributes RIP routes in Type-7 LSAs into Area 1. Upon receiving the Type-7 LSAs, the NSSA ABR translates them to Type-5 LSAs, and advertises the Type-5 LSAs to Area 0.

The ASBR of Area 2 redistributes RIP routes in Type-5 LSAs into the OSPF routing domain. However, Area 1 does not receive Type-5 LSAs because it is an NSSA area.

**Figure 20 NSSA area**

**Router types**

OSPF routers are classified into the following types based on their positions in the AS:

- **Internal router**—All interfaces on an internal router belong to one OSPF area.
- **ABR**—Belongs to more than two areas, one of which must be the backbone area. ABR connects the backbone area to a non-backbone area. An ABR and the backbone area can be connected through a physical or logical link.
- **Backbone router**—No less than one interface of a backbone router must reside in the backbone area. All ABRs and internal routers in Area 0 are backbone routers.
- **ASBR**—Exchanges routing information with another AS is an ASBR. An ASBR might not reside on the border of the AS. It can be an internal router or an ABR.
Route types

OSPF prioritizes routes into the following route levels:

- Intra-area route.
- Inter-area route.
- Type-1 external route.
- Type-2 external route.

The intra-area and inter-area routes describe the network topology of the AS. The external routes describe routes to external ASs.

A Type-1 external route has high credibility. The cost of a Type-1 external route = the cost from the router to the corresponding ASBR + the cost from the ASBR to the destination of the external route.

A Type-2 external route has low credibility. OSPF considers that the cost from the ASBR to the destination of a Type-2 external route is much greater than the cost from the ASBR to an OSPF internal router. The cost of a Type-2 external route = the cost from the ASBR to the destination of the Type-2 external route. If two Type-2 routes to the same destination have the same cost, OSPF takes the cost from the router to the ASBR into consideration to determine the best route.

Route calculation

OSPF computes routes in an area as follows:

- Each router generates LSAs based on the network topology around itself, and sends them to other routers in update packets.
- Each OSPF router collects LSAs from other routers to compose an LSDB. An LSA describes the network topology around a router, and the LSDB describes the entire network topology of the area.
Each router transforms the LSDB to a weighted directed graph that shows the topology of the area. All the routers within the area have the same graph.

Each router uses the SPF algorithm to compute a shortest path tree that shows the routes to the nodes in the area. The router itself is the root of the tree.

**OSPF network types**

OSPF classifies networks into the following types, depending on different link layer protocols:

- **Broadcast**—If the link layer protocol is Ethernet or FDDI, OSPF considers the network type as broadcast by default. On a broadcast network, hello, LSU, and LSAck packets are multicast to 224.0.0.5 that identifies all OSPF routers or to 224.0.0.6 that identifies the DR and BDR. DD packets and LSR packets are unicast.

- **NBMA**—If the link layer protocol is Frame Relay, ATM, or X.25, OSPF considers the network type as NBMA by default. OSPF packets are unicast on an NBMA network.

- **P2MP**—No link is P2MP type by default. P2MP must be a conversion from other network types such as NBMA. On a P2MP network, OSPF packets are multicast to 224.0.0.5.

- **P2P**—If the link layer protocol is PPP or HDLC, OSPF considers the network type as P2P. On a P2P network, OSPF packets are multicast to 224.0.0.5.

The following are the differences between NBMA and P2MP networks:

- NBMA networks are fully meshed. P2MP networks are not required to be fully meshed.
- NBMA networks require DR and BDR election. P2MP networks do not have DR or BDR.
- On an NBMA network, OSPF packets are unicast, and neighbors are manually configured. On a P2MP network, OSPF packets are multicast by default, and you can configure OSPF to unicast protocol packets.

**DR and BDR**

**DR and BDR mechanism**

On a broadcast or NBMA network, any two routers must establish an adjacency to exchange routing information with each other. If n routers are present on the network, n(n-1)/2 adjacencies are established. Any topology change on the network results in an increase in traffic for route synchronization, which consumes a large amount of system and bandwidth resources.

Using the DR and BDR mechanisms can solve this problem.

- **DR**—Elected to advertise routing information among other routers. If the DR fails, routers on the network must elect another DR and synchronize information with the new DR. Using this mechanism without BDR is time-consuming and is prone to route calculation errors.

- **BDR**—Elected along with the DR to establish adjacencies with all other routers. If the DR fails, the BDR immediately becomes the new DR, and other routers elect a new BDR.

Routers other than the DR and BDR are called DR Others. They do not establish adjacencies with one another, so the number of adjacencies is reduced.

The role of a router is subnet (or interface) specific. It might be a DR on one interface and a BDR or DR Other on another interface.

As shown in Figure 22, solid lines are Ethernet physical links, and dashed lines represent OSPF adjacencies. With the DR and BDR, only seven adjacencies are established.
NOTE:
In OSPF, neighbor and adjacency are different concepts. After startup, OSPF sends a hello packet on each OSPF interface. A receiving router checks parameters in the packet. If the parameters match its own, the receiving router considers the sending router an OSPF neighbor. Two OSPF neighbors establish an adjacency relationship after they synchronize their LSDBs through exchange of DD packets and LSAs.

DR and BDR election

DR election is performed on broadcast or NBMA networks but not on P2P and P2MP networks.

Routers in a broadcast or NBMA network elect the DR and BDR by router priority and ID. Routers with a router priority value higher than 0 are candidates for DR and BDR election.

The election votes are hello packets. Each router sends the DR elected by itself in a hello packet to all the other routers. If two routers on the network declare themselves as the DR, the router with the higher router priority wins. If router priorities are the same, the router with the higher router ID wins.

If a router with a higher router priority becomes active after DR and BDR election, the router cannot replace the DR or BDR until a new election is performed. Therefore, the DR of a network might not be the router with the highest priority, and the BDR might not be the router with the second highest priority.

Protocols and standards

- RFC 1765, OSPF Database Overflow
- RFC 2328, OSPF Version 2
- RFC 3101, OSPF Not-So-Stubby Area (NSSA) Option
- RFC 3137, OSPF Stub Router Advertisement
- RFC 4811, OSPF Out-of-Band LSDB Resynchronization
- RFC 4812, OSPF Restart Signaling
- RFC 4813, OSPF Link-Local Signaling

OSPF configuration task list

To run OSPF, you must first enable OSPF on the router. Make a proper configuration plan to avoid incorrect settings that can result in route blocking and routing loops.

To configure OSPF, perform the following tasks:
<table>
<thead>
<tr>
<th>Tasks at a glance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>(Required.)</strong> Enabling OSPF</td>
</tr>
<tr>
<td><strong>(Optional.)</strong> Configuring OSPF areas:</td>
</tr>
<tr>
<td>• Configuring a stub area</td>
</tr>
<tr>
<td>• Configuring an NSSA area</td>
</tr>
<tr>
<td>• Configuring a virtual link</td>
</tr>
<tr>
<td><strong>(Optional.)</strong> Configuring OSPF network types:</td>
</tr>
<tr>
<td>• Configuring the broadcast network type for an interface</td>
</tr>
<tr>
<td>• Configuring the NBMA network type for an interface</td>
</tr>
<tr>
<td>• Configuring the P2MP network type for an interface</td>
</tr>
<tr>
<td>• Configuring the P2P network type for an interface</td>
</tr>
<tr>
<td><strong>(Optional.)</strong> Configuring OSPF route control:</td>
</tr>
<tr>
<td>• Configuring OSPF route summarization</td>
</tr>
<tr>
<td>o Configuring route summarization on an ABR</td>
</tr>
<tr>
<td>o Configuring route summarization on an ASBR</td>
</tr>
<tr>
<td>• Configuring received OSPF route filtering</td>
</tr>
<tr>
<td>• Configuring Type-3 LSA filtering</td>
</tr>
<tr>
<td>• Setting an OSPF cost for an interface</td>
</tr>
<tr>
<td>• Setting the maximum number of ECMP routes</td>
</tr>
<tr>
<td>• Setting OSPF preference</td>
</tr>
<tr>
<td>• Configuring discard routes for summary networks</td>
</tr>
<tr>
<td>• Configuring OSPF route redistribution</td>
</tr>
<tr>
<td>o Redistributing routes from another routing protocol</td>
</tr>
<tr>
<td>o Redistributing a default route</td>
</tr>
<tr>
<td>o Configuring default parameters for redistributed routes</td>
</tr>
<tr>
<td>• Advertising a host route</td>
</tr>
<tr>
<td><strong>(Optional.)</strong> Tuning and optimizing OSPF networks:</td>
</tr>
<tr>
<td>• Setting OSPF timers</td>
</tr>
<tr>
<td>• Setting LSA transmission delay</td>
</tr>
<tr>
<td>• Setting SPF calculation interval</td>
</tr>
<tr>
<td>• Setting the LSA arrival interval</td>
</tr>
<tr>
<td>• Setting the LSA generation interval</td>
</tr>
<tr>
<td>• Disabling interfaces from receiving and sending OSPF packets</td>
</tr>
<tr>
<td>• Configuring stub routers</td>
</tr>
<tr>
<td>• Configuring OSPF authentication</td>
</tr>
<tr>
<td>• Adding the interface MTU into DD packets</td>
</tr>
<tr>
<td>• Setting a DSCP value for OSPF packets</td>
</tr>
<tr>
<td>• Setting the maximum number of external LSAs in LSDB</td>
</tr>
<tr>
<td>• Setting OSPF exit overflow interval</td>
</tr>
<tr>
<td>• Enabling compatibility with RFC 1583</td>
</tr>
<tr>
<td>• Logging neighbor state changes</td>
</tr>
<tr>
<td>• Configuring OSPF network management</td>
</tr>
<tr>
<td>• Setting the LSU transmit rate</td>
</tr>
<tr>
<td>• Enabling OSPF ISPF</td>
</tr>
<tr>
<td>• Configuring prefix suppression</td>
</tr>
<tr>
<td>• Configuring prefix prioritization</td>
</tr>
</tbody>
</table>
## Tasks at a glance

- Configuring OSPF PIC
- Setting the number of OSPF logs
- Filtering outbound LSAs on an interface
- Filtering LSAs for the specified neighbor
- Configuring GTSM for OSPF

(Optional.) Configuring OSPF GR
- Configuring OSPF GR restarter
- Configuring OSPF GR helper
- Triggering OSPF GR

(Optional.) Configuring OSPF NSR

(Optional.) Configuring BFD for OSPF

(Optional.) Configuring OSPF FRR

---

## Enabling OSPF

Enable OSPF before you perform other OSPF configuration tasks.

### Configuration prerequisites

Configure the link layer protocol and IP addresses for interfaces to ensure IP connectivity between neighboring nodes.

### Configuration guidelines

To enable OSPF on an interface, you can enable OSPF on the network where the interface resides or directly enable OSPF on that interface. If you configure both, the latter takes precedence.

You can specify a global router ID, or specify a router ID when you create an OSPF process.

- If you specify a router ID when you create an OSPF process, any two routers in an AS must have different router IDs. A common practice is to specify the IP address of an interface as the router ID.
- If you specify no router ID when you create the OSPF process, the global router ID is used. As a best practice, specify a router ID when you create the OSPF process.

OSPF supports multiple processes and VPNs.

- To run multiple OSPF processes, you must specify an ID for each process. The process IDs take effect locally and have no influence on packet exchange between routers. Two routers with different process IDs can exchange packets.
- You can configure an OSPF process to run in a specified VPN instance. For more information about VPN, see *MPLS Configuration Guide*.

### Enabling OSPF on a network

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Step | Command | Remarks
--- | --- | ---
2. (Optional.) Configure a global router ID. | router id router-id | By default, no global router ID is configured. If no global router ID is configured, the highest loopback interface IP address, if any, is used as the router ID. If no loopback interface IP address is available, the highest physical interface IP address is used, regardless of the interface status (up or down).

3. Enable an OSPF process and enter OSPF view. | ospf [ process-id | router-id router-id | vpn-instance vpn-instance-name ] * | By default, OSPF is disabled.

4. (Optional.) Configure a description for the OSPF process. | description text | By default, no description is configured for the OSPF process. As a best practice, configure a description for each OSPF process.

5. Create an OSPF area and enter OSPF area view. | area area-id | By default, no OSPF areas exist.

6. (Optional.) Configure a description for the area. | description text | By default, no description is configured for the area. As a best practice, configure a description for each OSPF area.

7. Specify a network to enable the interface attached to the network to run the OSPF process in the area. | network ip-address wildcard-mask | By default, no network is specified. A network can be added to only one area.

---

### Enabling OSPF on an interface

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter interface view.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
</tbody>
</table>

3. Enable an OSPF process on the interface. | ospf process-id area area-id [ exclude-subip ] | By default, OSPF is disabled on an interface. If the specified OSPF process and area do not exist, the command creates the OSPF process and area. Disabling an OSPF process on an interface does not delete the OSPF process or the area.

---

### Configuring OSPF areas

Before you configure an OSPF area, perform the following tasks:

- Configure IP addresses for interfaces to ensure IP connectivity between neighboring nodes.
- Enable OSPF.
Configuring a stub area

You can configure a non-backbone area at an AS edge as a stub area. To do so, execute the stub command on all routers attached to the area. The routing table size is reduced because Type-5 LSAs will not be flooded within the stub area. The ABR generates a default route into the stub area so all packets destined outside of the AS are sent through the default route.

To further reduce the routing table size and routing information exchanged in the stub area, configure a totally stub area by using the stub no-summary command on the ABR. AS external routes and inter-area routes will not be distributed into the area. All the packets destined outside of the AS or area will be sent to the ABR for forwarding.

A stub or totally stub area cannot have an ASBR because external routes cannot be distributed into the area.

To configure an OSPF stub area:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>ospf [ process-id</td>
<td>router-id router-id ]</td>
</tr>
<tr>
<td>3.</td>
<td>area area-id</td>
<td>N/A</td>
</tr>
<tr>
<td>4.</td>
<td>stub [ default-route-advertise-always</td>
<td>no-summary ]</td>
</tr>
<tr>
<td>5.</td>
<td>default-cost cost-value</td>
<td>The default setting is 1. The default-cost cost command takes effect only on the ABR of a stub area or totally stub area.</td>
</tr>
</tbody>
</table>

Configuring an NSSA area

A stub area cannot import external routes, but an NSSA area can import external routes into the OSPF routing domain while retaining other stub area characteristics.

Do not configure the backbone area as an NSSA area or totally NSSA area.

To configure an NSSA area, configure the nssa command on all the routers attached to the area.

To configure a totally NSSA area, configure the nssa command on all the routers attached to the area and configure the nssa no-summary command on the ABR. The ABR of a totally NSSA area does not advertise inter-area routes into the area.

To configure an NSSA area:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>ospf [ process-id</td>
<td>router-id router-id ]</td>
</tr>
<tr>
<td>3.</td>
<td>area area-id</td>
<td>N/A</td>
</tr>
</tbody>
</table>
### Configuring a virtual link

Virtual links are configured for connecting backbone area routers that have no direct physical links.

To configure a virtual link:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>ospf [ process-id</td>
<td>router-id</td>
</tr>
<tr>
<td>3.</td>
<td>area area-id</td>
<td>N/A</td>
</tr>
<tr>
<td>4.</td>
<td>vlink-peer router-id [ dead seconds</td>
<td>hello seconds</td>
</tr>
</tbody>
</table>

### Configuring OSPF network types

OSPF classifies networks into the following types based on the link layer protocol:

- **Broadcast**—When the link layer protocol is Ethernet or FDDI, OSPF classifies the network type as broadcast by default.
- **NBMA**—When the link layer protocol is Frame Relay, ATM, or X.25, OSPF classifies the network type as NBMA by default.
- **P2P**—When the link layer protocol is PPP, LAPB, or HDLC, OSPF classifies the network type as P2P by default.

When you change the network type of an interface, follow these guidelines:

- When an NBMA network becomes fully meshed, change the network type to broadcast to avoid manual configuration of neighbors.
- If any routers in a broadcast network do not support multicasting, change the network type to NBMA.
• An NBMA network must be fully meshed. OSPF requires that an NBMA network be fully meshed. If a network is partially meshed, change the network type to P2MP.
• If a router on an NBMA network has only one neighbor, you can change the network type to P2P to save costs.

Two broadcast-, NBMA-, and P2MP-interfaces can establish a neighbor relationship only when they are on the same network segment.

Configuration prerequisites

Before you configure OSPF network types, perform the following tasks:
• Configure IP addresses for interfaces to ensure IP connectivity between neighboring nodes.
• Enable OSPF.

Configuring the broadcast network type for an interface

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter interface view.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3. Configure the OSPF network type for the interface as broadcast.</td>
<td>ospf network-type broadcast</td>
<td>By default, the network type of an interface depends on the link layer protocol.</td>
</tr>
<tr>
<td>4. (Optional.) Set a router priority for the interface.</td>
<td>ospf dr-priority priority</td>
<td>The default router priority is 1.</td>
</tr>
</tbody>
</table>

Configuring the NBMA network type for an interface

After you configure the network type as NBMA, you must specify neighbors and their router priorities because NBMA interfaces cannot find neighbors by broadcasting hello packets.

To configure the NBMA network type for an interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter interface view.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3. Configure the OSPF network type for the interface as NBMA.</td>
<td>ospf network-type nbma</td>
<td>By default, the network type of an interface depends on the link layer protocol.</td>
</tr>
<tr>
<td>4. (Optional.) Set a router priority for the interface.</td>
<td>ospf dr-priority priority</td>
<td>The default setting is 1. The router priority configured with this command is for DR election.</td>
</tr>
<tr>
<td>5. Return to system view.</td>
<td>quit</td>
<td>N/A</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>6.</td>
<td>Enter OSPF view. **`ospf [ process-id</td>
<td>router-id router-id</td>
</tr>
<tr>
<td>7.</td>
<td>Specify a neighbor and set its router priority. <strong><code>peer ip-address [ dr-priority priority ]</code></strong></td>
<td>By default, no neighbor is specified. The priority configured with this command indicates whether a neighbor has the election right or not. If you configure the router priority for a neighbor as 0, the local router determines the neighbor has no election right, and does not send hello packets to this neighbor. However, if the local router is the DR or BDR, it still sends hello packets to the neighbor for neighbor relationship establishment.</td>
</tr>
</tbody>
</table>

### Configuring the P2MP network type for an interface

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view. <strong><code>system-view</code></strong></td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view. <strong><code>interface interface-type interface-number</code></strong></td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the OSPF network type for the interface as P2MP. <strong><code>ospf network-type p2mp [ unicast ]</code></strong></td>
<td>By default, the network type of an interface depends on the link layer protocol. After you configure the OSPF network type for an interface as P2MP unicast, all packets are unicast over the interface. The interface cannot broadcast hello packets to discover neighbors, so you must manually specify the neighbors.</td>
</tr>
<tr>
<td>4.</td>
<td>Return to system view. <strong><code>quit</code></strong></td>
<td>N/A</td>
</tr>
<tr>
<td>5.</td>
<td>Enter OSPF view. **`ospf [ process-id</td>
<td>router-id router-id</td>
</tr>
<tr>
<td>6.</td>
<td>(Optional.) Specify a neighbor and set its router priority. <strong><code>peer ip-address [ cost cost-value ]</code></strong></td>
<td>By default, no neighbor is specified. This step must be performed if the network type is P2MP unicast, and is optional if the network type is P2MP.</td>
</tr>
</tbody>
</table>

### Configuring the P2P network type for an interface

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view. <strong><code>system-view</code></strong></td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view. <strong><code>interface interface-type interface-number</code></strong></td>
<td>N/A</td>
</tr>
</tbody>
</table>
Configuring OSPF route control

This section describes how to control the advertisement and reception of OSPF routing information, as well as route redistribution from other protocols.

Configuration prerequisites

Before you configure OSPF route control, perform the following tasks:

- Configure IP addresses for interfaces to ensure IP connectivity between neighboring nodes.
- Enable OSPF.
- Configure filters if routing information filtering is needed.

Configuring OSPF route summarization

Route summarization enables an ABR or ASBR to summarize contiguous networks into a single network and advertise the network to other areas.

Route summarization reduces the routing information exchanged between areas and the size of routing tables, and improves routing performance. For example, three internal networks 19.1.1.0/24, 19.1.2.0/24, and 19.1.3.0/24 are available within an area. You can summarize the three networks into network 19.1.0.0/16, and advertise the summary network to other areas.

Configuring route summarization on an ABR

After you configure a summary route on an ABR, the ABR generates a summary LSA instead of specific LSAs. The scale of LSDBs on routers in other areas and the influence of topology changes are reduced.

To configure route summarization on an ABR:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
</tbody>
</table>
| 2.   | ospf [ process-id | router-id
|      | router-id | vpn-instance
|      | vpn-instance-name ] * | N/A     |
| 3.   | area area-id | N/A     |
| 4.   | abr-summary ip-address
|      | ( mask-length | mask ) [ advertise | not-advertise ] | [ cost cost-value ] | By default, route summarization is not configured on an ABR. |

Configuring route summarization on an ASBR

Perform this task to enable an ASBR to summarize external routes within the specified address range into a single route. The ASBR advertises only the summary route to reduce the number of LSAs in the LSDB.

An ASBR can summarize routes in the following LSAs:

- Type-5 LSAs.
• Type-7 LSAs in an NSSA area.
• Type-5 LSAs translated by the ASBR (also an ABR) from Type-7 LSAs in an NSSA area.

If the ASBR (ABR) is not a translator, it cannot summarize routes in Type-5 LSAs translated from Type-7 LSAs.

To configure route summarization on an ASBR:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter OSPF view.</td>
<td>ospf [ process-id</td>
</tr>
<tr>
<td>3.</td>
<td>Configure ASBR route summarization.</td>
<td>asbr-summary ip-address { mask-length</td>
</tr>
</tbody>
</table>

Configuring received OSPF route filtering

Perform this task to filter routes calculated using received LSAs.

The following filtering methods are available:
• Use an ACL or IP prefix list to filter routing information by destination address.
• Use the gateway keyword to filter routing information by next hop.
• Use an ACL or IP prefix list to filter routing information by destination address. At the same time use the gateway keyword to filter routing information by next hop.
• Use a routing policy to filter routing information.

To configure OSPF to filter routes calculated using received LSAs:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter OSPF view.</td>
<td>ospf [ process-id</td>
</tr>
<tr>
<td>3.</td>
<td>Configure OSPF to filter routes calculated using received LSAs.</td>
<td>filter-policy { ipv4-acl-number</td>
</tr>
</tbody>
</table>

Configuring Type-3 LSA filtering

Perform this task to filter Type-3 LSAs advertised to an area on an ABR.

To configure Type-3 LSA filtering:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter OSPF view.</td>
<td>ospf [ process-id</td>
</tr>
</tbody>
</table>
### Setting an OSPF cost for an interface

Set an OSPF cost for an interface by using either of the following methods:

- Set the cost value in interface view.
- Set a bandwidth reference value for the interface. OSPF computes the cost with this formula:
  
  Interface OSPF cost = Bandwidth reference value (100 Mbps) / Expected interface bandwidth (Mbps).

  The expected bandwidth of an interface is configured with the `bandwidth` command (see [Interface Command Reference](#)).

  - If the calculated cost is greater than 65535, the value of 65535 is used. If the calculated cost is less than 1, the value of 1 is used.
  - If no cost or bandwidth reference value is configured for an interface, OSPF computes the interface cost based on the interface bandwidth and default bandwidth reference value.

To set an OSPF cost for an interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>ospf cost cost-value</td>
<td>By default, the OSPF cost is calculated according to the interface bandwidth. For a loopback interface, the OSPF cost is 0 by default.</td>
</tr>
</tbody>
</table>

To set a bandwidth reference value:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>ospf [ process-id</td>
<td>router-id router-id</td>
</tr>
<tr>
<td>3.</td>
<td>bandwidth-reference value</td>
<td>The default setting is 100 Mbps.</td>
</tr>
</tbody>
</table>

### Setting the maximum number of ECMP routes

Perform this task to implement load sharing over ECMP routes.

To set the maximum number of ECMP routes:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
</tbody>
</table>
### Setting OSPF preference

A router can run multiple routing protocols, and each protocol is assigned a preference. If multiple routes are available to the same destination, the one with the highest protocol preference is selected as the best route.

To set OSPF preference:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>ospf [ process-id</td>
<td>router-id router-id</td>
</tr>
<tr>
<td>3.</td>
<td>preference [ ase ] { preference</td>
<td>route-policy route-policy-name }</td>
</tr>
</tbody>
</table>

### Configuring discard routes for summary networks

Perform this task on an ABR or ASBR to specify whether to generate discard routes for summary networks. You can also specify a preference for the discard routes.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>ospf [ process-id</td>
<td>router-id router-id</td>
</tr>
</tbody>
</table>
| 3.   | discard-route { external { preference | suppression } | internal { preference | suppression } } | By default:  
• The ABR or ASBR generates discard routes for summary networks.  
• The preference of discard routes is 255. |

### Configuring OSPF route redistribution

On a router running OSPF and other routing protocols, you can configure OSPF to redistribute static routes, direct routes, or routes from other protocols, such as RIP, IS-IS, and BGP. OSPF advertises the routes in Type-5 LSAs or Type-7 LSAs. In addition, you can configure OSPF to filter redistributed routes so that OSPF advertises only permitted routes.
IMPORTANT:
The `import-route bgp` command redistributes only EBGP routes. Because the `import-route bgp allow-ibgp` command redistributes both EBGP and IBGP routes, and might cause routing loops, use it with caution.

**Redistributing routes from another routing protocol**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>2.</td>
<td>Enter OSPF view.</td>
<td>`ospf [ process-id</td>
</tr>
<tr>
<td>3.</td>
<td>Configure OSPF to redistribute routes from another routing protocol.</td>
<td>`import-route protocol [ as-number ] [ process-id</td>
</tr>
<tr>
<td>4.</td>
<td>(Optional.) Configure OSPF to filter redistributed routes.</td>
<td>`filter-policy { ipv4-acl-number</td>
</tr>
</tbody>
</table>

**Redistributing a default route**

The `import-route` command cannot redistribute a default external route. Perform this task to redistribute a default route.

To redistribute a default route:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>2.</td>
<td>Enter OSPF view.</td>
<td>`ospf [ process-id</td>
</tr>
<tr>
<td>3.</td>
<td>Redistribute a default route.</td>
<td>`default-route-advertise [ [ [ always</td>
</tr>
</tbody>
</table>

**Configuring default parameters for redistributed routes**

Perform this task to configure default parameters for redistributed routes, including cost, tag, and type. Tags identify information about protocols. For example, when redistributing BGP routes, OSPF uses tags to identify AS IDs.

To configure the default parameters for redistributed routes:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>2.</td>
<td>Enter OSPF view.</td>
<td>`ospf [ process-id</td>
</tr>
</tbody>
</table>
### Step Command Remarks

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td>Configure the default parameters for redistributed routes (cost, upper limit, tag, and type).</td>
<td>default { cost \ cost-value \ tag \ tag \ type \ type } *</td>
</tr>
<tr>
<td></td>
<td>By default, the cost is 1, the tag is 1, and the type is Type-2.</td>
<td></td>
</tr>
</tbody>
</table>

### Advertising a host route

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter OSPF view.</td>
<td>ospf [ process-id \ router-id \ router-id \ vpn-instance \ vpn-instance-name ] *</td>
</tr>
<tr>
<td>3.</td>
<td>Enter area view.</td>
<td>area area-id</td>
</tr>
<tr>
<td>4.</td>
<td>Advertise a host route.</td>
<td>host-advertise ip-address cost</td>
</tr>
</tbody>
</table>

### Tuning and optimizing OSPF networks

You can use one of the following methods to optimize an OSPF network:

- Change OSPF packet timers to adjust the convergence speed and network load. On low-speed links, consider the delay time for sending LSAs.
- Change the SPF calculation interval to reduce resource consumption caused by frequent network changes.
- Configure OSPF authentication to improve security.

### Configuration prerequisites

Before you configure OSPF network optimization, perform the following tasks:

- Configure IP addresses for interfaces to ensure IP connectivity between neighboring nodes.
- Enable OSPF.

### Setting OSPF timers

An OSPF interface includes the following timers:

- **Hello timer**—Interval for sending hello packets. It must be identical on OSPF neighbors.
- **Poll timer**—Interval for sending hello packets to a neighbor that is down on the NBMA network.
- **Dead timer**—Interval within which if the interface does not receive any hello packet from the neighbor, it declares the neighbor is down.
- **LSA retransmission timer**—Interval within which if the interface does not receive any acknowledgment packets after sending an LSA to the neighbor, it retransmits the LSA.

To set OSPF timers:
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
</tbody>
</table>
| 3.   | Set the hello interval. | ospf timer hello seconds | By default:  
- The hello interval on P2P and broadcast interfaces is 10 seconds.  
- The hello interval on P2MP and NBMA interfaces is 30 seconds.  
The default hello interval is restored when the network type for an interface is changed. |
| 4.   | Set the poll interval. | ospf timer poll seconds | The default setting is 120 seconds.  
The poll interval is a minimum of four times the hello interval. |
| 5.   | Set the dead interval. | ospf timer dead seconds | By default:  
- The dead interval on P2P and broadcast interfaces is 40 seconds.  
- The dead interval on P2MP and NBMA interfaces is 120 seconds.  
The dead interval must be a minimum of four times the hello interval on an interface.  
The default dead interval is restored when the network type for an interface is changed. |
| 6.   | Set the retransmission interval. | ospf timer retransmit interval | The default setting is 5 seconds.  
A retransmission interval setting that is too small can cause unnecessary LSA retransmissions. This interval is typically set bigger than the round-trip time of a packet between two neighbors. |

### Setting LSA transmission delay

To avoid LSAs from aging out during transmission, set an LSA retransmission delay especially for low speed links.

To set the LSA transmission delay on an interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Set the LSA transmission delay.</td>
<td>ospf trans-delay seconds</td>
</tr>
</tbody>
</table>
Setting SPF calculation interval

LSDB changes result in SPF calculations. When the topology changes frequently, a large amount of network and router resources are occupied by SPF calculation. You can adjust the SPF calculation interval to reduce the impact.

For a stable network, the minimum interval is used. If network changes become frequent, the SPF calculation interval is incremented by the incremental interval $\times 2^{n-2}$ for each calculation until the maximum interval is reached. The value $n$ is the number of calculation times.

To set the SPF calculation interval:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter OSPF view.</td>
<td>ospf [ process-id</td>
</tr>
</tbody>
</table>
  • The maximum interval is 5 seconds.  
  • The minimum interval is 50 milliseconds.  
  • The incremental interval is 200 milliseconds. |

Setting the LSA arrival interval

If OSPF receives an LSA that has the same LSA type, LS ID, and router ID as the previously received LSA within the LSA arrival interval, OSPF discards the LSA to save bandwidth and route resources.

To set the LSA arrival interval:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter OSPF view.</td>
<td>ospf [ process-id</td>
</tr>
</tbody>
</table>
| 3.   | Set the LSA arrival interval. | lsa-arrival-interval | interval | The default setting is 1000 milliseconds.  
Make sure this interval is smaller than or equal to the interval set with the lsa-generation-interval command. |

Setting the LSA generation interval

Adjust the LSA generation interval to protect network resources and routers from being overwhelmed by LSAs at the time of frequent network changes.

For a stable network, the minimum interval is used. If network changes become frequent, the LSA generation interval is incremented by the incremental interval $\times 2^{n-2}$ for each generation until the maximum interval is reached. The value $n$ is the number of generation times.

To set the LSA generation interval:
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter OSPF view.</td>
<td>ospf [ process-id</td>
</tr>
<tr>
<td>3.</td>
<td>Set the LSA generation interval.</td>
<td>lsa-generation-interval maximum-interval [ minimum-interval [ incremental-interval ] ]</td>
</tr>
</tbody>
</table>

### Disabling interfaces from receiving and sending OSPF packets

To enhance OSPF adaptability and reduce resource consumption, you can set an OSPF interface to "silent." A silent OSPF interface blocks OSPF packets and cannot establish any OSPF neighbor relationship. However, other interfaces on the router can still advertise direct routes of the interface in Router LSAs.

To disable interfaces from receiving and sending routing information:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter OSPF view.</td>
<td>ospf [ process-id</td>
</tr>
<tr>
<td>3.</td>
<td>Disable interfaces from receiving and sending OSPF packets.</td>
<td>silent-interface { interface-type interface-number</td>
</tr>
</tbody>
</table>

### Configuring stub routers

A stub router is used for traffic control. It reports its status as a stub router to neighboring OSPF routers. The neighboring routers can have a route to the stub router, but they do not use the stub router to forward data.

Router LSAs from the stub router might contain different link type values. A value of 3 means a link to a stub network, and the cost of the link will not be changed by default. To set the cost of the link to 65535, specify the include-stub keyword in the stub-router command. A value of 1, 2 or 4 means a point-to-point link, a link to a transit network, or a virtual link. On such links, a maximum cost value of 65535 is used. Neighbors do not send packets to the stub router as long as they have a route with a smaller cost.

To configure a router as a stub router:
### Configuring OSPF authentication

Perform this task to configure OSPF area and interface authentication.

OSPF adds the configured key into sent packets, and uses the key to authenticate received packets. Only packets that pass the authentication can be received. If a packet fails the authentication, the OSPF neighbor relationship cannot be established.

If you configure OSPF authentication for both an area and an interface in that area, the interface uses the OSPF authentication configured on it.

#### Configuring OSPF area authentication

You must configure the same authentication mode and key on all the routers in an area.

To configure OSPF area authentication:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>ospf [ process-id</td>
<td>router-id router-id</td>
</tr>
<tr>
<td>3.</td>
<td>area area-id</td>
<td>N/A</td>
</tr>
<tr>
<td>4.</td>
<td>• Configure MD5 authentication: authentication-mode { hmac-md5</td>
<td>md5 } key-id { cipher</td>
</tr>
</tbody>
</table>

#### Configuring OSPF interface authentication

You must configure the same authentication mode and key on both the local interface and its peer interface.

To configure OSPF interface authentication:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
</tbody>
</table>
3. Configure interface authentication mode.

- Configure simple authentication:
  `ospf authentication-mode simple cipher [plain] string`
- Configure MD5 authentication:
  `ospf authentication-mode hmac-md5 [md5] key-id [cipher | plain] string`
- Configure keychain authentication:
  `ospf authentication-mode keychain keychain-name`

By default, no authentication is configured. For information about keychain, see Security Configuration Guide.

### Adding the interface MTU into DD packets

By default, an OSPF interface adds a value of 0 into the interface MTU field of a DD packet rather than the actual interface MTU. You can enable an interface to add its MTU into DD packets.

To add the interface MTU into DD packets:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>ospf mtu-enable</td>
<td>By default, the interface adds an MTU value of 0 into DD packets.</td>
</tr>
</tbody>
</table>

### Setting a DSCP value for OSPF packets

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>ospf [process-id</td>
<td>router-id</td>
</tr>
<tr>
<td>3.</td>
<td>dscp dscp-value</td>
<td>By default, the DSCP value for OSPF packets is 48.</td>
</tr>
</tbody>
</table>

### Setting the maximum number of external LSAs in LSDB

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>ospf [process-id</td>
<td>router-id</td>
</tr>
<tr>
<td>3.</td>
<td>lsdb-overflow-limit number</td>
<td>By default, the maximum number of external LSAs in the LSDB is not limited.</td>
</tr>
</tbody>
</table>
Setting OSPF exit overflow interval

When the number of LSAs in the LSDB exceeds the upper limit, the LSDB is in an overflow state. To save resources, OSPF does not receive any external LSAs and deletes the external LSAs generated by itself when in this state.

Perform this task to configure the interval that OSPF exits overflow state.

To set the OSPF exit overflow interval:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter OSPF view.</td>
<td>ospf [ process-id</td>
</tr>
<tr>
<td>3.</td>
<td>Set the OSPF exit overflow interval.</td>
<td>lsdb-overflow-interval interval</td>
</tr>
</tbody>
</table>

Enabling compatibility with RFC 1583

RFC 1583 specifies a different method than RFC 2328 for selecting the optimal route to a destination in another AS. When multiple routes are available to the ASBR, OSPF selects the optimal route by using the following procedure:

1. Selects the route with the highest preference.
   - If RFC 2328 is compatible with RFC 1583, all these routes have equal preference.
   - If RFC 2328 is not compatible with RFC 1583, the intra-area route in a non-backbone area is preferred to reduce the burden of the backbone area. The inter-area route and intra-area route in the backbone area have equal preference.

2. Selects the route with the lower cost if two routes have equal preference.

3. Selects the route with the larger originating area ID if two routes have equal cost.

To avoid routing loops, set identical RFC 1583-compatibility on all routers in a routing domain.

To enable compatibility with RFC 1583:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter OSPF view.</td>
<td>ospf [ process-id</td>
</tr>
<tr>
<td>3.</td>
<td>Enable compatibility with RFC 1583.</td>
<td>rfc1583 compatible</td>
</tr>
</tbody>
</table>

Logging neighbor state changes

Perform this task to enable output of neighbor state change logs to the information center. The information center processes the logs according to user-defined output rules (whether and where to output logs). For more information about the information center, see Network Management and Monitoring Configuration Guide.

To enable the logging of neighbor state changes:
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter OSPF view.</td>
<td>ospf [ process-id</td>
</tr>
<tr>
<td>3.</td>
<td>Enable the logging of neighbor state changes.</td>
<td>log-peer-change</td>
</tr>
</tbody>
</table>

### Configuring OSPF network management

This task involves the following configurations:

- Bind an OSPF process to MIB so that you can use network management software to manage the specified OSPF process.
- Enable SNMP notifications for OSPF to report important events.
- Configure the SNMP notification output interval and the maximum number of SNMP notifications that can be output at each interval.

To report critical OSPF events to an NMS, enable SNMP notifications for OSPF. For SNMP notifications to be sent correctly, you must also configure SNMP on the device. For more information about SNMP configuration, see the network management and monitoring configuration guide for the device.

To configure OSPF network management:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Bind an OSPF process to MIB.</td>
<td>ospf mib-binding process-id</td>
</tr>
<tr>
<td>4.</td>
<td>Enter OSPF view.</td>
<td>ospf [ process-id</td>
</tr>
<tr>
<td>5.</td>
<td>Configure the SNMP notification output interval and the maximum number of SNMP notifications that can be output at each interval.</td>
<td>snmp trap rate-limit interval trap-interval count trap-number</td>
</tr>
</tbody>
</table>
Setting the LSU transmit rate

Sending large numbers of LSU packets affects router performance and consumes a large amount of network bandwidth. You can configure the router to send LSU packets at an interval and to limit the maximum number of LSU packets sent out of an OSPF interface at each interval.

To set the LSU transmit rate:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter OSPF view.</td>
<td>ospf [ process-id</td>
</tr>
<tr>
<td>3.</td>
<td>Set the LSU transmit rate.</td>
<td>transmit-pacing interval interval count count</td>
</tr>
</tbody>
</table>

Enabling OSPF ISPF

When the topology changes, Incremental Shortest Path First (ISPF) computes only the affected part of the SPT, instead of the entire SPT.

To enable OSPF ISPF:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter OSPF view.</td>
<td>ospf [ process-id</td>
</tr>
<tr>
<td>3.</td>
<td>Enable OSPF ISPF.</td>
<td>ispf enable</td>
</tr>
</tbody>
</table>

Configuring prefix suppression

By default, an OSPF interface advertises all of its prefixes in LSAs. To speed up OSPF convergence, you can suppress interfaces from advertising all of their prefixes. This feature helps improve network security by preventing IP routing to the suppressed networks.

When prefix suppression is enabled:

- On P2P and P2MP networks, OSPF does not advertise Type-3 links in Type-1 LSAs. Other routing information can still be advertised to ensure traffic forwarding.
- On broadcast and NBMA networks, the DR generates Type-2 LSAs with a mask length of 32 to suppress network routes. Other routing information can still be advertised to ensure traffic forwarding. If no neighbors exist, the DR does not advertise the primary IP addresses of interfaces in Type-1 LSAs.

**IMPORTANT:**

As a best practice, configure prefix suppression on all OSPF routers if you want to use prefix suppression.
**Configuring prefix suppression for an OSPF process**

Enabling prefix suppression for an OSPF process does not suppress the prefixes of secondary IP addresses, loopback interfaces, and passive interfaces. To suppress the prefixes of loopback interfaces and passive interfaces, enable prefix suppression on the interfaces.

To configure prefix suppression for an OSPF process:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter OSPF view.</td>
<td>ospf { process-id</td>
</tr>
<tr>
<td>3.</td>
<td>Enable prefix suppression for the OSPF process.</td>
<td>prefix-suppression</td>
</tr>
</tbody>
</table>

**Configuring prefix suppression for an interface**

Interface prefix suppression does not suppress prefixes of secondary IP addresses.

To configure interface prefix suppression:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Enable prefix suppression for the interface.</td>
<td>ospf prefix-suppression [ disable ]</td>
</tr>
</tbody>
</table>

**Configuring prefix prioritization**

This feature enables the device to install prefixes in descending priority order: critical, high, medium, and low. The prefix priorities are assigned through routing policies. When a route is assigned multiple prefix priorities, the route uses the highest priority.

By default, the 32-bit OSPF host routes have a medium priority and other routes a low priority.

To configure prefix prioritization:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter OSPF view.</td>
<td>ospf { process-id</td>
</tr>
<tr>
<td>3.</td>
<td>Enable prefix prioritization.</td>
<td>prefix-priority route-policy route-policy-name</td>
</tr>
</tbody>
</table>

**Configuring OSPF PIC**

Prefix Independent Convergence (PIC) enables the device to speed up network convergence by ignoring the number of prefixes.

When both OSPF PIC and OSPF FRR are configured, OSPF FRR takes effect.
OSPF PIC applies only to inter-area routes and external routes.

### Enabling OSPF PIC

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter OSPF view.</td>
<td>ospf [ process-id</td>
</tr>
<tr>
<td>3.</td>
<td>Enable PIC for OSPF.</td>
<td>pic [ additional-path-always ]</td>
</tr>
</tbody>
</table>

### Configuring BFD for OSPF PIC

By default, OSPF PIC does not use BFD to detect primary link failures. To speed up OSPF convergence, enable BFD for OSPF PIC to detect the primary link failures.

To configure BFD control packet mode for OSPF PIC:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Enable BFD control packet mode for OSPF PIC.</td>
<td>ospf primary-path-detect bfd ctrl</td>
</tr>
</tbody>
</table>

To configure BFD echo packet mode for OSPF PIC:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure the source IP address of BFD echo packets.</td>
<td>bfd echo-source-ip ip-address</td>
</tr>
<tr>
<td>3.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>4.</td>
<td>Enable BFD echo packet mode for OSPF PIC.</td>
<td>ospf primary-path-detect bfd echo</td>
</tr>
</tbody>
</table>

### Setting the number of OSPF logs

OSPF logs include LSA aging logs, route calculation logs, and neighbor logs.

To set the number of OSPF logs:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
</tbody>
</table>
## Filtering outbound LSAs on an interface

To reduce the LSDB size for the neighbor and save bandwidth, you can perform this task on an interface to filter LSAs to be sent to the neighbor.

To filter outbound LSAs on an interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>ospf database-filter { all</td>
<td>{ ase [ acl ipv4-acl-number ]</td>
</tr>
</tbody>
</table>

## Filtering LSAs for the specified neighbor

On an P2MP network, a router might have multiple OSPF neighbors with the P2MP type. Perform this task to prevent the router from sending LSAs to the specified neighbor.

To filter LSAs for the specified neighbor:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>ospf [ process-id</td>
<td>router-id router-id</td>
</tr>
<tr>
<td>3.</td>
<td>database-filter peer ip-address { all</td>
<td>{ ase [ acl ipv4-acl-number ]</td>
</tr>
</tbody>
</table>

## Configuring GTSM for OSPF

The Generalized TTL Security Mechanism (GTSM) protects the device by comparing the TTL value in the IP header of incoming OSPF packets against a valid TTL range. If the TTL value is within the valid TTL range, the packet is accepted. If not, the packet is discarded.

The valid TTL range is from 255 – the configured hop count + 1 to 255.

When GTSM is configured, the OSPF packets sent by the device have a TTL of 255.
GTSM checks OSPF packets from common neighbors and virtual link neighbors. It does not check OSPF packets from sham link neighbors. For information about GTSM for OSPF sham links, see MPLS Configuration Guide.

You can configure GTSM in OSPF area view or interface view.

- The configuration in OSPF area view applies to all OSPF interfaces in the area.
- The configuration in interface view takes precedence over OSPF area view.

**IMPORTANT:**
To use GTSM, you must configure GTSM on both the local and peer devices. You can specify different hop-count values for them.

To configure GTSM in OSPF area view:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter OSPF view.</td>
<td>`ospf [ process-id</td>
<td>router-id</td>
</tr>
<tr>
<td>3. Enter OSPF area view.</td>
<td><code>area area-id</code></td>
<td>N/A</td>
</tr>
<tr>
<td>4. Enable GTSM for the OSPF area.</td>
<td><code>ttl-security [ hops hop-count ]</code></td>
<td>By default, GTSM is disabled for the OSPF area.</td>
</tr>
</tbody>
</table>

To configure GTSM in interface view:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter interface view.</td>
<td><code>interface interface-type interface-number</code></td>
<td>N/A</td>
</tr>
<tr>
<td>3. Enable GTSM for the interface.</td>
<td>`ospf ttl-security [ hops hop-count</td>
<td>disable ]`</td>
</tr>
</tbody>
</table>

**Configuring OSPF GR**

GR ensures forwarding continuity when a routing protocol restarts or an active/standby switchover occurs.

Two routers are required to complete a GR process. The following are router roles in a GR process:

- **GR restarter**—Graceful restarting router. It must have GR capability.
- **GR helper**—A neighbor of the GR restarter. It helps the GR restarter to complete the GR process.

OSPF GR has the following types:

- **IETF GR**—Uses Opaque LSAs to implement GR.
- **Non-IETF GR**—Uses link local signaling (LLS) to advertise GR capability and uses out of band synchronization to synchronize the LSDB.

A device can act as a GR restarter and GR helper at the same time.
Configuring OSPF GR restarter

You can configure the IETF or non-IETF OSPF GR restarter.

**IMPORTANT:**
You cannot enable OSPF NSR on a device that acts as GR restarter.

### Configuring the IETF OSPF GR restarter

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>ospf [ process-id</td>
<td>router-id</td>
</tr>
<tr>
<td>3.</td>
<td>opaque-capability enable</td>
<td>By default, opaque LSA reception and advertisement capability is enabled.</td>
</tr>
<tr>
<td>4.</td>
<td>graceful-restart ietf [ global</td>
<td>planned-only ] *</td>
</tr>
<tr>
<td>5.</td>
<td>graceful-restart interval interval</td>
<td>By default, the GR interval is 120 seconds.</td>
</tr>
</tbody>
</table>

### Configuring the non-IETF OSPF GR restarter

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>ospf [ process-id</td>
<td>router-id</td>
</tr>
<tr>
<td>3.</td>
<td>enable link-local-signaling</td>
<td>By default, the link-local signaling capability is disabled.</td>
</tr>
<tr>
<td>4.</td>
<td>enable out-of-band re-synchronization</td>
<td>By default, the out-of-band re-synchronization capability is disabled.</td>
</tr>
<tr>
<td>5.</td>
<td>graceful-restart [ nonstandard</td>
<td>[ global</td>
</tr>
<tr>
<td>6.</td>
<td>graceful-restart interval interval</td>
<td>By default, the GR interval is 120 seconds.</td>
</tr>
</tbody>
</table>

### Configuring OSPF GR helper

You can configure the IETF or non-IETF OSPF GR helper.

### Configuring the IETF OSPF GR helper

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>ospf [ process-id</td>
<td>router-id</td>
</tr>
</tbody>
</table>
### Configuring the non-IETF OSPF GR helper

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>ospf [ process-id</td>
<td>router-id router-id</td>
</tr>
<tr>
<td>3.</td>
<td>enable link-local-signaling</td>
<td>By default, the link-local signaling capability is disabled.</td>
</tr>
<tr>
<td>4.</td>
<td>enable out-of-band re-synchronization capability.</td>
<td>By default, the out-of-band re-synchronization capability is disabled.</td>
</tr>
<tr>
<td>5.</td>
<td>graceful-restart helper enable</td>
<td>By default, GR helper is enabled.</td>
</tr>
<tr>
<td>6.</td>
<td>graceful-restart helper strict-lsa-checking</td>
<td>By default, strict LSA checking for the GR helper is disabled.</td>
</tr>
</tbody>
</table>

### Triggering OSPF GR

OSPF GR is triggered by an active/standby switchover or when the following command is executed.

To trigger OSPF GR, perform the following command in user view:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trigger OSPF GR.</td>
<td>reset ospf [ process-id ] process graceful-restart</td>
</tr>
</tbody>
</table>

### Configuring OSPF NSR

The following matrix shows the feature and hardware compatibility:

<table>
<thead>
<tr>
<th>Hardware</th>
<th>OSPF NSR compatibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSR954(JH296A/JH297A/JH298A/JH299A/JH373A)</td>
<td>No</td>
</tr>
<tr>
<td>MSR958(JH300A/JH301A)</td>
<td>No</td>
</tr>
<tr>
<td>MSR1002-4/1003-8S</td>
<td>No</td>
</tr>
</tbody>
</table>
| MSR2003           | • In standalone mode: No  
                     • In IRF mode: Yes   |
| MSR2004-24/2004-48 | • In standalone mode: No  
                      • In IRF mode: Yes   |
Nonstop routing (NSR) backs up OSPF link state information from the active process to the standby process. After an active/standby switchover, NSR can complete link state recovery and route regeneration without tearing down adjacencies or impacting forwarding services.

NSR does not require the cooperation of neighboring devices to recover routing information, and it is typically used more often than GR.

**IMPORTANT:**
A device that has OSPF NSR enabled cannot act as GR restarter.

To enable OSPF NSR:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view. system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter OSPF view. ospf [ process-id</td>
<td>router-id router-id</td>
</tr>
<tr>
<td>3.</td>
<td>Enable OSPF NSR. non-stop-routing</td>
<td>By default, OSPF NSR is disabled. This command takes effect only for the current process. As a best practice, enable OSPF NSR for each process if multiple OSPF processes exist.</td>
</tr>
</tbody>
</table>

### Configuring BFD for OSPF

BFD provides a single mechanism to quickly detect and monitor the connectivity of links between OSPF neighbors, which improves the network convergence speed. For more information about BFD, see High Availability Configuration Guide.

OSPF supports the following BFD detection modes:

- **Bidirectional control detection**—Requires BFD configuration to be made on both OSPF routers on the link.
- **Single-hop echo detection**—Requires BFD configuration to be made on one OSPF router on the link.

#### Configuring bidirectional control detection

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view. system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view. interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>Enable BFD bidirectional control detection. ospf bfd enable</td>
<td>By default, BFD bidirectional control detection is disabled. Both ends of a BFD session must be</td>
</tr>
</tbody>
</table>
Configuring single-hop echo detection

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure the source address of echo packets.</td>
<td>bfd echo-source-ip ip-address</td>
</tr>
<tr>
<td>3.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>4.</td>
<td>Enable BFD single-hop echo detection.</td>
<td>ospf bfd enable echo</td>
</tr>
</tbody>
</table>

Configuring OSPF FRR

A link or router failure on a path can cause packet loss and even routing loop until OSPF completes routing convergence based on the new network topology. FRR enables fast rerouting to minimize the impact of link or node failures.

Figure 23 Network diagram for OSPF FRR

As shown in Figure 23, configure FRR on Router B by using a routing policy to specify a backup next hop. When the primary link fails, OSPF directs packets to the backup next hop. At the same time, OSPF calculates the shortest path based on the new network topology. It forwards packets over the path after network convergence.

You can configure OSPF FRR to calculate a backup next hop by using the loop free alternate (LFA) algorithm, or specify a backup next hop by using a routing policy.

Configuration prerequisites

Before you configure OSPF FRR, perform the following tasks:

- Configure IP addresses for interfaces to ensure IP connectivity between neighboring nodes.
- Enable OSPF.

Configuration guidelines

- Do not use the fast-reroute lfa command together with the vlink-peer command.
- When both OSPF PIC and OSPF FRR are configured, OSPF FRR takes effect.
Configuration procedure

Configuring OSPF FRR to calculate a backup next hop using the LFA algorithm

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>(Optional.) Enable LFA on an</td>
<td>ospf fast-reroute lfa-backup</td>
</tr>
<tr>
<td></td>
<td>interface.</td>
<td>By default, the interface is enabled with LFA and it can be selected as</td>
</tr>
<tr>
<td></td>
<td></td>
<td>a backup interface.</td>
</tr>
<tr>
<td>4.</td>
<td>Return to system view.</td>
<td>quit</td>
</tr>
<tr>
<td>5.</td>
<td>Enter OSPF view.</td>
<td>ospf [ process-id</td>
</tr>
<tr>
<td>6.</td>
<td>Enable OSPF FRR to</td>
<td>fast-reroute lfa [ abr-only ]</td>
</tr>
<tr>
<td></td>
<td>calculate a backup next hop</td>
<td>By default, OSPF FRR is disabled. If abr-only is specified, the route</td>
</tr>
<tr>
<td></td>
<td>by using the LFA algorithm.</td>
<td>to the ABR is selected as the backup path.</td>
</tr>
</tbody>
</table>

Configuring OSPF FRR to specify a backup next hop using a routing policy

Before you configure this task, use the **apply fast-reroute backup-interface** command to specify a backup next hop in the routing policy to be used. For more information about the **apply fast-reroute backup-interface** command and routing policy configuration, see "Configuring routing policies."

To configure OSPF FRR to specify a backup next hop using a routing policy:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter OSPF view.</td>
<td>ospf [ process-id</td>
</tr>
<tr>
<td>3.</td>
<td>Enable OSPF FRR to</td>
<td>fast-reroute route-policy</td>
</tr>
<tr>
<td></td>
<td>specify a backup next hop</td>
<td>route-policy-name</td>
</tr>
<tr>
<td></td>
<td>by using a routing policy.</td>
<td>By default, OSPF FRR is disabled.</td>
</tr>
</tbody>
</table>

Configuring BFD for OSPF FRR

By default, OSPF FRR does not use BFD to detect primary link failures. To speed up OSPF convergence, enable BFD for OSPF FRR to detect primary link failures.

To configure BFD control packet mode for OSPF FRR:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Enable BFD control packet</td>
<td>ospf primary-path-detect bfd ctrl</td>
</tr>
<tr>
<td></td>
<td>mode for OSPF FRR.</td>
<td>By default, BFD control packet mode for OSPF FRR is disabled.</td>
</tr>
</tbody>
</table>

To configure BFD echo packet mode for OSPF FRR:
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Configure the source IP address of BFD echo packets.</td>
<td>bfd echo-source-ip ip-address</td>
<td>By default, the source IP address of BFD echo packets is not configured. The source IP address cannot be on the same network segment as any local interface’s IP address. For more information about this command, see High Availability Command Reference.</td>
</tr>
<tr>
<td>3. Enter interface view.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>4. Enable BFD echo packet mode for OSPF FRR.</td>
<td>ospf primary-path-detect bfd echo</td>
<td>By default, BFD echo packet mode for OSPF FRR is disabled.</td>
</tr>
</tbody>
</table>

Displaying and maintaining OSPF

Execute `display` commands in any view and `reset` commands in user view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display OSPF process information.</td>
<td><code>display ospf [process-id] [verbose]</code></td>
</tr>
<tr>
<td>Display OSPF GR information.</td>
<td><code>display ospf [process-id] graceful-restart [verbose]</code></td>
</tr>
<tr>
<td>Display OSPF FRR backup next hop information.</td>
<td><code>display ospf [process-id] [area area-id] fast-reroute lfa-candidate</code></td>
</tr>
<tr>
<td>Display OSPF LSDB information.</td>
<td>`display ospf [process-id] lsdb [brief</td>
</tr>
<tr>
<td></td>
<td>`display ospf [process-id] lsdb [opaque-as</td>
</tr>
<tr>
<td></td>
<td>`display ospf [process-id] lsdb [asbr</td>
</tr>
<tr>
<td></td>
<td>`display ospf [process-id] [area area-id] lsdb [link-state-id] [originator-router advertising-router-id</td>
</tr>
<tr>
<td>Display OSPF next hop information.</td>
<td><code>display ospf [process-id] nexthop</code></td>
</tr>
<tr>
<td>Display OSPF NSR information.</td>
<td><code>display ospf [process-id] non-stop-routing status</code></td>
</tr>
<tr>
<td>Display OSPF neighbor information.</td>
<td><code>display ospf [process-id] peer [verbose] [interface-type interface-number] [neighbor-id]</code></td>
</tr>
<tr>
<td>Display neighbor statistics for OSPF areas.</td>
<td><code>display ospf [process-id] peer statistics</code></td>
</tr>
<tr>
<td>Display OSPF routing table information.</td>
<td>`display ospf [process-id] routing [ip-address {mask-length</td>
</tr>
<tr>
<td>Display OSPF topology information.</td>
<td><code>display ospf [process-id] [area area-id] spf-tree [verbose]</code></td>
</tr>
<tr>
<td>Display OSPF statistics.</td>
<td>`display ospf [process-id] statistics [error</td>
</tr>
<tr>
<td>Display OSPF virtual link information.</td>
<td><code>display ospf [process-id] vlink</code></td>
</tr>
</tbody>
</table>
### Task Command

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display OSPF request queue information.</td>
<td>display ospf [ process-id ] request-queue [ interface-type interface-number ] [ neighbor-id ]</td>
</tr>
<tr>
<td>Display OSPF retransmission queue information.</td>
<td>display ospf [ process-id ] retrans-queue [ interface-type interface-number ] [ neighbor-id ]</td>
</tr>
<tr>
<td>Display OSPF ABR and ASBR information.</td>
<td>display ospf [ process-id ] abr-asbr [ verbose ]</td>
</tr>
<tr>
<td>Display summary route information on the OSPF ABR.</td>
<td>display ospf [ process-id ] [ area area-id ] abr-summary [ ip-address { mask-length</td>
</tr>
<tr>
<td>Display OSPF interface information.</td>
<td>display ospf [ process-id ] interface [ interface-type interface-number ] [ verbose ]</td>
</tr>
<tr>
<td>Display OSPF log information.</td>
<td>display ospf [ process-id ] event-log { lsa-flush</td>
</tr>
<tr>
<td>Display OSPF ASBR route summarization information.</td>
<td>display ospf [ process-id ] asbr-summary [ ip-address { mask-length</td>
</tr>
<tr>
<td>Display the global route ID.</td>
<td>display router id</td>
</tr>
<tr>
<td>Clear OSPF statistics.</td>
<td>reset ospf [ process-id ] statistics</td>
</tr>
<tr>
<td>Clear OSPF log information.</td>
<td>reset ospf [ process-id ] event-log { lsa-flush</td>
</tr>
<tr>
<td>Restart an OSPF process.</td>
<td>reset ospf [ process-id ] process [ graceful-restart ]</td>
</tr>
<tr>
<td>Re-enable OSPF route redistribution.</td>
<td>reset ospf [ process-id ] redistribution</td>
</tr>
</tbody>
</table>

### NOTE:

Support for the `display ospf non-stop-routing status` command depends on the device model. For more information, see *Layer 3—IP Routing Command Reference*.

### OSPF configuration examples

#### Basic OSPF configuration example

**Network requirements**

As shown in Figure 24:

- Enable OSPF on all routers, and split the AS into three areas.
- Configure Router A and Router B as ABRs.
Figure 24 Network diagram

Configuration procedure

1. Configure IP addresses for interfaces. (Details not shown.)
2. Enable OSPF:

# Configure Router A.

```
<RouterA> system-view
[RouterA] router id 10.2.1.1
[RouterA] ospf
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] area 1
[RouterA-ospf-1-area-0.0.0.1] network 10.2.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.1] quit
[RouterA-ospf-1] quit
```

# Configure Router B.

```
<RouterB> system-view
[RouterB] router id 10.3.1.1
[RouterB] ospf
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 10.3.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
```

# Configure Router C.

```
<RouterC> system-view
[RouterC] router id 10.4.1.1
[RouterC] ospf
[RouterC-ospf-1] area 1
[RouterC-ospf-1-area-0.0.0.1] network 10.2.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.1] network 10.4.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.1] quit
```

# Configure Router D.
Verifying the configuration

# Display the OSPF neighbors of Router A.

[RouterA] display ospf peer verbose

OSPF Process 1 with Router ID 10.2.1.1
Neighbors

Area 0.0.0.0 interface 10.1.1.1(GigabitEthernet1/0/1)'s neighbors
Router ID: 10.3.1.1 Address: 10.1.1.2 GR State: Normal
State: Full Mode: Nbr is master Priority: 1
DR: 10.1.1.1 BDR: 10.1.1.2 MTU: 0
Options is 0x02 (-|-|-|-|-|E|-)
Dead timer due in 37 sec
Neighbor is up for 06:03:59
Authentication Sequence: [ 0 ]
Neighbor state change count: 5
BFD status: Disabled

Area 0.0.0.1 interface 10.2.1.1(GigabitEthernet1/0/2)'s neighbors
Router ID: 10.4.1.1 Address: 10.2.1.2 GR State: Normal
State: Full Mode: Nbr is master Priority: 1
DR: 10.2.1.1 BDR: 10.2.1.2 MTU: 0
Options is 0x02 (-|-|-|-|-|E|-)
Dead timer due in 32 sec
Neighbor is up for 06:03:12
Authentication Sequence: [ 0 ]
Neighbor state change count: 5
BFD status: Disabled

# Display OSPF routing information on Router A.

[RouterA] display ospf routing

OSPF Process 1 with Router ID 10.2.1.1
Routing Table

<table>
<thead>
<tr>
<th>Destination</th>
<th>Cost</th>
<th>Type</th>
<th>NextHop</th>
<th>AdvRouter</th>
<th>Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.2.1.0/24</td>
<td>1</td>
<td>Transit</td>
<td>0.0.0.0</td>
<td>10.2.1.1</td>
<td>0.0.0.1</td>
</tr>
<tr>
<td>10.3.1.0/24</td>
<td>2</td>
<td>Inter</td>
<td>10.1.1.2</td>
<td>10.3.1.1</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>10.4.1.0/24</td>
<td>2</td>
<td>Stub</td>
<td>10.2.1.2</td>
<td>10.4.1.1</td>
<td>0.0.0.1</td>
</tr>
<tr>
<td>10.5.1.0/24</td>
<td>3</td>
<td>Inter</td>
<td>10.1.1.2</td>
<td>10.3.1.1</td>
<td>0.0.0.0</td>
</tr>
</tbody>
</table>
OSPF route redistribution configuration example

Network requirements

As shown in Figure 25:

- Enable OSPF on all the routers.
- Split the AS into three areas.
- Configure Router A and Router B as ABRs.
- Configure Router C as an ASBR to redistribute external routes (static routes).
Configuration procedure

1. Configure IP addresses for interfaces. (Details not shown.)
2. Enable OSPF (see "Basic OSPF configuration example").
3. Configure OSPF to redistribute routes:
   
   # On Router C, configure a static route destined for network 3.1.2.0/24.
   <RouterC> system-view
   [RouterC] ip route-static 3.1.2.1 24 10.4.1.2
   
   # On Router C, configure OSPF to redistribute the static route.
   [RouterC] ospf 1
   [RouterC-ospf-1] import-route static

Verifying the configuration

# Display the ABR/ASBR information on Router D.
<RouterD> display ospf abr-asbr

OSPF Process 1 with Router ID 10.5.1.1
Routing Table to ABR and ASBR

<table>
<thead>
<tr>
<th>Type</th>
<th>Destination</th>
<th>Area</th>
<th>Cost</th>
<th>Nexthop</th>
<th>RtType</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intra</td>
<td>10.3.1.1</td>
<td>0.0.0.2</td>
<td>10</td>
<td>10.3.1.1</td>
<td>ABR</td>
</tr>
<tr>
<td>Inter</td>
<td>10.4.1.1</td>
<td>0.0.0.2</td>
<td>22</td>
<td>10.3.1.1</td>
<td>ASBR</td>
</tr>
</tbody>
</table>

# Display the OSPF routing information on Router D.
<RouterD> display ospf routing

OSPF Process 1 with Router ID 10.5.1.1
Routing Table

<table>
<thead>
<tr>
<th>Destination</th>
<th>Cost</th>
<th>Type</th>
<th>NextHop</th>
<th>AdvRouter</th>
<th>Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.2.1.0/24</td>
<td>22</td>
<td>Inter</td>
<td>10.3.1.1</td>
<td>10.3.1.1</td>
<td>0.0.0.2</td>
</tr>
<tr>
<td>10.3.1.0/24</td>
<td>10</td>
<td>Transit</td>
<td>0.0.0.0</td>
<td>10.3.1.1</td>
<td>0.0.0.2</td>
</tr>
<tr>
<td>10.4.1.0/24</td>
<td>25</td>
<td>Inter</td>
<td>10.3.1.1</td>
<td>10.3.1.1</td>
<td>0.0.0.2</td>
</tr>
<tr>
<td>10.5.1.0/24</td>
<td>10</td>
<td>Stub</td>
<td>0.0.0.0</td>
<td>10.5.1.1</td>
<td>0.0.0.2</td>
</tr>
<tr>
<td>10.1.1.0/24</td>
<td>12</td>
<td>Inter</td>
<td>10.3.1.1</td>
<td>10.3.1.1</td>
<td>0.0.0.2</td>
</tr>
</tbody>
</table>
Routing for ASEs

<table>
<thead>
<tr>
<th>Destination</th>
<th>Cost</th>
<th>Type</th>
<th>Tag</th>
<th>NextHop</th>
<th>AdvRouter</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.2.0/24</td>
<td>1</td>
<td>Type2</td>
<td>1</td>
<td>10.3.1.1</td>
<td>10.4.1.1</td>
</tr>
</tbody>
</table>

Total nets: 6
Intra area: 2  Inter area: 3  ASE: 1  NSSA: 0

**OSPF route summarization configuration example**

**Network requirements**

As shown in Figure 26:
- Configure OSPF on Router A and Router B in AS 200.
- Configure OSPF on Router C, Router D, and Router E in AS 100.
- Configure an EBGP connection between Router B and Router C. Configure Router B and Router C to redistribute OSPF routes and direct routes into BGP and BGP routes into OSPF.
- Configure Router B to advertise only summary route 10.0.0.0/8 to Router A.

**Figure 26 Network diagram**

**Configuration procedure**

1. Configure IP addresses for interfaces. (Details not shown.)
2. Enable OSPF:
   ```
   # Configure Router A.
   <RouterA> system-view
   [RouterA] router id 11.2.1.2
   [RouterA] ospf
   [RouterA-ospf-1] area 0
   [RouterA-ospf-1-area-0.0.0.0] network 11.2.1.0 0.0.0.255
   [RouterA-ospf-1-area-0.0.0.0] quit
   [RouterA-ospf-1] quit
   # Configure Router B.
   ```
# Configure Router B.
<RouterB> system-view
[RouterB] router id 11.2.1.1
[RouterB] ospf
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 11.2.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] quit

# Configure Router C.
<RouterC> system-view
[RouterC] router id 11.1.1.2
[RouterC] ospf
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] network 10.2.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] quit
[RouterC-ospf-1] quit

# Configure Router D.
<RouterD> system-view
[RouterD] router id 10.3.1.1
[RouterD] ospf
[RouterD-ospf-1] area 0
[RouterD-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[RouterD-ospf-1-area-0.0.0.0] network 10.3.1.0 0.0.0.255
[RouterD-ospf-1-area-0.0.0.0] quit
[RouterD-ospf-1] quit

# Configure Router E.
<RouterE> system-view
[RouterE] router id 10.4.1.1
[RouterE] ospf
[RouterE-ospf-1] area 0
[RouterE-ospf-1-area-0.0.0.0] network 10.2.1.0 0.0.0.255
[RouterE-ospf-1-area-0.0.0.0] network 10.4.1.0 0.0.0.255
[RouterE-ospf-1-area-0.0.0.0] quit
[RouterE-ospf-1] quit

3. Configure BGP to redistribute OSPF routes and direct routes:

# Configure Router B.
[RouterB] bgp 200
[RouterB-bgp-default] peer 11.1.1.2 as-number 100
[RouterB-bgp-default] address-family ipv4 unicast
[RouterB-bgp-default-ipv4] peer 11.1.1.2 enable
[RouterB-bgp-default-ipv4] import-route ospf
[RouterB-bgp-default-ipv4] import-route direct
[RouterB-bgp-default-ipv4] quit
[RouterB-bgp-default] quit

# Configure Router C.
[RouterC] bgp 100
[RouterC-bgp-default] peer 11.1.1.1 as-number 200
[RouterC-bgp-default] address-family ipv4 unicast
4. Configure Router B and Router C to redistribute BGP routes into OSPF:

# Configure OSPF to redistribute routes from BGP on Router B.
[RouterB] ospf
[RouterB-ospf-1] import-route bgp

# Configure OSPF to redistribute routes from BGP on Router C.
[RouterC] ospf
[RouterC-ospf-1] import-route bgp

# Display the IP routing table on Router A.
[RouterA] display ip routing-table

<table>
<thead>
<tr>
<th>Destination/Mask</th>
<th>Proto</th>
<th>Pre</th>
<th>Cost</th>
<th>NextHop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>10.1.1.0/24</td>
<td>O_ASE2</td>
<td>150</td>
<td>1</td>
<td>11.2.1.1</td>
<td>GE1/0/1</td>
</tr>
<tr>
<td>10.2.1.0/24</td>
<td>O_ASE2</td>
<td>150</td>
<td>1</td>
<td>11.2.1.1</td>
<td>GE1/0/1</td>
</tr>
<tr>
<td>10.3.1.0/24</td>
<td>O_ASE2</td>
<td>150</td>
<td>1</td>
<td>11.2.1.1</td>
<td>GE1/0/1</td>
</tr>
<tr>
<td>10.4.1.0/24</td>
<td>O_ASE2</td>
<td>150</td>
<td>1</td>
<td>11.2.1.1</td>
<td>GE1/0/1</td>
</tr>
<tr>
<td>11.2.1.0/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>11.2.1.2</td>
<td>GE1/0/1</td>
</tr>
<tr>
<td>11.2.1.2/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>11.2.1.255/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>11.2.1.2</td>
<td>GE1/0/1</td>
</tr>
<tr>
<td>127.0.0.0/8</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>127.0.0.0/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>127.0.0.1/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>127.255.255.255</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>224.0.0.0/4</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0</td>
<td>NULL0</td>
</tr>
<tr>
<td>224.0.0.0/24</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0</td>
<td>NULL0</td>
</tr>
<tr>
<td>255.255.255.255</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
</tbody>
</table>

5. Configure route summarization:

# Configure route summarization on Router B to advertise a single route 10.0.0.0/8.
[RouterB-ospf-1] asbr-summary 10.0.0.0 8

# Display the IP routing table on Router A.
[RouterA] display ip routing-table

<table>
<thead>
<tr>
<th>Destination/Mask</th>
<th>Proto</th>
<th>Pre</th>
<th>Cost</th>
<th>NextHop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>10.0.0.0/8</td>
<td>O_ASE2</td>
<td>150</td>
<td>2</td>
<td>11.2.1.1</td>
<td>GE1/0/1</td>
</tr>
<tr>
<td>11.2.1.0/24</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>11.2.1.2</td>
<td>GE1/0/1</td>
</tr>
<tr>
<td>11.2.1.0/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>11.2.1.2</td>
<td>GE1/0/1</td>
</tr>
<tr>
<td>11.2.1.2/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
</tbody>
</table>
The output shows that routes 10.1.1.0/24, 10.2.1.0/24, 10.3.1.0/24 and 10.4.1.0/24 are summarized into a single route 10.0.0.0/8.

**OSPF stub area configuration example**

**Network requirements**

As shown in Figure 27:

- Enable OSPF on all routers, and split the AS into three areas.
- Configure Router A and Router B as ABRs to forward routing information between areas.
- Configure Router D as the ASBR to redistribute static routes.
- Configure Area 1 as a stub area to reduce advertised LSAs without influencing reachability.

**Figure 27 Network diagram**

**Configuration procedure**

1. Configure IP addresses for interfaces. (Details not shown.)
2. Enable OSPF (see "Basic OSPF configuration example").
3. Configure route redistribution:
   
   # Configure Router D to redistribute static routes.
   
   ```
   <RouterD> system-view
   [RouterD] ip route-static 3.1.2.1 24 10.5.1.2
   [RouterD] ospf
   [RouterD-ospf-1] import-route static
   [RouterD-ospf-1] quit
   ```

   # Display ABR/ASBR information on Router C.

   ```
   <RouterC> display ospf abr-asbr
   ```
<table>
<thead>
<tr>
<th>Type</th>
<th>Destination</th>
<th>Area</th>
<th>Cost</th>
<th>NextHop</th>
<th>RtType</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intra</td>
<td>10.2.1.1</td>
<td>0.0.0.1</td>
<td>3</td>
<td>10.2.1.1</td>
<td>ABR</td>
</tr>
<tr>
<td>Inter</td>
<td>10.5.1.1</td>
<td>0.0.0.1</td>
<td>7</td>
<td>10.2.1.1</td>
<td>ASBR</td>
</tr>
</tbody>
</table>

# Display OSPF routing information on Router C.

```
<RouterC> display ospf routing
```

```
OSPF Process 1 with Router ID 10.4.1.1
Routing Table

Routing for network

<table>
<thead>
<tr>
<th>Destination</th>
<th>Cost</th>
<th>Type</th>
<th>NextHop</th>
<th>AdvRouter</th>
<th>Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.2.1.0/24</td>
<td>3</td>
<td>Transit</td>
<td>0.0.0.0</td>
<td>10.2.1.1</td>
<td>0.0.0.1</td>
</tr>
<tr>
<td>10.3.1.0/24</td>
<td>7</td>
<td>Inter</td>
<td>10.2.1.1</td>
<td>10.2.1.1</td>
<td>0.0.0.1</td>
</tr>
<tr>
<td>10.4.1.0/24</td>
<td>3</td>
<td>Stub</td>
<td>0.0.0.0</td>
<td>10.4.1.1</td>
<td>0.0.0.1</td>
</tr>
<tr>
<td>10.5.1.0/24</td>
<td>17</td>
<td>Inter</td>
<td>10.2.1.1</td>
<td>10.2.1.1</td>
<td>0.0.0.1</td>
</tr>
<tr>
<td>10.1.1.0/24</td>
<td>5</td>
<td>Inter</td>
<td>10.2.1.1</td>
<td>10.2.1.1</td>
<td>0.0.0.1</td>
</tr>
</tbody>
</table>

Routing for ASEs

<table>
<thead>
<tr>
<th>Destination</th>
<th>Cost</th>
<th>Type</th>
<th>Tag</th>
<th>NextHop</th>
<th>AdvRouter</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.2.0/24</td>
<td>1</td>
<td>Type2</td>
<td>1</td>
<td>10.2.1.1</td>
<td>10.5.1.1</td>
</tr>
</tbody>
</table>

Total nets: 6
Intra area: 2  Inter area: 3  ASE: 1  NSSA: 0

The output shows that Router C’s routing table contains an AS external route.

4. Configure Area 1 as a stub area:

# Configure Router A.

```
<RouterA> system-view
[RouterA] ospf
[RouterA-ospf-1] area 1
[RouterA-ospf-1-area-0.0.0.1] stub
[RouterA-ospf-1-area-0.0.0.1] quit
[RouterA-ospf-1] quit
```

# Configure Router C.

```
<RouterC> system-view
[RouterC] ospf
[RouterC-ospf-1] area 1
[RouterC-ospf-1-area-0.0.0.1] stub
[RouterC-ospf-1-area-0.0.0.1] quit
[RouterC-ospf-1] quit
```

# Display OSPF routing information on Router C.

```
[RouterC] display ospf routing
```

```
OSPF Process 1 with Router ID 10.4.1.1
Routing Table

Routing for network

<table>
<thead>
<tr>
<th>Destination</th>
<th>Cost</th>
<th>Type</th>
<th>NextHop</th>
<th>AdvRouter</th>
<th>Area</th>
</tr>
</thead>
</table>

114
The output shows that a default route replaces the AS external route.

# Configure Area 1 as a totally stub area.

```bash
[RouterA] ospf
[RouterA-ospf-1] area 1
[RouterA-ospf-1-area-0.0.0.1] stub no-summary
[RouterA-ospf-1-area-0.0.0.1] quit
```

# Display OSPF routing information on Router C.

```bash
[RouterC] display ospf routing
```

OSPF Process 1 with Router ID 10.4.1.1
Routing Table

Routing for network

<table>
<thead>
<tr>
<th>Destination</th>
<th>Cost</th>
<th>Type</th>
<th>NextHop</th>
<th>AdvRouter</th>
<th>Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0/0</td>
<td>4</td>
<td>Inter</td>
<td>10.2.1.1</td>
<td>10.2.1.1</td>
<td>0.0.0.1</td>
</tr>
<tr>
<td>10.2.1.0/24</td>
<td>3</td>
<td>Transit</td>
<td>0.0.0.0</td>
<td>10.2.1.1</td>
<td>0.0.0.1</td>
</tr>
<tr>
<td>10.4.1.0/24</td>
<td>3</td>
<td>Stub</td>
<td>0.0.0.0</td>
<td>10.4.1.1</td>
<td>0.0.0.1</td>
</tr>
</tbody>
</table>

Total nets: 3
Intra area: 2 Inter area: 1 ASE: 0 NSSA: 0

The output shows that inter-area routes are removed, and only one external route (a default route) exists on Router C.

**OSPF NSSA area configuration example**

**Network requirements**

As shown in Figure 28:
- Configure OSPF on all routers and split AS into three areas.
- Configure Router A and Router B as ABRs to forward routing information between areas.
- Configure Area 1 as an NSSA area and configure Router C as an ASBR to redistribute static routes into the AS.
Configuration procedure

1. Configure IP addresses for interfaces. (Details not shown.)
2. Enable OSPF (see "Basic OSPF configuration example").
3. Configure Area 1 as an NSSA area:

   # Configure Router A.
   <RouterA> system-view
   [RouterA] ospf
   [RouterA-ospf-1] area 1
   [RouterA-ospf-1-area-0.0.0.1] nssa
   [RouterA-ospf-1-area-0.0.0.1] quit
   [RouterA-ospf-1] quit

   # Configure Router C.
   <RouterC> system-view
   [RouterC] ospf
   [RouterC-ospf-1] area 1
   [RouterC-ospf-1-area-0.0.0.1] nssa
   [RouterC-ospf-1-area-0.0.0.1] quit
   [RouterC-ospf-1] quit

   # Display routing information on Router C.
   [RouterC] display ospf routing

   OSPF Process 1 with Router ID 10.4.1.1
   Routing Table

<table>
<thead>
<tr>
<th>Destination</th>
<th>Cost</th>
<th>Type</th>
<th>NextHop</th>
<th>AdvRouter</th>
<th>Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.2.1.0/24</td>
<td>3</td>
<td>Transit</td>
<td>0.0.0.0</td>
<td>10.4.1.1</td>
<td>0.0.0.1</td>
</tr>
<tr>
<td>10.3.1.0/24</td>
<td>7</td>
<td>Inter</td>
<td>10.2.1.1</td>
<td>10.2.1.1</td>
<td>0.0.0.1</td>
</tr>
<tr>
<td>10.4.1.0/24</td>
<td>3</td>
<td>Stub</td>
<td>0.0.0.0</td>
<td>10.4.1.1</td>
<td>0.0.0.1</td>
</tr>
<tr>
<td>10.5.1.0/24</td>
<td>17</td>
<td>Inter</td>
<td>10.2.1.1</td>
<td>10.2.1.1</td>
<td>0.0.0.1</td>
</tr>
<tr>
<td>10.1.1.0/24</td>
<td>5</td>
<td>Inter</td>
<td>10.2.1.1</td>
<td>10.2.1.1</td>
<td>0.0.0.1</td>
</tr>
</tbody>
</table>

   Total nets: 5
   Intra area: 2  Inter area: 3  ASE: 0  NSSA: 0

4. Configure route redistribution:
Configure OSPF to redistribute the static route on Router C.

```
[RouterC] ip route-static 3.1.2.1 24 10.4.1.2
[RouterC] ospf
[RouterC-ospf-1] import-route static
[RouterC-ospf-1] quit
```

Display routing information on Router D.

```
<RouterD> display ospf routing
```

```
OSPF Process 1 with Router ID 10.5.1.1
Routing Table

Routing for network

<table>
<thead>
<tr>
<th>Destination</th>
<th>Cost</th>
<th>Type</th>
<th>NextHop</th>
<th>AdvRouter</th>
<th>Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.2.1.0/24</td>
<td>22</td>
<td>Inter</td>
<td>10.3.1.1</td>
<td>10.3.1.1</td>
<td>0.0.0.2</td>
</tr>
<tr>
<td>10.3.1.0/24</td>
<td>10</td>
<td>Transit</td>
<td>0.0.0.0</td>
<td>10.3.1.1</td>
<td>0.0.0.2</td>
</tr>
<tr>
<td>10.4.1.0/24</td>
<td>25</td>
<td>Inter</td>
<td>10.3.1.1</td>
<td>10.3.1.1</td>
<td>0.0.0.2</td>
</tr>
<tr>
<td>10.5.1.0/24</td>
<td>10</td>
<td>Stub</td>
<td>0.0.0.0</td>
<td>10.5.1.1</td>
<td>0.0.0.2</td>
</tr>
<tr>
<td>10.1.1.0/24</td>
<td>12</td>
<td>Inter</td>
<td>10.3.1.1</td>
<td>10.3.1.1</td>
<td>0.0.0.2</td>
</tr>
</tbody>
</table>

Routing for ASEs

<table>
<thead>
<tr>
<th>Destination</th>
<th>Cost</th>
<th>Type</th>
<th>Tag</th>
<th>NextHop</th>
<th>AdvRouter</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.2.0/24</td>
<td>1</td>
<td>Type2</td>
<td>1</td>
<td>10.3.1.1</td>
<td>10.2.1.1</td>
</tr>
</tbody>
</table>

Total nets: 6
Intra area: 2  Inter area: 3  ASE: 1  NSSA: 0
```

The output shows that an AS external route imported from the NSSA area exists on Router D.

**OSPF DR election configuration example**

**Network requirements**

As shown in **Figure 29**:

- Enable OSPF on Routers A, B, C, and D on the same network.
- Configure Router A as the DR, and configure Router C as the BDR.

**Figure 29 Network diagram**

![Network Diagram]

**Configuration procedure**

1. Configure IP addresses for interfaces. (Details not shown.)
2. **Enable OSPF:**

   # Configure Router A.
   ```
   <RouterA> system-view
   [RouterA] router id 1.1.1.1
   [RouterA] ospf
   [RouterA-ospf-1] area 0
   [RouterA-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
   [RouterA-ospf-1-area-0.0.0.0] quit
   [RouterA-ospf-1] quit
   ```

   # Configure Router B.
   ```
   <RouterB> system-view
   [RouterB] router id 2.2.2.2
   [RouterB] ospf
   [RouterB-ospf-1] area 0
   [RouterB-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
   [RouterB-ospf-1-area-0.0.0.0] quit
   [RouterB-ospf-1] quit
   ```

   # Configure Router C.
   ```
   <RouterC> system-view
   [RouterC] router id 3.3.3.3
   [RouterC] ospf
   [RouterC-ospf-1] area 0
   [RouterC-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
   [RouterC-ospf-1-area-0.0.0.0] quit
   [RouterC-ospf-1] quit
   ```

   # Configure Router D.
   ```
   <RouterD> system-view
   [RouterD] router id 4.4.4.4
   [RouterD] ospf
   [RouterD-ospf-1] area 0
   [RouterD-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
   [RouterD-ospf-1-area-0.0.0.0] quit
   [RouterD-ospf-1] quit
   ```

   # Display neighbor information on Router A.
   ```
   [RouterA] display ospf peer verbose
   ```

   OSPF Process 1 with Router ID 1.1.1.1
   Neighbors

   Area 0.0.0.0 interface 192.168.1.1(GigabitEthernet1/0/1)'s neighbors
   Router ID: 2.2.2.2 Address: 192.168.1.2 GR State: Normal
   State: 2-Way Mode: None Priority: 1
   DR: 192.168.1.4 BDR: 192.168.1.3 MTU: 0
   Options is 0x02 (-|--|--|--|--|--|E|--)
   Dead timer due in 38 sec
   Neighbor is up for 00:01:31
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 6
BFD status: Disabled

Router ID: 3.3.3.3 Address: 192.168.1.3 GR State: Normal
State: Full Mode: Nbr is master Priority: 1
DR: 192.168.1.4 BDR: 192.168.1.3 MTU: 0
Options is 0x02 (-|-|-|-|-|-|E|-)
Dead timer due in 31 sec
Neighbor is up for 00:01:28
Authentication Sequence: [ 0 ]
Neighbor state change count: 6
BFD status: Disabled

Router ID: 4.4.4.4 Address: 192.168.1.4 GR State: Normal
State: Full Mode: Nbr is master Priority: 1
DR: 192.168.1.4 BDR: 192.168.1.3 MTU: 0
Options is 0x02 (-|-|-|-|-|-|E|-)
Dead timer due in 31 sec
Neighbor is up for 00:01:28
Authentication Sequence: [ 0 ]
Neighbor state change count: 6
BFD status: Disabled

The output shows that Router D is the DR and Router C is the BDR.

3. Configure router priorities on interfaces:

   # Configure Router A.
   [RouterA] interface gigabitethernet 1/0/1
   [RouterA-GigabitEthernet1/0/1] ospf dr-priority 100
   [RouterA-GigabitEthernet1/0/1] quit

   # Configure Router B.
   [RouterB] interface gigabitethernet 1/0/1
   [RouterB-GigabitEthernet1/0/1] ospf dr-priority 0
   [RouterB-GigabitEthernet1/0/1] quit

   # Configure Router C.
   [RouterC] interface gigabitethernet 1/0/1
   [RouterC-GigabitEthernet1/0/1] ospf dr-priority 2
   [RouterC-GigabitEthernet1/0/1] quit

   # Display information about neighbors of Router D.
   <RouterD> display ospf peer verbose

       OSPF Process 1 with Router ID 4.4.4.4
       Neighbors

       Area 0.0.0.0 interface 192.168.1.4(GigabitEthernet1/0/1)'s neighbors
       Router ID: 1.1.1.1 Address: 192.168.1.1 GR State: Normal
       State: Full Mode: Nbr is slave Priority: 100
       DR: 192.168.1.4 BDR: 192.168.1.3 MTU: 0
       Options is 0x02 (-|-|-|-|-|-|E|-)
       Dead timer due in 31 sec
       Neighbor is up for 00:11:17
Authentication Sequence: [ 0 ]
Neighbor state change count: 6
BFD status: Disabled

Router ID: 2.2.2.2 Address: 192.168.1.2 GR State: Normal
State: Full Mode:Nbr is slave Priority: 0
DR: 192.168.1.4 BDR: 192.168.1.3 MTU: 0
Options is 0x02 (-|-|-|-|-|-|E|-
Dead timer due in 35 sec
Neighbor is up for 00:11:19
Authentication Sequence: [ 0 ]
Neighbor state change count: 6
BFD status: Disabled

Router ID: 3.3.3.3 Address: 192.168.1.3 GR State: Normal
State: Full Mode:Nbr is slave Priority: 2
DR: 192.168.1.4 BDR: 192.168.1.3 MTU: 0
Options is 0x02 (-|-|-|-|-|-|E|-
Dead timer due in 33 sec
Neighbor is up for 00:11:15
Authentication Sequence: [ 0 ]
Neighbor state change count: 6
BFD status: Disabled

The output shows that the DR and BDR are not changed, because the new router priority settings do not take effect immediately.

4. Restart the OSPF process:
   # Restart the OSPF process on Router D.
   <RouterD> reset ospf 1 process
   Reset OSPF process? [Y/N]: y
   # Display neighbor information on Router D.
   <RouterD> display ospf peer verbose

   OSPF Process 1 with Router ID 4.4.4.4
   Neighbors

   Area 0.0.0.0 interface 192.168.1.4(GigabitEthernet1/0/1)'s neighbors
   Router ID: 1.1.1.1 Address: 192.168.1.1 GR State: Normal
   State: Full Mode: Nbr is slave Priority: 100
   DR: 192.168.1.1 BDR: 192.168.1.3 MTU: 0
   Options is 0x02 (-|-|-|-|-|-|E|-
   Dead timer due in 39 sec
   Neighbor is up for 00:01:40
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 6
   BFD status: Disabled

   Router ID: 2.2.2.2 Address: 192.168.1.2 GR State: Normal
   State: 2-Way Mode: None Priority: 0
The output shows that Router A becomes the DR and Router C becomes the BDR. The full neighbor state means an adjacency has been established. The 2-way neighbor state means the two routers are not the DR or BDR, and they do not exchange LSAs.

Display OSPF interface information.

```
[RouterA] display ospf interface

OSPF Process 1 with Router ID 1.1.1.1
Interfaces

Area: 0.0.0.0
IP Address      Type      State   Cost  Pri   DR             BDR
192.168.1.1     Broadcast DR      1     100   192.168.1.1    192.168.1.3
```

```
[RouterB] display ospf interface

OSPF Process 1 with Router ID 2.2.2.2
Interfaces

Area: 0.0.0.0
IP Address      Type      State    Cost  Pri   DR             BDR
192.168.1.2     Broadcast DROther 1     0     192.168.1.1    192.168.1.3
```

The interface state DROther means the interface is not the DR or BDR.

**OSPF virtual link configuration example**

**Network requirements**

As shown in Figure 30, configure a virtual link between Router B and Router C to connect Area 2 to the backbone area. After configuration, Router B can learn routes to Area 2.
Configuration procedure

1. Configure IP addresses for interfaces. (Details not shown.)

2. Enable OSPF:
   
   # Configure Router A.
   
   `<RouterA> system-view
   [RouterA] ospf 1 router-id 1.1.1.1
   [RouterA-ospf-1] area 0
   [RouterA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
   [RouterA-ospf-1-area-0.0.0.0] quit
   [RouterA-ospf-1] quit
   `# Configure Router B.
   
   `<RouterB> system-view
   [RouterB] ospf 1 router-id 2.2.2.2
   [RouterB-ospf-1] area 0
   [RouterB-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
   [RouterB-ospf-1-area-0.0.0.0] quit
   [RouterB-ospf-1] area 1
   [RouterB-ospf-1-area-0.0.0.1] network 10.2.1.0 0.0.0.255
   [RouterB-ospf-1-area-0.0.0.1] quit
   [RouterB-ospf-1] quit
   `# Configure Router C.
   
   `<RouterC> system-view
   [RouterC] ospf 1 router-id 3.3.3.3
   [RouterC-ospf-1] area 1
   [RouterC-ospf-1-area-0.0.0.1] network 10.2.1.0 0.0.0.255
   [RouterC-ospf-1-area-0.0.0.1] quit
   [RouterC-ospf-1] area 2
   [RouterC-ospf-1-area-0.0.0.2] network 10.3.1.0 0.0.0.255
   [RouterC-ospf-1-area-0.0.0.2] quit
   [RouterC-ospf-1] quit
   `# Configure Router D.
   
   `<RouterD> system-view
   [RouterD] ospf 1 router-id 4.4.4.4
   [RouterD-ospf-1] area 2
   [RouterD-ospf-1-area-0.0.0.2] network 10.3.1.0 0.0.0.255
   [RouterD-ospf-1-area-0.0.0.2] quit
   [RouterD-ospf-1] quit

Figure 30 Network diagram
# Display OSPF routing information on Router B.

```
[RouterB] display ospf routing
```

```
OSPF Process 1 with Router ID 2.2.2.2
Routing Table
Routing for network
Destination        Cost     Type    NextHop         AdvRouter       Area
10.2.1.0/24        2        Transit 0.0.0.0         3.3.3.3         0.0.0.1
10.1.1.0/24        2        Transit 0.0.0.0         2.2.2.2         0.0.0.0
Total nets: 2
Intra area: 2  Inter area: 0  ASE: 0  NSSA: 0
```

The output shows that Router B does not have routes to Area 2 because Area 0 is not directly connected to Area 2.

3. Configure a virtual link:

# Configure Router B.

```
[RouterB] ospf
[RouterB-ospf-1] area 1
[RouterB-ospf-1-area-0.0.0.1] vlink-peer 3.3.3.3
[RouterB-ospf-1-area-0.0.0.1] quit
[RouterB-ospf-1] quit
```

# Configure Router C.

```
[RouterC] ospf
[RouterC-ospf-1] area 1
[RouterC-ospf-1-area-0.0.0.1] vlink-peer 2.2.2.2
[RouterC-ospf-1-area-0.0.0.1] quit
[RouterC-ospf-1] quit
```

# Display OSPF routing information on Router B.

```
[RouterB] display ospf routing
```

```
OSPF Process 1 with Router ID 2.2.2.2
Routing Table
Routing for network
Destination        Cost     Type    NextHop         AdvRouter       Area
10.2.1.0/24        2        Transit 0.0.0.0         3.3.3.3         0.0.0.1
10.3.1.0/24        5        Inter 10.2.1.2        3.3.3.3         0.0.0.0
10.1.1.0/24        2        Transit 0.0.0.0         2.2.2.2         0.0.0.0
Total nets: 3
Intra area: 2  Inter area: 1  ASE: 0  NSSA: 0
```

The output shows that Router B has learned the route 10.3.1.0/24 to Area 2.

**OSPF GR configuration example**

**Network requirements**

As shown in Figure 31:

- Router A, Router B, and Router C that belong to the same autonomous system and the same OSPF routing domain are GR capable.
• Router A acts as the non-IETF GR restarter. Router B and Router C are the GR helpers, and synchronize their LSDBs with Router A through OOB communication of GR.

Figure 31 Network diagram

Configuration procedure
1. Configure IP addresses for interfaces. (Details not shown.)
2. Enable OSPF:
   # Configure Router A.
   <RouterA> system-view
   [RouterA] router id 1.1.1.1
   [RouterA] ospf 100
   [RouterA-ospf-100] area 0
   [RouterA-ospf-100-area-0.0.0.0] network 192.1.1.0 0.0.0.255
   [RouterA-ospf-100-area-0.0.0.0] quit
   [RouterA-ospf-100] quit
   # Configure Router B.
   <RouterB> system-view
   [RouterB] router id 2.2.2.2
   [RouterB] ospf 100
   [RouterB-ospf-100] area 0
   [RouterB-ospf-100-area-0.0.0.0] network 192.1.1.0 0.0.0.255
   [RouterB-ospf-100-area-0.0.0.0] quit
   [RouterB-ospf-100] quit
   # Configure Router C.
   <RouterC> system-view
   [RouterC] router id 3.3.3.3
   [RouterC] ospf 100
   [RouterC-ospf-100] area 0
   [RouterC-ospf-100-area-0.0.0.0] network 192.1.1.0 0.0.0.255
   [RouterC-ospf-100-area-0.0.0.0] quit
   [RouterC-ospf-100] quit
3. Configure OSPF GR:
   # Configure Router A as the non-IETF OSPF GR restarter: enable the link-local signaling capability, the out-of-band re-synchronization capability, and non-IETF GR for OSPF process 100.
[RouterA-ospf-100] enable link-local-signaling
[RouterA-ospf-100] enable out-of-band-resynchronization
[RouterA-ospf-100] graceful-restart
[RouterA-ospf-100] quit

# Configure Router B as the GR helper: enable the link-local signaling capability and the out-of-band re-synchronization capability for OSPF process 100.
[RouterB-ospf-100] enable link-local-signaling
[RouterB-ospf-100] enable out-of-band-resynchronization

# Configure Router C as the GR helper: enable the link-local signaling capability and the out-of-band re-synchronization capability for OSPF process 100.
[RouterC-ospf-100] enable link-local-signaling
[RouterC-ospf-100] enable out-of-band-resynchronization

Verifying the configuration

# Enable OSPF GR event debugging and restart the OSPF process by using GR on Router A.
<RouterA> debugging ospf event graceful-restart
<RouterA> terminal monitor
<RouterA> terminal logging level 7
<RouterA> reset ospf 100 process graceful-restart
Reset OSPF process? [Y/N]: y

OSPF NSR configuration example

Network requirements
As shown in Figure 32, Router S, Router A, and Router B belong to the same OSPF routing domain. Enable OSPF NSR on Router S to ensure correct routing when an active/standby switchover occurs on Router S.

Figure 32 Network diagram

Configuration procedure

1. Configure IP addresses and subnet masks for interfaces on the routers. (Details not shown.)
2. Configure OSPF on the routers to ensure the following: (Details not shown.)
   o Router S, Router A, and Router B can communicate with each other at Layer 3.
   o Dynamic route update can be implemented among them with OSPF.

3. Enable OSPF NSR on Router S.
   <RouterS> system-view
   [RouterS] ospf 100
   [RouterS-ospf-100] non-stop-routing
   [RouterS-ospf-100] quit

Verifying the configuration

# Perform an active/standby switchover on Router S.
[RouterS] placement reoptimize
Predicted changes to the placement
Program                           Current location       New location
---------------------------------------------------------------------------------------------------
lb                                0/0                    0/0
lsm                               0/0                    0/0
slsp                              0/0                    0/0
rib6                              0/0                    0/0
routepolicy                       0/0                    0/0
rib                                0/0                    0/0
staticroute6                      0/0                    0/0
staticroute                       0/0                    0/0
eviisis                           0/0                    0/0
ospf                              0/0                    1/0

Continue? [y/n]: y
Re-optimization of the placement start. You will be notified on completion
Re-optimization of the placement complete. Use 'display placement' to view the new placement

# During the switchover period, display OSPF neighbors on Router A to verify the neighbor relationship between Router A and Router S.

<RouterA> display ospf peer

    OSPF Process 1 with Router ID 2.2.2.1
    Neighbor Brief Information

    Area: 0.0.0.0
    Router ID       Address         Pri Dead-Time  State             Interface
    3.3.3.1         12.12.12.2      1   37         Full/BDR          GE1/0/1

# Display OSPF routes on Router A to verify if Router A has a route to the loopback interface on Router B.

<RouterA> display ospf routing

    OSPF Process 1 with Router ID 2.2.2.1
    Routing Table

    Routing for network
    Destination        Cost     Type    NextHop         AdvRouter       Area
    44.44.44.44/32     2        Stub    12.12.12.2      4.4.4.1         0.0.0.0
    14.14.14.0/24      2        Transit 12.12.12.2    4.4.4.1         0.0.0.0
    22.22.22.22/32     0        Stub    0.0.0.0         2.2.2.1         0.0.0.0
    12.12.12.0/24      1        Transit 0.0.0.0        2.2.2.1         0.0.0.0

    Total nets: 4
    Intra area: 4  Inter area: 0  ASE: 0  NSSA: 0

# Display OSPF neighbors on Router B to verify the neighbor relationship between Router B and Router S.

<RouterB> display ospf peer

    OSPF Process 1 with Router ID 4.4.4.1
    Neighbor Brief Information
# Display OSPF routes on Router B to verify if Router B has a route to the loopback interface on Router A.

```
<RouterB> display ospf routing
```

```
OSPF Process 1 with Router ID 4.4.4.1
Routing Table

Routing for network

<table>
<thead>
<tr>
<th>Destination</th>
<th>Cost</th>
<th>Type</th>
<th>NextHop</th>
<th>AdvRouter</th>
<th>Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>44.44.44.44/32</td>
<td>0</td>
<td>Stub</td>
<td>0.0.0.0</td>
<td>4.4.4.1</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>14.14.14.0/24</td>
<td>1</td>
<td>Transit</td>
<td>0.0.0.0</td>
<td>4.4.4.1</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>22.22.22.22/32</td>
<td>2</td>
<td>Stub</td>
<td>14.14.14.2</td>
<td>2.2.2.1</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>12.12.12.0/24</td>
<td>2</td>
<td>Transit</td>
<td>14.14.14.2</td>
<td>2.2.2.1</td>
<td>0.0.0.0</td>
</tr>
</tbody>
</table>

Total nets: 4  
Intra area: 4  Inter area: 0  ASE: 0  NSSA: 0
```

The output shows the following when an active/standby switchover occurs on Router S:

- The neighbor relationships and routing information on Router A and Router B have not changed.
- The traffic from Router A to Router B has not been impacted.

## BFD for OSPF configuration example

### Network requirements

As shown in Figure 33, run OSPF on Router A, Router B, and Router C so that they can reach each other at the network layer.

- When the link over which Router A and Router B communicate through a Layer 2 switch fails, BFD can quickly detect the failure and notify OSPF of the failure.
- Router A and Router B then communicate through Router C.

**Figure 33 Network diagram**
## Table 9 Interface and IP address assignment

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router A</td>
<td>GE1/0/1</td>
<td>192.168.0.102/24</td>
</tr>
<tr>
<td>Router A</td>
<td>GE1/0/2</td>
<td>10.1.1.102/24</td>
</tr>
<tr>
<td>Router A</td>
<td>Loop0</td>
<td>121.1.1.1/32</td>
</tr>
<tr>
<td>Router B</td>
<td>GE1/0/1</td>
<td>192.168.0.100/24</td>
</tr>
<tr>
<td>Router B</td>
<td>GE1/0/2</td>
<td>13.1.1.1/24</td>
</tr>
<tr>
<td>Router B</td>
<td>Loop0</td>
<td>120.1.1.1/32</td>
</tr>
<tr>
<td>Router C</td>
<td>GE1/0/1</td>
<td>10.1.1.100/24</td>
</tr>
<tr>
<td>Router C</td>
<td>GE1/0/2</td>
<td>13.1.1.2/24</td>
</tr>
</tbody>
</table>

### Configuration procedure

1. **Configure IP addresses for interfaces.** *(Details not shown.)*
2. **Enable OSPF:**
   
   # Configure Router A.
   
   `<RouterA> system-view
   [RouterA] ospf
   [RouterA-ospf-1] area 0
   [RouterA-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
   [RouterA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
   [RouterA-ospf-1-area-0.0.0.0] network 121.1.1.1 0.0.0.0
   [RouterA-ospf-1-area-0.0.0.0] quit
   [RouterA-ospf-1] quit
   
   # Configure Router B.
   
   `<RouterB> system-view
   [RouterB] ospf
   [RouterB-ospf-1] area 0
   [RouterB-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
   [RouterB-ospf-1-area-0.0.0.0] network 13.1.1.0 0.0.0.255
   [RouterB-ospf-1-area-0.0.0.0] network 120.1.1.1 0.0.0.0
   [RouterB-ospf-1-area-0.0.0.0] quit
   [RouterB-ospf-1] quit
   
   # Configure Router C.
   
   `<RouterC> system-view
   [RouterC] ospf
   [RouterC-ospf-1] area 0
   [RouterC-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
   [RouterC-ospf-1-area-0.0.0.0] network 13.1.1.0 0.0.0.255
   [RouterC-ospf-1-area-0.0.0.0] quit
   [RouterC-ospf-1] quit

3. **Configure BFD:**
   
   # Enable BFD on Router A and configure BFD parameters.
   
   `[RouterA] bfd session init-mode active
   [RouterA] interface gigabitethernet 1/0/1
   [RouterA-GigabitEthernet1/0/1] ospf bfd enable
[RouterA-GigabitEthernet1/0/1] bfd min-transmit-interval 500
[RouterA-GigabitEthernet1/0/1] bfd min-receive-interval 500
[RouterA-GigabitEthernet1/0/1] bfd detect-multiplier 7
[RouterA-GigabitEthernet1/0/1] quit

# Enable BFD on Router B and configure BFD parameters.
[RouterB] bfd session init-mode active
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] ospf bfd enable
[RouterB-GigabitEthernet1/0/1] bfd min-transmit-interval 500
[RouterB-GigabitEthernet1/0/1] bfd min-receive-interval 500
[RouterB-GigabitEthernet1/0/1] bfd detect-multiplier 6
[RouterB-GigabitEthernet1/0/1] quit

Verifying the configuration

# Display the BFD information on Router A.
<RouterA> display bfd session

Total Session Num: 1     Up Session Num: 1     Init Mode: Active
IPv4 Session Working Under Ctrl Mode:

<table>
<thead>
<tr>
<th>LD/RD</th>
<th>SourceAddr</th>
<th>DestAddr</th>
<th>State</th>
<th>Holdtime</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>3/1</td>
<td>192.168.0.102</td>
<td>192.168.0.100</td>
<td>Up</td>
<td>1700ms</td>
<td>GE1/0/1</td>
</tr>
</tbody>
</table>

# Display routes destined for 120.1.1.1/32 on Router A.
<RouterA> display ip routing-table 120.1.1.1 verbose

Summary Count : 1

Destination: 120.1.1.1/32
Protocol: O_INTRA
Process ID: 1
SubProtID: 0x1
Cost: 1
IpPre: N/A
QosLocalID: N/A
Tag: 0
State: Active Adv
OrigTblID: 0x0
OrigVrf: default-vrf
TableID: 0x2
OrigAs: 0
NibID: 0x26000002
LastAs: 0
AttrID: 0xffffffff
Neighbor: 0.0.0.0
Flags: 0x1008c
OrigNextHop: 192.168.0.100
Label: NULL
RealNextHop: 192.168.0.100
BkLabel: NULL
BkNextHop: N/A
Tunnel ID: Invalid
Interface: GigabitEthernet1/0/1
BkTunnel ID: Invalid
BkInterface: N/A
FtnIndex: 0x0
TrafficIndex: N/A
Connector: N/A

The output shows that Router A communicates with Router B through GigabitEthernet 1/0/1. Then the link over GigabitEthernet 1/0/1 fails.
Display routes destined for 120.1.1.1/32 on Router A.

```
<RouterA> display ip routing-table 120.1.1.1 verbose
```

Summary Count : 1

---

**Destination:** 120.1.1.1/32  
**Protocol:** O_INTRA  
**Process ID:** 1  
**SubProtID:** 0x1  
**Cost:** 2  
**IpPre:** N/A  
**Tag:** 0  
**OrigTbID:** 0x0  
**TableID:** 0x2  
**NibID:** 0x26000002  
**AttrID:** 0xffffffff  
**Flags:** 0x1008c  
**Label:** NULL  
**BkLabel:** NULL  
**Tunnel ID:** Invalid  
**BkTunnel ID:** Invalid  
**FtnIndex:** 0x0  
**Interface:** GigabitEthernet1/0/2  
**Neighbor:** 0.0.0.0  

The output shows that Router A communicates with Router B through GigabitEthernet 1/0/2.

### OSPF FRR configuration example

#### Network requirements

As shown in [Figure 34](#), Router A, Router B, and Router C reside in the same OSPF domain. Configure OSPF FRR so that when Link A fails, traffic is immediately switched to Link B.

#### Figure 34 Network diagram

![Network Diagram](#)

#### Table 10 Interface and IP address assignment

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router A</td>
<td>GE1/0/1</td>
<td>12.12.12.1/24</td>
</tr>
<tr>
<td>Router A</td>
<td>GE1/0/2</td>
<td>13.13.13.1/24</td>
</tr>
<tr>
<td>Router A</td>
<td>Loop0</td>
<td>1.1.1.1/32</td>
</tr>
</tbody>
</table>
### Configuration procedure

1. Configure IP addresses and subnet masks for interfaces on the routers. (Details not shown.)
2. Configure OSPF on the routers to ensure that Router A, Router B, and Router C can communicate with each other at the network layer. (Details not shown.)
3. Configure OSPF FRR:
   You can enable OSPF FRR to either calculate a backup next hop by using the LFA algorithm, or specify a backup next hop by using a routing policy.
   - (Method 1.) Enable OSPF FRR to calculate a backup next hop by using the LFA algorithm:
     ```
     # Configure Router A.
     <RouterA> system-view
     [RouterA] ospf 1
     [RouterA-ospf-1] fast-reroute lfa
     [RouterA-ospf-1] quit
     
     # Configure Router B.
     <RouterB> system-view
     [RouterB] ospf 1
     [RouterB-ospf-1] fast-reroute lfa
     [RouterB-ospf-1] quit
     ```
   - (Method 2.) Enable OSPF FRR to specify a backup next hop by using a routing policy:
     ```
     # Configure Router A.
     <RouterA> system-view
     [RouterA] ip prefix-list abc index 10 permit 4.4.4.4 32
     [RouterA] route-policy frr permit node 10
     [RouterA-route-policy-frr-10] if-match ip address prefix-list abc
     [RouterA-route-policy-frr-10] apply fast-reroute backup-interface
gigabitethernet 1/0/1 backup-nexthop 12.12.12.2
     [RouterA-route-policy-frr-10] quit
     [RouterA] ospf 1
     [RouterA-ospf-1] fast-reroute route-policy frr
     [RouterA-ospf-1] quit
     
     # Configure Router B.
     <RouterB> system-view
     [RouterB] ip prefix-list abc index 10 permit 1.1.1.1 32
     [RouterB] route-policy frr permit node 10
     [RouterB-route-policy-frr-10] if-match ip address prefix-list abc
     [RouterB-route-policy-frr-10] apply fast-reroute backup-interface
gigabitethernet 1/0/1 backup-nexthop 24.24.24.2
     [RouterB-route-policy-frr-10] quit
     [RouterB] ospf 1
     ```

---

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router B</td>
<td>GE1/0/1</td>
<td>24.24.24.4/24</td>
</tr>
<tr>
<td>Router B</td>
<td>GE1/0/2</td>
<td>13.13.13.2/24</td>
</tr>
<tr>
<td>Router B</td>
<td>Loop0</td>
<td>4.4.4.4/32</td>
</tr>
<tr>
<td>Router C</td>
<td>GE1/0/1</td>
<td>12.12.12.2/24</td>
</tr>
<tr>
<td>Router C</td>
<td>GE1/0/2</td>
<td>24.24.24.2/24</td>
</tr>
</tbody>
</table>
Verifying the configuration

# Display route 4.4.4.4/32 on Router A to view the backup next hop information.
[RouterA] display ip routing-table 4.4.4.4 verbose

Summary Count : 1

Destination: 4.4.4.4/32
   Protocol: O_INTRA
   Process ID: 1
   SubProtID: 0x1
   Cost: 1
   IpPre: N/A
   Tag: 0
   OrigTblID: 0x0
   TableID: 0x2
  NibID: 0x26000002
   AttrID: 0xffffffff
   Flags: 0x1008c
   Neighbor: 0.0.0.0
   OrigVrf: default-vrf
   OrigAs: 0
   RealNextHop: 13.13.13.2
   OrigNextHop: 13.13.13.2
   BkLabel: NULL
   BkNextHop: 24.24.24.2
   Tunnel ID: Invalid
   BkTunnel ID: Invalid
   FtnIndex: 0x0
   Interface: GigabitEthernet1/0/2
   TrafficIndex: N/A
   Connector: N/A

# Display route 1.1.1.1/32 on Router B to view the backup next hop information.
[RouterB] display ip routing-table 1.1.1.1 verbose

Summary Count : 1

Destination: 1.1.1.1/32
   Protocol: O_INTRA
   Process ID: 1
   SubProtID: 0x1
   Cost: 1
   IpPre: N/A
   Tag: 0
   OrigTblID: 0x0
   TableID: 0x2
   NibID: 0x26000002
   AttrID: 0xffffffff
   Flags: 0x1008c
   Neighbor: 0.0.0.0
   OrigVrf: default-vrf
   OrigAs: 0
   RealNextHop: 13.13.13.2
   OrigNextHop: 13.13.13.2
   BkLabel: NULL
   BkNextHop: 24.24.24.2
   Tunnel ID: Invalid
   BkTunnel ID: Invalid
   FtnIndex: 0x0
   Interface: GigabitEthernet1/0/2
   TrafficIndex: N/A
   Connector: N/A
Troubleshooting OSPF configuration

No OSPF neighbor relationship established

Symptom
No OSPF neighbor relationship can be established.

Analysis
If the physical link and lower layer protocols work correctly, verify OSPF parameters configured on interfaces. Two neighbors must have the same parameters, such as the area ID, network segment, and mask. (A P2P or virtual link can have different network segments and masks.)

Solution
To resolve the problem:
1. Use the `display ospf peer` command to verify OSPF neighbor information.
2. Use the `display ospf interface` command to verify OSPF interface information.
3. Ping the neighbor router’s IP address to verify that the connectivity is normal.
4. Verify OSPF timers. The dead interval on an interface must be a minimum of four times the hello interval.
5. On an NBMA network, use the `peer ip-address` command to manually specify the neighbor.
6. A minimum of one interface must have a router priority higher than 0 on an NBMA or a broadcast network.
7. If the problem persists, contact Hewlett Packard Enterprise Support.

Incorrect routing information

Symptom
OSPF cannot find routes to other areas.

Analysis
The backbone area must maintain connectivity to all other areas. If a router connects to more than one area, a minimum of one area must be connected to the backbone. The backbone cannot be configured as a stub area.

In a stub area, all routers cannot receive external routes, and all interfaces connected to the stub area must belong to the stub area.

Solution
To resolve the problem:
1. Use the `display ospf peer` command to verify neighbor information.
2. Use the `display ospf interface` command to verify OSPF interface information.
3. Use the `display ospf lsdb` command to verify the LSDB.
4. Use the `display current-configuration configuration ospf` command to verify area configuration. If more than two areas are configured, a minimum of one area is connected to the backbone.
5. In a stub area, all routers attached are configured with the `stub` command. In an NSSA area, all routers attached are configured with the `nssa` command.
6. If a virtual link is configured, use the `display ospf vlink` command to verify the state of the virtual link.

7. If the problem persists, contact Hewlett Packard Enterprise Support.
Configuring IS-IS

Overview

Intermediate System-to-Intermediate System (IS-IS) is a dynamic routing protocol designed by the ISO to operate on the connectionless network protocol (CLNP).

IS-IS was modified and extended in RFC 1195 by the IETF for application in both TCP/IP and OSI reference models, called "Integrated IS-IS" or "Dual IS-IS."

IS-IS is an IGP used within an AS. It uses the SPF algorithm for route calculation.

Terminology

- **Intermediate system**—Similar to a router in TCP/IP, IS is the basic unit used in an IS-IS routing domain to generate and propagate routing information. Throughout this chapter, an IS refers to a router.
- **End system**—Similar to a host in TCP/IP, an ES does not run IS-IS. ISO defines the ES-IS protocol for communication between an ES and an IS.
- **Routing domain**—An RD comprises a group of ISs that exchange routing information with each other by using the same routing protocol.
- **Area**—An IS-IS routing domain can be split into multiple areas.
- **Link State Database**—All link states in the network form the LSDB. Each IS has a minimum of one LSDB. An IS uses the SPF algorithm and LSDB to generate IS-IS routes.
- **Link State Protocol Data Unit or Link State Packet**—An IS advertises link state information in an LSP.
- **Network Protocol Data Unit**—An NPDU is a network layer protocol packet in OSI, similar to an IP packet in TCP/IP.
- **Designated IS**—A DIS is elected on a broadcast network.
- **Network service access point**—An NSAP is an OSI network layer address. The NSAP identifies an abstract network service access point and describes the network address format in the OSI reference model.

IS-IS address format

**NSAP**

As shown in Figure 35, an NSAP address comprises the Initial Domain Part (IDP) and the Domain Specific Part (DSP). The IDP is analogous to the network ID of an IP address, and the DSP is analogous to the subnet and host ID.

The IDP includes the Authority and Format Identifier (AFI) and the Initial Domain Identifier (IDI).

The DSP includes:

- **High Order Part of DSP (HO-DSP)**—Identifies the area.
- **System ID**—Identifies the host.
- **SEL**—Identifies the type of service.

The IDP and DSP are variable in length. The length of an NSAP address is in the range of 8 to 20 bytes.
Area address

The area address comprises the IDP and the HO-DSP of the DSP, which identify the area and the routing domain. Different routing domains cannot have the same area address.

Typically, a router only needs one area address, and all nodes in the same area must have the same area address. To support smooth area merging, partitioning, and switching, a router can have a maximum of three area addresses.

System ID

A system ID uniquely identifies a host or router. It has a fixed length of 48 bits (6 bytes).

The system ID of a device can be generated from the router ID. For example, suppose a router uses the IP address 168.10.1.1 of Loopback 0 as the router ID. The system ID can be obtained in the following steps:

1. Extend each decimal number of the IP address to three digits by adding 0s from the left, such as 168.010.001.001.
2. Divide the extended IP address into three sections that each has four digits to get the system ID 1680.1000.1001.

If you use other methods to define a system ID, make sure that it can uniquely identify the host or router.

SEL

The N-SEL, or the NSAP selector (SEL), is similar to the protocol identifier in IP. Different transport layer protocols correspond to different SELs. All SELs in IP are 00.

Routing method

The IS-IS address format identifies the area, so a Level-1 router can easily identify packets destined to other areas. IS-IS routers perform routing as follows:

- A Level-1 router performs intra-area routing according to the system ID. If the destination address of a packet does not belong to the local area, the Level-1 router forwards it to the nearest Level-1-2 router.
- A Level-2 router performs inter-area routing according to the area address.

NET

A network entity title (NET) identifies the network layer information of an IS. It does not include transport layer information. A NET is a special NSAP address with the SEL being 0. The length of a NET is in the range of 8 to 20 bytes, same as a NSAP address.

A NET includes the following parts:

- **Area ID**—Has a length of 1 to 13 bytes.
- **System ID**—A system ID uniquely identifies a host or router in the area and has a fixed length of 6 bytes.
- **SEL**—Has a value of 0 and a fixed length of 1 byte.

For example, for a NET ab.cdef.1234.5678.9abc.00, the area ID is ab.cdef, the system ID is 1234.5678.9abc, and the SEL is 00.
Typically, a router only needs one NET, but it can have a maximum of three NETs for smooth area merging and partitioning. When you configure multiple NETs, make sure the system IDs are the same.

IS-IS area

IS-IS has a 2-level hierarchy to support large-scale networks. A large-scale routing domain is divided into multiple areas. Typically, a Level-1 router is deployed within an area. A Level-2 router is deployed between areas. A Level-1-2 router is deployed between Level-1 and Level-2 routers.

Level-1 and Level-2

- **Level-1 router**—A Level-1 router establishes neighbor relationships with Level-1 and Level-1-2 routers in the same area. It maintains an LSDB comprising intra-area routing information. A Level-1 router forwards packets destined for external areas to the nearest Level-1-2 router. Level-1 routers in different areas cannot establish neighbor relationships.

- **Level-2 router**—A Level-2 router establishes neighbor relationships with Level-2 and Level-1-2 routers in the same area or in different areas. It maintains a Level-2 LSDB containing inter-area routing information. All the Level-2 and Level-1-2 routers must be contiguous to form the backbone of the IS-IS routing domain. Level-2 routers can establish neighbor relationships even if they are in different areas.

- **Level-1-2 router**—A router with both Level-1 and Level-2 router functions is a Level-1-2 router. It can establish Level-1 neighbor relationships with Level-1 and Level-1-2 routers in the same area. It can establish Level-2 neighbor relationships with Level-2 and Level-1-2 routers in different areas. A Level-1 router can reach other areas only through a Level-1-2 router. The Level-1-2 router maintains two LSDBs, a Level-1 LSDB for intra-area routing and a Level-2 LSDB for inter-area routing.

Figure 36 shows one IS-IS network topology. Area 1 is the backbone that comprises a set of Level-2 routers. The other four areas are non-backbone areas connected to the backbone through Level-1-2 routers.

**Figure 36 IS-IS topology 1**
Figure 37 shows another IS-IS topology. The Level-1-2 routers connect to the Level-1 and Level-2 routers, and form the IS-IS backbone together with the Level-2 routers. No area is defined as the backbone in this topology. The backbone comprises all contiguous Level-2 and Level-1-2 routers in different areas. The IS-IS backbone does not need to be a specific area.

Both the Level-1 and Level-2 routers use the SPF algorithm to generate the shortest path tree.

Route leaking

Level-2 and Level-1-2 routers form a Level-2 area. An IS-IS routing domain comprises only one Level-2 area and multiple Level-1 areas. A Level-1 area must connect to the Level-2 area rather than another Level-1 area.

Level-1-2 routers send the routing information of Level-1 areas to the Level-2 area. Level-2 routers know the routing information of the entire IS-IS routing domain. By default, a Level-2 router does not advertise the routing information of other areas to a Level-1 area. A Level-1 router simply sends packets destined for other areas to the nearest Level-1-2 router. The path passing through the Level-1-2 router might not be the best. To solve this problem, IS-IS provides the route leaking feature.

Route leaking enables a Level-1-2 router to advertise the routes of other areas to the connected Level-1 area so that the Level-1 routers can select the optimal routes.

IS-IS network types

Network types

IS-IS supports broadcast networks (for example, Ethernet and Token Ring) and point-to-point networks (for example, PPP and HDLC).

For an NBMA interface, such as an ATM interface, you must configure point-to-point or broadcast subinterfaces. IS-IS cannot run on P2MP links.

DIS and pseudonodes

IS-IS routers on a broadcast network must elect a DIS.

The Level-1 and Level-2 DISs are elected separately. You can assign different priorities to a router for different level DIS elections. The higher the router priority, the more likely the router becomes the DIS. If multiple routers with the same highest DIS priority exist, the one with the highest Subnetwork Point of Attachment (SNPA) address will be elected. On a broadcast network, the SNPA address is the MAC address. A router can be the DIS for different levels.

IS-IS DIS election differs from OSPF DIS election in the following ways:

- A router with priority 0 can also participate in the DIS election.
When a router with a higher priority is added to the network, an LSP flooding process is performed to elect the router as the new DIS.

As shown in Figure 38, the same level routers on a network, including non-DIS routers, establish adjacency with each other.

**Figure 38 DIS in the IS-IS broadcast network**

The DIS creates and updates pseudonodes, and generates LSPs for the pseudonodes, to describe all routers on the network.

A pseudonode represents a virtual node on the broadcast network. It is not a real router. In IS-IS, it is identified by the system ID of the DIS and a 1-byte Circuit ID (a non-zero value).

Using pseudonodes simplifies network topology and can reduce the amount of resources consumed by SPF.

**NOTE:**
On an IS-IS broadcast network, all routers establish adjacency relationships, but they synchronize their LSDBs through the DIS.

**IS-IS PDUs**

**PDU**

IS-IS PDUs are encapsulated into link layer frames. An IS-IS PDU has two parts, the headers and the variable length fields. The headers comprise the PDU common header and the PDU specific header. All PDUs have the same PDU common header. The specific headers vary by PDU type.

**Figure 39 PDU format**

<table>
<thead>
<tr>
<th>PDU common header</th>
<th>PDU specific header</th>
<th>Variable length fields (CLV)</th>
</tr>
</thead>
</table>

**Table 11 PDU types**

<table>
<thead>
<tr>
<th>Type</th>
<th>PDU Type</th>
<th>Acronym</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>Level-1 LAN IS-IS hello PDU</td>
<td>L1 LAN IIH</td>
</tr>
<tr>
<td>16</td>
<td>Level-2 LAN IS-IS hello PDU</td>
<td>L2 LAN IIH</td>
</tr>
<tr>
<td>17</td>
<td>Point-to-Point IS-IS hello PDU</td>
<td>P2P IIH</td>
</tr>
<tr>
<td>18</td>
<td>Level-1 Link State PDU</td>
<td>L1 LSP</td>
</tr>
<tr>
<td>20</td>
<td>Level-2 Link State PDU</td>
<td>L2 LSP</td>
</tr>
</tbody>
</table>
Hello PDU

IS-to-IS hello (IIH) PDUs are used by routers to establish and maintain neighbor relationships. On broadcast networks, Level-1 routers use Level-1 LAN IIHs, and Level-2 routers use Level-2 LAN IIHs. The P2P IIHs are used on point-to-point networks.

LSP

The LSPs carry link state information. LSPs include Level-1 LSPs and Level-2 LSPs. The Level-2 LSPs are sent by the Level-2 routers, and the Level-1 LSPs are sent by the Level-1 routers. The Level-1-2 router can send both types of LSPs.

SNP

A sequence number PDU (SNP) describes the complete or partial LSPs for LSDB synchronization.

SNPs include CSNP and PSNP, which are further divided into Level-1 CSNP, Level-2 CSNP, Level-1 PSNP, and Level-2 PSNP.

A CSNP describes the summary of all LSPs for LSDB synchronization between neighboring routers. On broadcast networks, CSNPs are sent by the DIS periodically (every 10 seconds by default). On point-to-point networks, CSNPs are sent only during the first adjacency establishment.

A PSNP only contains the sequence numbers of one or multiple latest received LSPs. It can acknowledge multiple LSPs at one time. When LSDBs are not synchronized, a PSNP is used to request missing LSPs from a neighbor.

CLV

The variable fields of PDU comprise multiple Code-Length-Value (CLV) triplets.

Figure 40 CLV format

<table>
<thead>
<tr>
<th>Code</th>
<th>Length</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Length</td>
</tr>
</tbody>
</table>

Table 12 shows that different PDUs contain different CLVs. Codes 1 through 10 are defined in ISO 10589 (code 3 and 5 are not shown in the table). Codes 128 through 132 are defined in RFC 1195. Codes 222 through 237 are defined in RFC 5120.

Table 12 CLV codes and PDU types

<table>
<thead>
<tr>
<th>CLV Code</th>
<th>Name</th>
<th>PDU Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Area Addresses</td>
<td>IIH, LSP</td>
</tr>
<tr>
<td>2</td>
<td>IS Neighbors (LSP)</td>
<td>LSP</td>
</tr>
<tr>
<td>4</td>
<td>Partition Designated Level 2 IS</td>
<td>L2 LSP</td>
</tr>
<tr>
<td>6</td>
<td>IS Neighbors (MAC Address)</td>
<td>LAN IIH</td>
</tr>
<tr>
<td>7</td>
<td>IS Neighbors (SNPA Address)</td>
<td>LAN IIH</td>
</tr>
<tr>
<td>CLV Code</td>
<td>Name</td>
<td>PDU Type</td>
</tr>
<tr>
<td>----------</td>
<td>--------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>8</td>
<td>Padding</td>
<td>IIH</td>
</tr>
<tr>
<td>9</td>
<td>LSP Entries</td>
<td>SNP</td>
</tr>
<tr>
<td>10</td>
<td>Authentication Information</td>
<td>IIH, LSP, SNP</td>
</tr>
<tr>
<td>128</td>
<td>IP Internal Reachability Information</td>
<td>LSP</td>
</tr>
<tr>
<td>129</td>
<td>Protocols Supported</td>
<td>IIH, LSP</td>
</tr>
<tr>
<td>130</td>
<td>IP External Reachability Information</td>
<td>L2 LSP</td>
</tr>
<tr>
<td>131</td>
<td>Inter-Domain Routing Protocol Information</td>
<td>L2 LSP</td>
</tr>
<tr>
<td>132</td>
<td>IP Interface Address</td>
<td>IIH, LSP</td>
</tr>
<tr>
<td>222</td>
<td>MT-ISN</td>
<td>LSP</td>
</tr>
<tr>
<td>229</td>
<td>M-Topologies</td>
<td>IIH, LSP</td>
</tr>
<tr>
<td>235</td>
<td>MT IP. Reach</td>
<td>LSP</td>
</tr>
<tr>
<td>237</td>
<td>MT IPv6 IP. Reach</td>
<td>LSP</td>
</tr>
</tbody>
</table>

**Protocols and standards**

- ISO 10589 ISO IS-IS Routing Protocol
- ISO 9542 ES-IS Routing Protocol
- ISO 8348/Ad2 Network Services Access Points
- RFC 1195, *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*
- RFC 2763, *Dynamic Hostname Exchange Mechanism for IS-IS*
- RFC 2966, *Domain-wide Prefix Distribution with Two-Level IS-IS*
- RFC 2973, *IS-IS Mesh Groups*
- RFC 3277, *IS-IS Transient Blackhole Avoidance*
- RFC 3358, *Optional Checksums in ISIS*
- RFC 3373, *Three-Way Handshake for IS-IS Point-to-Point Adjacencies*
- RFC 3719, *Recommendations for Interoperable Networks using IS-IS*
- RFC 3786, *Extending the Number of IS-IS LSP Fragments Beyond the 256 Limit*
- RFC 3787, *Recommendations for Interoperable IP Networks using IS-IS*
- RFC 3847, *Restart Signaling for IS-IS*
- RFC 5303, *Three-Way Handshake for IS-IS Point-to-Point Adjacencies*
- RFC 5310, *IS-IS Generic Cryptographic Authentication*

**Command and hardware compatibility**

Commands and descriptions for centralized devices apply to the following routers:
- MSR1002-4/1003-8S.
- MSR2003.
- MSR3012/3024/3044/3064.
- MSR958(JH300A/JH301A).

Commands and descriptions for distributed devices apply to MSR4060 and MSR4080 routers.

### IS-IS configuration task list

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configuring basic IS-IS:</strong></td>
</tr>
<tr>
<td>• (Required.) Enabling IS-IS</td>
</tr>
<tr>
<td>• (Optional.) Setting the IS level and circuit level</td>
</tr>
<tr>
<td>• (Optional.) Configuring P2P network type for an interface</td>
</tr>
<tr>
<td><strong>(Optional.) Configuring IS-IS route control:</strong></td>
</tr>
<tr>
<td>• Configuring IS-IS link cost</td>
</tr>
<tr>
<td>• Specifying a preference for IS-IS</td>
</tr>
<tr>
<td>• Configuring the maximum number of ECMP routes</td>
</tr>
<tr>
<td>• Configuring IS-IS route summarization</td>
</tr>
<tr>
<td>• Advertising a default route</td>
</tr>
<tr>
<td>• Configuring IS-IS route redistribution</td>
</tr>
<tr>
<td>• Configuring IS-IS route filtering</td>
</tr>
<tr>
<td>• Configuring IS-IS route leaking</td>
</tr>
<tr>
<td><strong>(Optional.) Tuning and optimizing IS-IS networks:</strong></td>
</tr>
<tr>
<td>• Specifying the interval for sending IS-IS hello packets</td>
</tr>
<tr>
<td>• Specifying the IS-IS hello multiplier</td>
</tr>
<tr>
<td>• Specifying the interval for sending IS-IS CSNP packets</td>
</tr>
<tr>
<td>• Configuring a DIS priority for an interface</td>
</tr>
<tr>
<td>• Enabling source address check for hello packets on a PPP interface</td>
</tr>
<tr>
<td>• Disabling an interface from sending/receiving IS-IS packets</td>
</tr>
<tr>
<td>• Enabling an interface to send small hello packets</td>
</tr>
<tr>
<td>• Configuring LSP parameters</td>
</tr>
<tr>
<td>• Controlling SPF calculation interval</td>
</tr>
<tr>
<td>• Configuring convergence priorities for specific routes</td>
</tr>
<tr>
<td>• Setting the LSDB overload bit</td>
</tr>
<tr>
<td>• Configuring the ATT bit</td>
</tr>
<tr>
<td>• Configuring the tag value for an interface</td>
</tr>
<tr>
<td>• Configuring system ID to host name mappings</td>
</tr>
<tr>
<td>• Enabling the logging of neighbor state changes</td>
</tr>
<tr>
<td>• Enabling IS-IS ISPF</td>
</tr>
<tr>
<td>• Enabling prefix suppression</td>
</tr>
<tr>
<td>• Configuring IS-IS network management</td>
</tr>
<tr>
<td>• Configuring IS-IS PIC</td>
</tr>
</tbody>
</table>
Tasks at a glance
(Optional.) Enhancing IS-IS network security:
- Configuring neighbor relationship authentication
- Configuring area authentication
- Configuring routing domain authentication

(Optional.) Configuring IS-IS GR

(Optional.) Configuring IS-IS NSR

(Optional.) Configuring BFD for IS-IS

(Optional.) Configuring IS-IS FRR

(Optional.) Configuring IS-IS MTR

Configuring basic IS-IS

Configuration prerequisites

Before the configuration, complete the following tasks:
- Configure the link layer protocol.
- Configure IP addresses for interfaces to ensure IP connectivity between neighboring nodes.

Enabling IS-IS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enable IS-IS and enter IS-IS view.</td>
<td>isis [ process-id ] [ vpn-instance vpn-instance-name ]</td>
<td>By default, IS-IS is disabled.</td>
</tr>
<tr>
<td>3. Assign a NET.</td>
<td>network-entity net</td>
<td>By default, NET is not assigned.</td>
</tr>
<tr>
<td>4. Return to system view.</td>
<td>quit</td>
<td>N/A</td>
</tr>
<tr>
<td>5. Enter interface view.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Setting the IS level and circuit level

Follow these guidelines when you configure the IS level for routers in only one area:
- Set the IS level of all routers to Level-1 or Level-2 rather than different levels because the routers do not need to maintain two identical LSDBs.
- Set the IS level to Level-2 on all routers in an IP network for good scalability.

For an interface of a Level-1 or Level-2 router, the circuit level can only be Level-1 or Level-2. For an interface of a Level-1-2 router, the default circuit level is Level-1-2. If the router only needs to form Level-1 or Level-2 neighbor relationships, set the circuit level for its interfaces to Level-1 or Level-2. This will limit neighbor relationship establishment.
To configure the IS level and circuit level:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter IS-IS view.</td>
<td>isis [ process-id ] [ vpn-instance vpn-instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Specify the IS level.</td>
<td>is-level { level-1</td>
</tr>
<tr>
<td>4.</td>
<td>Return to system view.</td>
<td>quit</td>
</tr>
<tr>
<td>5.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>6.</td>
<td>Specify the circuit level.</td>
<td>isis circuit-level [ level-1</td>
</tr>
</tbody>
</table>

Configuring P2P network type for an interface

Perform this task only for a broadcast network that has up to two attached routers.

Interfaces with different network types operate differently. For example, broadcast interfaces on a network must elect the DIS and flood CSNP packets to synchronize the LSDBs. However, P2P interfaces on a network do not need to elect the DIS, and have a different LSDB synchronization mechanism.

If only two routers exist on a broadcast network, set the network type of attached interfaces to P2P. This avoids DIS election and CSNP flooding, saving network bandwidth and speeding up network convergence.

To configure P2P network type for an interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Configure P2P network type for an interface.</td>
<td>isis circuit-type p2p</td>
</tr>
</tbody>
</table>

Configuring IS-IS route control

Configuration prerequisites

Before the configuration, complete the following tasks:

- Configure IP addresses for interfaces to ensure IP connectivity between neighboring nodes.
- Enable IS-IS.

Configuring IS-IS link cost

The IS-IS cost of an interface is determined in the following order:
1. IS-IS cost specified in interface view.
2. IS-IS cost specified in system view.
The cost is applied to the interfaces associated with the IS-IS process.
3. Automatically calculated cost.
   If the cost style is wide or wide-compatible, IS-IS automatically calculates the cost using the formula: Interface cost = (Bandwidth reference value / Expected interface bandwidth) × 10, in the range of 1 to 16777214. For other cost styles, Table 13 applies.
   Configure the expected bandwidth of an interface with the bandwidth command. For more information, see Interface Command Reference.

   Table 13 Automatic cost calculation scheme for cost styles other than wide and wide-compatible

<table>
<thead>
<tr>
<th>Interface bandwidth</th>
<th>Interface cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>≤ 10 Mbps</td>
<td>60</td>
</tr>
<tr>
<td>≤ 100 Mbps</td>
<td>50</td>
</tr>
<tr>
<td>≤ 155 Mbps</td>
<td>40</td>
</tr>
<tr>
<td>≤ 622 Mbps</td>
<td>30</td>
</tr>
<tr>
<td>≤ 2500 Mbps</td>
<td>20</td>
</tr>
<tr>
<td>&gt; 2500 Mbps</td>
<td>10</td>
</tr>
</tbody>
</table>

4. If none of the above costs is used, a default cost of 10 applies.

Configuring an IS-IS cost for an interface

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter IS-IS view.</td>
<td>isis [ process-id ] [ vpn-instance vpn-instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>(Optional.) Specify an IS-IS cost style.</td>
<td>cost-style { narrow</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the IS-IS cost type is narrow.</td>
</tr>
<tr>
<td>4.</td>
<td>Return to system view.</td>
<td>quit</td>
</tr>
<tr>
<td>5.</td>
<td>Enter interface view or IPv4 unicast topology view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td></td>
<td></td>
<td>topology ipv4 [ unicast ] topo-name</td>
</tr>
<tr>
<td>6.</td>
<td>Specify a cost for the IS-IS interface.</td>
<td>isis cost cost-value [ level-1</td>
</tr>
</tbody>
</table>

By default, no cost for the interface is specified.

Configuring a global IS-IS cost

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td></td>
<td></td>
<td>N/A</td>
</tr>
</tbody>
</table>
### Step Command Remarks

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>Enter IS-IS view or IS-IS IPv4 unicast topology view.</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• Enter IS-IS view:</td>
<td></td>
</tr>
</tbody>
</table>
|      |   ```
|      |     isis [ process-id ] [ vpn-instance vpn-instance-name ]
|      |   ``` |
|      | • Enter IS-IS IPv4 unicast topology view: | |
|      |   a. isis [ process-id ] [ vpn-instance vpn-instance-name ] | |
|      |   b. cost-style { wide | wide-compatible } | |
|      |   c. address-family ipv4 [ unicast ] | |
|      |   d. topology topo-name tid tid | |
| 3.   | Specify a global IS-IS cost. | By default, no global cost is specified. |
|      | circuit-cost cost-value [ level-1 | level-2 ] | |

### Enabling automatic IS-IS cost calculation

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Enter IS-IS view or IS-IS IPv4 unicast topology view.</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• Enter IS-IS view:</td>
<td></td>
</tr>
</tbody>
</table>
|      |   ```
|      |     isis [ process-id ] [ vpn-instance vpn-instance-name ]
|      |   ``` |
|      | • Enter IS-IS IPv4 unicast topology view: | |
|      |   a. isis [ process-id ] [ vpn-instance vpn-instance-name ] | |
|      |   b. cost-style { wide | wide-compatible } | |
|      |   c. address-family ipv4 [ unicast ] | |
|      |   d. topology topo-name tid tid | |
| 3.   | Enable automatic IS-IS cost calculation. | By default, automatic IS-IS cost calculation is disabled. |
|      | auto-cost enable | |
| 4.   | (Optional.) Configure a bandwidth reference value for automatic IS-IS cost calculation. | The default setting is 100 Mbps. |
|      | bandwidth-reference value | |

### Specifying a preference for IS-IS

If multiple routing protocols find routes to the same destination, the route found by the routing protocol that has the highest preference is selected as the optimal route.

Perform this task to assign a preference to IS-IS directly or by using a routing policy. For more information about the routing policy, see "Configuring routing policies."

To configure a preference for IS-IS:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>system-view</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring the maximum number of ECMP routes

Perform this task to implement load sharing over ECMP routes.

To configure the maximum number of ECMP routes:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>

2. Enter IS-IS IPv4 unicast address family view or IS-IS IPv4 unicast topology view.

- Enter IS-IS IPv4 unicast address family view:
  a. `isis [ process-id ] [ vpn-instance vpn-instance-name ]`
  b. `cost-style { wide | wide-compatible }`
  c. `address-family ipv4 [ unicast ]`

- Enter IS-IS IPv4 unicast topology view:
  d. `isis [ process-id ] [ vpn-instance vpn-instance-name ]`
  e. `cost-style { wide | wide-compatible }`
  f. `address-family ipv4 [ unicast ]`
  g. `topology topo-name tid tid`

3. Specify the maximum number of ECMP routes.

- `maximum load-balancing number`

By default, the maximum number of ECMP routes is 32.
Configuring IS-IS route summarization

Perform this task to summarize specific routes, including IS-IS routes and redistributed routes, into a single route. Route summarization can reduce the routing table size and the LSDB scale.

Route summarization applies only to locally generated LSPs. The cost of the summary route is the lowest one among the costs of the more-specific routes.

To configure route summarization:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
| 2.   | Enter IS-IS IPv4 unicast address family view or IS-IS IPv4 unicast topology view. | • Enter IS-IS IPv4 unicast address family view:  
  a. isis [ process-id ] [ vpn-instance vpn-instance-name ]  
  b. cost-style { wide | wide-compatible }  
  c. address-family ipv4 { unicast }  
  • Enter IS-IS IPv4 unicast topology view:  
  d. isis [ process-id ] [ vpn-instance vpn-instance-name ]  
  e. cost-style { wide | wide-compatible }  
  f. address-family ipv4 { unicast }  
  g. topology topo-name tid tid | N/A |
| 3.   | Configure IS-IS route summarization. | summary ip-address { mask-length | mask } [ avoid-feedback | generate_null0_route | [ level-1 | level-1-2 | level-2 ] | tag tag ] * | By default, route summarization is not configured. |

Advertising a default route

IS-IS cannot redistribute a default route to its neighbors. This task enables IS-IS to advertise a default route of 0.0.0.0/0 in an LSP to the same-level neighbors. Upon receiving the default route, the neighbors add it into their routing table.

To advertise a default route:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
| 2.   | Enter IS-IS IPv4 unicast address family view or IS-IS IPv4 unicast topology view. | • Enter IS-IS IPv4 unicast address family view:  
  a. isis [ process-id ] [ vpn-instance vpn-instance-name ]  
  b. cost-style { wide | wide-compatible }  
  c. address-family ipv4 { unicast }  
  • Enter IS-IS IPv4 unicast topology view:  
  d. isis [ process-id ] [ vpn-instance vpn-instance-name ]  
  e. cost-style { wide | wide-compatible }  
  f. address-family ipv4 { unicast } | N/A |
### Configuring IS-IS route redistribution

Perform this task to redistribute routes from other routing protocols into IS-IS. You can specify a cost for redistributed routes and specify the maximum number of redistributed routes.

To configure IS-IS route redistribution from other routing protocols:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td></td>
<td>Enter IS-IS IPv4 unicast address family view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>a. isis [ process-id ] [ vpn-instance vpn-instance-name ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. cost-style { wide</td>
<td>wide-compatible }</td>
</tr>
<tr>
<td></td>
<td>c. address-family ipv4 [ unicast ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter IS-IS IPv4 unicast topology view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>d. isis [ process-id ] [ vpn-instance vpn-instance-name ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>e. cost-style { wide</td>
<td>wide-compatible }</td>
</tr>
<tr>
<td></td>
<td>f. address-family ipv4 [ unicast ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>g. topology topo-name tid tid</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Enter IS-IS IPv4 unicast address family view or IS-IS IPv4 unicast topology view.</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Redistribute routes from other routing protocols or other IS-IS processes.</td>
<td>import-route protocol [ as-number ] [ process-id ] all-processes allow-ibgp ] [ allow-direct</td>
</tr>
</tbody>
</table>
### Configuring IS-IS route filtering

You can use an ACL, IP prefix list, or routing policy to filter routes calculated using received LSPs and routes redistributed from other routing protocols.

#### Filtering routes calculated from received LSPs

IS-IS saves LSPs received from neighbors in the LSDB, and uses the SPF algorithm to calculate the shortest path tree with itself as the root. IS-IS installs the calculated routes to the IS-IS routing table and the optimal routes to the IP routing table.

Perform this task to filter calculated routes. Only routes that are not filtered can be added to the IP routing table. The filtered routes retain in the IS-IS routing table and can be advertised to neighbors.

To filter routes calculated using received LSPs:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter IS-IS IPv4 unicast address family view or IS-IS IPv4 unicast topology view.</td>
<td>filter-policy { ipv4-acl-number</td>
</tr>
<tr>
<td>3.</td>
<td>Filter routes calculated using received LSPs.</td>
<td>filter-policy { ipv4-acl-number</td>
</tr>
</tbody>
</table>

#### Filtering redistributed routes

IS-IS can redistribute routes from other routing protocols or other IS-IS processes, add them to the IS-IS routing table, and advertise them in LSPs.

Perform this task to filter redistributed routes. Only routes that are not filtered can be added to the IS-IS routing table and advertised to neighbors.

To filter redistributed routes:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
### Configuring IS-IS route leaking

Perform this task to control route advertisement (route leaking) between Level-1 and Level-2. You can configure IS-IS to advertise routes from Level-2 to Level-1, and to not advertise routes from Level-1 to Level-2.

To configure IS-IS route leaking:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter IS-IS IPv4 unicast address family view or IS-IS IPv4 unicast topology view.</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Configure route leaking from Level-1 to Level-2.</td>
<td>import-route isis level-1 into level-2 [ filter-policy { ipv4-acl-number</td>
</tr>
<tr>
<td>4.</td>
<td>Configure route leaking from Level-2 to Level-1.</td>
<td>import-route isis level-2 into level-1 [ filter-policy { ipv4-acl-number</td>
</tr>
</tbody>
</table>

#### Step 2. Enter IS-IS IPv4 unicast address family view or IS-IS IPv4 unicast topology view.

- Enter IS-IS IPv4 unicast address family view:
  - isis [ process-id ] [ vpn-instance vpn-instance-name ]
  - cost-style { wide | wide-compatible }
  - address-family ipv4 [ unicast ]

- Enter IS-IS IPv4 unicast topology view:
  - isis [ process-id ] [ vpn-instance vpn-instance-name ]
  - cost-style { wide | wide-compatible }
  - address-family ipv4 [ unicast ]
  - topology topo-name tid tid

#### Step 3. Filter routes redistributed from other routing protocols or IS-IS processes.

Filter policies can be specified for each protocol or IS-IS process. The default policy is to allow all routes.

<table>
<thead>
<tr>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter-policy { ipv4-acl-number</td>
<td>prefix-list prefix-list-name</td>
</tr>
</tbody>
</table>
Tuning and optimizing IS-IS networks

Configuration prerequisites

Before you tune and optimize IS-IS networks, complete the following tasks:

- Configure IP addresses for interfaces to ensure IP connectivity between neighboring nodes.
- Enable IS-IS.

Specifying the interval for sending IS-IS hello packets

If a neighbor does not receive any hello packets from the router within the advertised hold time, it considers the router down and recalculates the routes. The hold time is the hello multiplier multiplied by the hello interval.

To specify the interval for sending hello packets:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>isis timer hello seconds [ level-1</td>
<td>level-2 ]</td>
</tr>
</tbody>
</table>

Specifying the IS-IS hello multiplier

The hello multiplier is the number of hello packets a neighbor must miss before it declares that the router is down.

If a neighbor receives no hello packets from the router within the advertised hold time, it considers the router down and recalculates the routes. The hold time is the hello multiplier multiplied by the hello interval.

On a broadcast link, Level-1 and Level-2 hello packets are advertised separately. You must set a hello multiplier for each level.

On a P2P link, Level-1 and Level-2 hello packets are advertised in P2P hello packets. You do not need to specify Level-1 or Level-2.

To specify the IS-IS hello multiplier:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>isis timer holding-multiplier value [ level-1</td>
<td>level-2 ]</td>
</tr>
</tbody>
</table>
Specifying the interval for sending IS-IS CSNP packets

On a broadcast network, perform this task on the DIS that uses CSNP packets to synchronize LSDBs.

To specify the interval for sending IS-IS CSNP packets:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Specify the interval for sending CSNP packets on the DIS of a broadcast network.</td>
<td>isis timer csnp seconds [ level-1</td>
</tr>
</tbody>
</table>

Configuring a DIS priority for an interface

On a broadcast network, IS-IS must elect a router as the DIS at a routing level. You can specify a DIS priority at a level for an interface. The greater the interface's priority, the more likely it becomes the DIS. If multiple routers in the broadcast network have the same highest DIS priority, the router with the highest MAC address becomes the DIS.

To configure a DIS priority for an interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Configure a DIS priority for the interface.</td>
<td>isis dis-priority priority [ level-1</td>
</tr>
</tbody>
</table>

Enabling source address check for hello packets on a PPP interface

An IS-IS PPP interface can have a peer on a different network. Perform this task to configure an IS-IS PPP interface to establish neighbor relationship only with a peer on the same network.

To enable source address check for hello packets on a PPP interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Enable source address check for hello packets on a PPP interface.</td>
<td>isis peer-ip-check</td>
</tr>
</tbody>
</table>
Disabling an interface from sending/receiving IS-IS packets

After being disabled from sending and receiving hello packets, an interface cannot form any neighbor relationship, but can advertise directly connected networks in LSPs through other interfaces. This can save bandwidth and CPU resources, and ensures that other routers know networks directly connected to the interface.

To disable an interface from sending and receiving IS-IS packets:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Disable the interface from sending and receiving IS-IS packets.</td>
<td>isis silent</td>
</tr>
</tbody>
</table>

Enabling an interface to send small hello packets

IS-IS messages cannot be fragmented at the IP layer because they are directly encapsulated in frames. Any two IS-IS neighboring routers must negotiate a common MTU. To avoid sending big hellos to save bandwidth, enable the interface to send small hello packets without CLVs.

To enable an interface to send small hello packets:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Enable the interface to send small hello packets without CLVs.</td>
<td>isis small-hello</td>
</tr>
</tbody>
</table>

Configuring LSP parameters

Configuring LSP timers

1. Specify the maximum age of LSPs.
   Each LSP has an age that decreases in the LSDB. Any LSP with an age of 0 is deleted from the LSDB. You can adjust the age value based on the scale of a network.

To specify the maximum age of LSPs:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter IS-IS view.</td>
<td>isis [ process-id ] [ vpn-instance vpn-instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Specify the maximum LSP age.</td>
<td>timer lsp-max-age seconds</td>
</tr>
</tbody>
</table>

2. Specify the LSP refresh interval and generation interval.
Each router needs to refresh its LSPs at a configurable interval and send them to other routers to prevent valid routes from aging out. A smaller refresh interval speeds up network convergence but consumes more bandwidth.

When network topology changes such as neighbor state, interface metric, system ID, or area ID changes occur, the router generates an LSP after a configurable interval. If such a change occurs frequently, excessive LSPs are generated, consuming a large amount of router resources and bandwidth. To solve the problem, you can adjust the LSP generation interval.

When network changes are not frequent, the minimum-interval is adopted. If network changes become frequent, the LSP generation interval is incremented by incremental-interval × 2n-2 (n is the number of calculation times) each time a generation occurs until the maximum-interval is reached.

To specify the LSP refresh interval and generation interval:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter IS-IS view.</td>
<td>isis [ process-id ] [ vpn-instance vpn-instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Specify the LSP refresh interval.</td>
<td>timer lsp-refresh seconds</td>
</tr>
</tbody>
</table>
| 4.   | Specify the LSP generation interval. | timer lsp-generation maximum-interval [ minimum-interval [ incremental-interval ] ] [ level-1 | level-2 ] | By default:  
  - The maximum interval is 5 seconds.  
  - The minimum interval is 50 milliseconds.  
  - The incremental interval is 200 milliseconds. |

3. Specify LSP sending intervals.

If a change occurs in the LSDB, IS-IS advertises the changed LSP to neighbors. You can specify the minimum interval for sending these LSPs to control the amount of LSPs on the network.

On a P2P link, IS-IS requires an advertised LSP be acknowledged. If no acknowledgment is received within a configurable interval, IS-IS will retransmit the LSP.

To configure LSP sending intervals:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Specify the minimum interval for sending LSPs and the maximum LSP number that can be sent at a time.</td>
<td>isis timer lsp time [ count count ]</td>
</tr>
<tr>
<td>4.</td>
<td>Specify the LSP retransmission interval on a P2P link.</td>
<td>isis timer retransmit seconds</td>
</tr>
</tbody>
</table>

Specifying LSP lengths

IS-IS messages cannot be fragmented at the IP layer because they are directly encapsulated in frames. IS-IS routers in an area must send LSPs smaller than the smallest interface MTU in the area.
If the IS-IS routers have different interface MTUs, configure the maximum size of generated LSP packets to be smaller than the smallest interface MTU in the area. Without the configuration, the routers must dynamically adjust the LSP packet size to fit the smallest interface MTU, which takes time and affects other services.

To specify LSP lengths:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter IS-IS view.</td>
<td>isis [ process-id ] [ vpn-instance vpn-instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Specify the maximum length of generated Level-1 LSPs or Level-2 LSPs.</td>
<td>lsp-length originate size [ level-1</td>
</tr>
<tr>
<td>4.</td>
<td>Specify the maximum length of received LSPs.</td>
<td>lsp-length receive size</td>
</tr>
</tbody>
</table>

**Enabling LSP flash flooding**

Changed LSPs can trigger SPF recalculation. To advertise the changed LSPs before the router recalculates routes for faster network convergence, enable LSP flash flooding.

To enable LSP flash flooding:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter IS-IS view.</td>
<td>isis [ process-id ] [ vpn-instance vpn-instance-name ]</td>
</tr>
</tbody>
</table>

**Enabling LSP fragment extension**

Perform this task to enable IS-IS fragment extension for an IS-IS process. The MTUs of all interfaces running the IS-IS process must not be less than 512. Otherwise, LSP fragment extension does not take effect.

To enable LSP fragment extension:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter IS-IS view.</td>
<td>isis [ process-id ] [ vpn-instance vpn-instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Enable LSP fragment extension.</td>
<td>lsp-fragments-extend [ level-1</td>
</tr>
<tr>
<td>4.</td>
<td>Configure a virtual system ID.</td>
<td>virtual-system virtual-system-id</td>
</tr>
</tbody>
</table>
Limiting LSP flooding

In NBMA networks such as ATM and FR, many P2P links exist. As shown in Figure 41, Routers A, B, C and D run IS-IS. When Router A generates an LSP, it floods the LSP out of GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3. After Router D receives the LSP from GigabitEthernet 1/0/3, it floods it out of GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to Router B and Router C. However, Router B and Router C have already received the LSP from Router A. Repeated LSP flooding consumes extra bandwidth.

Figure 41 Network diagram of a fully meshed network

To avoid this problem, you can add interfaces to a mesh group or block some interfaces.

- An interface in a mesh group floods a received LSP only to interfaces not in the mesh group.
- A blocked interface sends LSPs only after receiving LSP requests.

Before you configure this task, you must consider redundancy for interfaces in case LSP packets cannot be flooded because of link failures.

To add an interface to a mesh group or block an interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
</tbody>
</table>
| 3.   | Add the interface to a mesh group or block the interface. | • Add the interface to a mesh group: isis mesh-group mesh-group-number  
• Block the interface: isis mesh-group mesh-blocked | By default, the interface does not belong to any mesh group and is not blocked. The mesh group feature takes effect only on P2P interfaces. |

Controlling SPF calculation interval

Based on the LSDB, an IS-IS router uses the SPF algorithm to calculate the shortest path tree with itself being the root, and uses the shortest path tree to determine the next hop to a destination network. By adjusting the SPF calculation interval, you can prevent bandwidth and router resources from being over consumed due to frequent topology changes.

When network changes are not frequent, the minimum-interval is adopted. If network changes become frequent, the SPF calculation interval is incremented by incremental-interval $\times 2^{n-2}$ ($n$ is the number of calculation times) each time a calculation occurs until the maximum-interval is reached.
To control SPF calculation interval:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter IS-IS view or IS-IS IPv4 unicast address family view.</td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td>3. Configure the SPF calculation interval.</td>
<td>timer spf maximum-interval [ minimum-interval [ incremental-interval ] ]</td>
<td>By default: • The maximum interval is 5 seconds. • The minimum interval is 50 milliseconds. • The incremental interval is 200 milliseconds.</td>
</tr>
</tbody>
</table>

Configuring convergence priorities for specific routes

A topology change causes IS-IS routing convergence. To improve convergence speed, you can assign convergence priorities to IS-IS routes. Convergence priority levels are critical, high, medium, and low. The higher the convergence priority, the faster the convergence speed.

By default, IS-IS host routes have medium convergence priority, and other IS-IS routes have low convergence priority.

To assign convergence priorities to specific IS-IS routes:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter IS-IS IPv4 unicast address family view or IS-IS IPv4 unicast topology view.</td>
<td></td>
<td>N/A</td>
</tr>
</tbody>
</table>
### Assign convergence priorities to specific IS-IS routes

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
</table>
| 3.   | • Method 1: `prefix-priority { critical | high | medium } { prefix-list prefix-list-name | tag tag-value }`  
      • Method 2: `prefix-priority route-policy route-policy-name` | By default, IS-IS routes, except IS-IS host routes, have the low convergence priority. |

### Setting the LSDB overload bit

By setting the overload bit in sent LSPs, a router informs other routers of failures that make it unable to select routes and forward packets.

When an IS-IS router cannot record the complete LSDB, for example, because of memory insufficiency, it will calculate wrong routes. To make troubleshooting easier, temporarily isolate the router from the IS-IS network by setting the overload bit.

To set the LSDB overload bit:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
</tbody>
</table>
| 2.   | • Enter IS-IS view: `isis [ process-id ] [ vpn-instance vpn-instance-name ]`  
      • Enter IS-IS IPv4 unicast topology view:  
        a. `isis [ process-id ] [ vpn-instance vpn-instance-name ]`  
        b. `cost-style { wide | wide-compatible }`  
        c. `address-family ipv4 [ unicast ]`  
        d. `topology topo-name tidx tid` | N/A |

### Configuring the ATT bit

A Level-1-2 router sends Level-1 LSPs with an ATT bit to inform the Level-1 routers that it can reach other areas.

#### Configuring IS-IS not to calculate the default route through the ATT bit

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td><code>isis [ process-id ] [ vpn-instance vpn-instance-name ]</code></td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td><code>ignore-att</code></td>
<td>By default, IS-IS uses the ATT bit to calculate the default route.</td>
</tr>
</tbody>
</table>
Setting the ATT bit of Level-1 LSPs

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter IS-IS view</td>
<td>isis [ process-id ] [ vpn-instance vpn-instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Set the ATT bit of Level-1 LSPs.</td>
<td>set-att { always</td>
</tr>
</tbody>
</table>

Configuring the tag value for an interface

Perform this task when the link cost style is wide, wide-compatible, or compatible.

When IS-IS advertises a prefix with a tag value, IS-IS adds the tag to the IP reachability information TLV of the prefix.

To configure the tag value for an interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
| 2.   | Enter interface view or IPv4 unicast topology view of the interface. | • Enter interface view: interface interface-type interface-number  
• Enter IPv4 unicast topology view of the interface: a. interface interface-type interface-number  
   b. topology ipv4 [ unicast ] topo-name | N/A |
| 3.   | Configure the tag value for the interface. | isis tag tag | By default, the tag value of the interface is not configured. |

Configuring system ID to host name mappings

A 6-byte system ID in hexadecimal notation uniquely identifies a router or host in an IS-IS network. To make a system ID easy to read, the system allows you to use host names to identify devices. It also provides mappings between system IDs and host names.

The mappings can be configured manually or dynamically. Follow these guidelines when you configure the mappings:

- To view host names rather than system IDs by using the display isis lsdb command, you must enable dynamic system ID to host name mapping.
- If you configure both dynamic mapping and static mapping on a router, the host name specified for dynamic mapping applies.

Configuring a static system ID to host name mapping

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter IS-IS view.</td>
<td>isis [ process-id ] [ vpn-instance vpn-instance-name ]</td>
</tr>
</tbody>
</table>
### Configuring dynamic system ID to host name mapping

Static system ID to host name mapping requires you to manually configure a mapping for each router in the network. When a new router is added to the network or a mapping must be modified, you must configure all routers manually.

When you use dynamic system ID to host name mapping, you only need to configure a host name for each router in the network. Each router advertises the host name in a dynamic host name CLV to other routers so all routers in the network can have all mappings.

To help check the origin of LSPs in the LSDB, you can configure a name for the DIS in a broadcast network.

To configure dynamic system ID to host name mapping:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter IS-IS view.</td>
<td>isis [ process-id ] [ vpn-instance vpn-instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Specify a host name for the IS and enable dynamic system ID to host name mapping.</td>
<td>is-name sys-name</td>
</tr>
<tr>
<td>4.</td>
<td>Return to system view.</td>
<td>quit</td>
</tr>
<tr>
<td>5.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>6.</td>
<td>Configure a DIS name.</td>
<td>isis dis-name symbolic-name</td>
</tr>
</tbody>
</table>

### Enabling the logging of neighbor state changes

With this feature enabled, the router delivers logs about neighbor state changes to its information center. The information center processes the logs according to user-defined output rules (whether to output logs and where to output). For more information about the information center, see *Network Management and Monitoring Configuration Guide*.

To enable the logging of neighbor state changes:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter IS-IS view.</td>
<td>isis [ process-id ] [ vpn-instance vpn-instance-name ]</td>
</tr>
</tbody>
</table>
Enabling IS-IS ISPF

When the network topology changes, Incremental Shortest Path First (ISPF) computes only the affected part of the SPT, instead of the entire SPT.

To enable IS-IS ISPF:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter IS-IS view or IS-IS IPv4 unicast topology view.</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Enable IS-IS ISPF.</td>
<td>ispf enable</td>
</tr>
</tbody>
</table>

Enabling prefix suppression

Perform this task to disable an interface from advertising its prefix in LSPs. This enhances network security by preventing IP routing to the interval nodes and speeds up network convergence.

To enable prefix suppression:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view or IPv4 unicast topology view of the interface.</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Enable prefix suppression on the interface.</td>
<td>isis prefix-suppression</td>
</tr>
</tbody>
</table>
Configuring IS-IS network management

This task includes the following configurations:

- Bind an IS-IS process to MIB so that you can use network management software to manage the specified IS-IS process.
- Enable IS-IS notifications to report important events.

To report critical IS-IS events to an NMS, enable SNMP notifications for IS-IS. For SNMP notifications to be sent correctly, you must also configure SNMP on the device. For more information about SNMP configuration, see the network management and monitoring configuration guide for the device.

TRILL shares the standard IS-IS MIB with IS-IS. The standard IS-IS MIB provides only single-instance MIB objects. For SNMP to correctly identify TRILL's management information in the standard IS-IS MIB, you must configure a unique context for TRILL.

Context is a method introduced to SNMPv3 for multiple-instance management. For SNMPv1/v2c, you must specify a community name as a context name for protocol identification.

To configure IS-IS network management:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>isis mib-binding process-id</td>
<td>By default, MIB is bound to the IS-IS process with the smallest process ID.</td>
</tr>
<tr>
<td>4.</td>
<td>isis [ process-id ] [ vpn-instance vpn-instance-name ]</td>
<td>N/A</td>
</tr>
<tr>
<td>5.</td>
<td>snmp context-name context-name</td>
<td>By default, no context name is set for the SNMP object for managing IS-IS.</td>
</tr>
</tbody>
</table>

Configuring IS-IS PIC

Prefix Independent Convergence (PIC) enables the device to speed up network convergence by ignoring the number of prefixes.

When both IS-IS PIC and IS-IS FRR are configured, IS-IS FRR takes effect.

IS-IS PIC applies only to LSPs sent by neighbors.
Enabling IS-IS PIC

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter IS-IS view.</td>
<td>isis [ process-id ] [ vpn-instance vpn-instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Enable PIC for IS-IS.</td>
<td>pic [ additional-path-always ]</td>
</tr>
</tbody>
</table>

Enabling BFD for IS-IS PIC

By default, IS-IS PIC does not use BFD to detect primary link failures. To speed up IS-IS convergence, enable BFD for IS-IS PIC to detect primary link failures.

To enable BFD control packet mode for IS-IS PIC:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Enable BFD control packet mode for IS-IS PIC.</td>
<td>isis primary-path-detect bfd ctrl</td>
</tr>
</tbody>
</table>

To configure BFD echo packet mode for IS-IS PIC:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure the source IP address of BFD echo packets.</td>
<td>bfd echo-source-ip ip-address</td>
</tr>
<tr>
<td>3.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>4.</td>
<td>Enable BFD echo packet mode for IS-IS PIC.</td>
<td>isis primary-path-detect bfd echo</td>
</tr>
</tbody>
</table>

Enhancing IS-IS network security

To enhance the security of an IS-IS network, you can configure IS-IS authentication. IS-IS authentication involves neighbor relationship authentication, area authentication, and routing domain authentication.

Configuration prerequisites

Before the configuration, complete the following tasks:
- Configure IP addresses for interfaces to ensure IP connectivity between neighboring nodes.
- Enable IS-IS.

**Configuring neighbor relationship authentication**

With neighbor relationship authentication configured, an interface adds the key in the specified mode into hello packets to the peer and checks the key in the received hello packets. If the authentication succeeds, it forms the neighbor relationship with the peer.

The authentication mode and key at both ends must be identical.

To prevent packet exchange failure in case of an authentication key change, configure the interface not to check the authentication information in the received packets.

To configure neighbor relationship authentication:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Specify the authentication mode and key.</td>
<td>isis authentication-mode { { gca key-id</td>
</tr>
<tr>
<td>4.</td>
<td>(Optional.) Configure the interface not to check the authentication information in the received hello packets.</td>
<td>isis authentication send-only [ level-1</td>
</tr>
</tbody>
</table>

**Configuring area authentication**

Area authentication prevents the router from installing routing information from untrusted routers into the Level-1 LSDB. The router encapsulates the authentication key in the specified mode in Level-1 packets (LSP, CSNP, and PSNP). It also checks the key in received Level-1 packets.

Routers in a common area must have the same authentication mode and key.

To prevent packet exchange failure in case of an authentication key change, configure IS-IS not to check the authentication information in the received packets.

To configure area authentication:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter IS-IS view.</td>
<td>isis [ process-id ] [ vpn-instance vpn-instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Specify the area authentication mode and key.</td>
<td>area-authentication-mode { { gca key-id</td>
</tr>
</tbody>
</table>
Configuring routing domain authentication

Routing domain authentication prevents untrusted routing information from entering into a routing domain. A router with the authentication configured encapsulates the key in the specified mode into Level-2 packets (LSP, CSNP, and PSNP) and check the key in received Level-2 packets.

All the routers in the backbone must have the same authentication mode and key.

To prevent packet exchange failure in case of an authentication key change, configure IS-IS not to check the authentication information in the received packets.

To configure routing domain authentication:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter IS-IS view.</td>
<td>isis [ process-id ] [ vpn-instance vpn-instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Specify the routing domain authentication mode and key.</td>
<td>domain-authentication-mode { { gca key-id { hmac-sha-1</td>
</tr>
<tr>
<td>4.</td>
<td>(Optional.) Configure the interface not to check the authentication information in the received Level-2 packets, including LSPs, CSNPs, and PSNPs.</td>
<td>domain-authentication send-only</td>
</tr>
</tbody>
</table>

Configuring IS-IS GR

GR ensures forwarding continuity when a routing protocol restarts or an active/standby switchover occurs.

Two routers are required to complete a GR process. The following are router roles in a GR process.

- **GR restarter**—Graceful restarting router. It must have GR capability.
- **GR helper**—A neighbor of the GR restarter. It assists the GR restarter to complete the GR process. By default, the device acts as the GR helper.

Configure IS-IS GR on the GR restarter.

GR restarter uses the following timers:
• **T1 timer**—Specifies the times that GR restarter can send a Restart TLV with the RR bit set. When rebooted, the GR restarter sends a Restart TLV with the RR bit set to its neighbor. If the GR restarter receives a Restart TLV with the RA set from its neighbor before the T1 timer expires, the GR process starts. Otherwise, the GR process fails.

• **T2 timer**—Specifies the LSDB synchronization interval. Each LSDB has a T2 timer. The Level-1-2 router has a Level-1 timer and a Level-2 timer. If the LSDBs have not synchronized before the two timers expire, the GR process fails.

• **T3 timer**—Specifies the GR interval. The GR interval is set as the holdtime in hello PDUs. Within the interval, the neighbors maintain their adjacency with the GR restarter. If the GR process has not completed within the holdtime, the neighbors tear down the neighbor relationship and the GR process fails.

**IMPORTANT:**
IS-IS GR and IS-IS NSR are mutually exclusive. Do not configure them at the same time.

To configure GR on the GR restarter:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable IS-IS and enter IS-IS view.</td>
<td>isis [process-id] [vpn-instance vpn-instance-name]</td>
</tr>
<tr>
<td>3.</td>
<td>Enable IS-IS GR.</td>
<td>graceful-restart</td>
</tr>
<tr>
<td>4.</td>
<td>(Optional.) Suppress the SA bit during restart.</td>
<td>graceful-restart suppress-sa</td>
</tr>
<tr>
<td>5.</td>
<td>(Optional.) Configure the T1 timer.</td>
<td>graceful-restart t1 seconds count</td>
</tr>
<tr>
<td>6.</td>
<td>(Optional.) Configure the T2 timer.</td>
<td>graceful-restart t2 seconds</td>
</tr>
<tr>
<td>7.</td>
<td>(Optional.) Configure the T3 timer.</td>
<td>graceful-restart t3 seconds</td>
</tr>
</tbody>
</table>

**Configuring IS-IS NSR**

The following matrix shows the feature and hardware compatibility:

<table>
<thead>
<tr>
<th>Hardware</th>
<th>IS-IS NSR compatibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSR954(JH296A/JH297A/JH298A/JH299A/JH373A)</td>
<td>No</td>
</tr>
<tr>
<td>MSR958(JH300A/JH301A)</td>
<td>No</td>
</tr>
</tbody>
</table>
| MSR1002-4/1003-8S | • In standalone mode: No  
• In IRF mode: Yes |
| MSR2003 | • In standalone mode: No  
• In IRF mode: Yes |
Hardware | IS-IS NSR compatibility
---|---
MSR2004-24/2004-48 | • In standalone mode: No  
                   • In IRF mode: Yes
MSR3012/3024/3044/3064 | • In standalone mode: No  
                          • In IRF mode: Yes
MSR4060/4080 | Yes

After an active/standby switchover, the GR restarter obtains routing information from its neighbors, and the IS-IS process must learn all the routes. If the network topology changes during the switchover, removed routes cannot be updated to the device, which can result in blackhole routes.

NSR solves the problem by backing up IS-IS link state information from the active process to the standby process. After an active/standby switchover, NSR can complete link state recovery and route regeneration without requiring the cooperation of other devices.

**IMPORTANT:**
IS-IS NSR and IS-IS GR are mutually exclusive. Do not configure them at the same time.

To configure IS-IS NSR:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter IS-IS view.</td>
<td>isis [ process-id ] [ vpn-instance vpn-instance-name ]</td>
<td>N/A</td>
</tr>
<tr>
<td>3. Enable IS-IS NSR.</td>
<td>non-stop-routing</td>
<td>By default, IS-IS NSR is disabled. IS-IS NSR takes effect on a per-process basis. As a best practice, enable NSR for each IS-IS process.</td>
</tr>
</tbody>
</table>

**Configuring BFD for IS-IS**

BFD provides a single mechanism to quickly detect and monitor the connectivity of links between IS-IS neighbors, reducing network convergence time. For more information about BFD, see *High Availability Configuration Guide*.

To configure BFD for IS-IS:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter interface view.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3. Enable IS-IS on an interface.</td>
<td>isis enable [ process-id ]</td>
<td>N/A</td>
</tr>
<tr>
<td>4. Enable BFD on an IS-IS interface.</td>
<td>isis bfd enable</td>
<td>By default, an IS-IS interface is not enabled with BFD.</td>
</tr>
</tbody>
</table>
Configuring IS-IS FRR

A link or router failure on a path can cause packet loss and routing loop. IS-IS FRR enables fast rerouting to minimize the failover time.

**Figure 42 Network diagram for IS-IS FRR**

In Figure 42, after you enable FRR on Router B, IS-IS automatically calculates or designates a backup next hop when a link failure is detected. In this way, packets are directed to the backup next hop to reduce traffic recovery time. Meanwhile, IS-IS calculates the shortest path based on the new network topology, and forwards packets over the path after network convergence.

You can assign a backup next hop for IS-IS FRR through the following ways:

- Enable IS-IS FRR to calculate a backup next hop through Loop Free Alternate (LFA) calculation.
- Designate a backup next hop with a routing policy for routes matching specific criteria.

**Configuration prerequisites**

Before you configure IS-IS FRR, complete the following tasks:

- Configure IP addresses for interfaces to ensure IP connectivity between neighboring nodes.
- Enable IS-IS.

**Configuration guidelines**

The LFA calculation of FRR and that of TE are mutually exclusive.

**Configuration procedure**

**Configuring IS-IS FRR to calculate a backup next hop through LFA calculation**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
| 2.   | Enter interface view or IPv4 unicast topology view of the interface. | • Enter interface view: interface interface-type interface-number  
• Enter IPv4 unicast topology view of the interface:  
  a. interface interface-type interface-number  
  b. topology ipv4 [ unicast ] topo-name | N/A |
| 3.   | (Optional.) Disable LFA calculation on the interface. | isis fast-reroute lfa-backup exclude | By default, the interface participates in LFA calculation, and can be elected as a backup |
### Configuring IS-IS FRR using a routing policy

You can use the `apply fast-reroute backup-interface` command to specify a backup next hop in a routing policy for routes matching specific criteria. You can also perform this task to reference the routing policy for IS-IS FRR. For more information about the `apply fast-reroute backup-interface` command and routing policy configurations, see "Configuring routing policies."

To configure IS-IS FRR using a routing policy:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view or IPv4 unicast topology view of the interface.</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• Enter interface view: interface interface-type interface-number</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter IPv4 unicast topology view of the interface:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>a. interface interface-type interface-number</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. topology ipv4 [ unicast ] topo-name</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>(Optional.) Disable LFA calculation on the interface.</td>
<td>By default, the interface participates in LFA calculation, and can be elected as a backup interface.</td>
</tr>
<tr>
<td></td>
<td>isis fast-reroute lfa-backup exclude</td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>Return to system view.</td>
<td>To return to system view from IPv4 unicast topology view of the interface, execute the <code>quit</code> command twice.</td>
</tr>
</tbody>
</table>

### Configuring IS-IS IPv4 unicast topology view or IS-IS IPv4 unicast topology view

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.</td>
<td>Return to system view.</td>
<td>To return to system view from IPv4 unicast topology view of the interface, execute the <code>quit</code> command twice.</td>
</tr>
<tr>
<td>5.</td>
<td>Enter IS-IS IPv4 unicast address family view or IS-IS IPv4 unicast topology view.</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• Enter IS-IS IPv4 unicast address family view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>a. isis [ process-id ] [ vpn-instance vpn-instance-name ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. cost-style { wide</td>
<td>wide-compatible }</td>
</tr>
<tr>
<td></td>
<td>c. address-family ipv4 [ unicast ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter IS-IS IPv4 unicast topology view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>d. isis [ process-id ] [ vpn-instance vpn-instance-name ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>e. cost-style { wide</td>
<td>wide-compatible }</td>
</tr>
<tr>
<td></td>
<td>f. address-family ipv4 [ unicast ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>g. topology topo-name tid tid</td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>Enable IS-IS FRR to calculate a backup next hop through LFA calculation.</td>
<td>By default, IS-IS FRR is disabled.</td>
</tr>
<tr>
<td></td>
<td>fast-reroute lfa</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| 5.   | - Enter IS-IS IPv4 unicast address family view or IS-IS IPv4 unicast topology view. | • Enter IS-IS IPv4 unicast address family view:  
  a. `isis [ process-id ] [ vpn-instance vpn-instance-name ]` 
  b. `cost-style { wide | wide-compatible }`  
  c. `address-family ipv4 [ unicast ]`  
  - Enter IS-IS IPv4 unicast topology view:  
  d. `isis [ process-id ] [ vpn-instance vpn-instance-name ]`  
  e. `cost-style { wide | wide-compatible }`  
  f. `address-family ipv4 [ unicast ]`  
  g. `topology topo-name tid tid` | N/A |
| 6.   | Enable IS-IS FRR using a routing policy. | `fast-reroute route-policy route-policy-name` | By default, this feature is not enabled. |

### Enabling BFD for IS-IS FRR

By default, IS-IS FRR does not use BFD to detect primary link failures. To speed up IS-IS convergence, enable BFD for IS-IS FRR to detect primary link failures.

To enable BFD control packet mode for IS-IS FRR:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td><code>interface interface-type interface-number</code></td>
</tr>
<tr>
<td>3.</td>
<td>Enable BFD control packet mode for IS-IS FRR.</td>
<td><code>isis primary-path-detect bfd ctrl</code></td>
</tr>
</tbody>
</table>

To enable BFD echo packet mode for IS-IS FRR:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
</tbody>
</table>
| 2.   | Configure the source IP address of BFD echo packets. | `bfd echo-source-ip ip-address` | By default, the source IP address of BFD echo packets is not configured.  
The source IP address cannot be on the same network segment as any local interface's IP address.  
For more information, see High Availability Command Reference. |
| 3.   | Enter interface view. | `interface interface-type interface-number` | N/A |
| 4.   | Enable BFD echo packet mode for IS-IS FRR. | `isis primary-path-detect bfd echo` | By default, BFD echo packet mode is disabled for IS-IS FRR. |
Configuring IS-IS MTR

Typically, service packets with the same destination are forwarded over the same link. To forward them over different links, you can use one of the following methods:

- Policy-based routing (PBR). Use PBR to change the next hop.
- Traffic engineering (TE).
- Multi-Topology Routing (MTR).

MTR is based on topology and is easier to deploy than TE. MTR splits the topology of a specific address family (for example, IPv4) into multiple topologies, and forwards traffic on a per-topology basis.

For more information about IPv6 IS-IS MTR, see "Configuring IPv6 IS-IS."

**Figure 43 Network diagram**

As shown in Figure 43, the base topology is split into two topologies, topology A and topology B. You can forward voice traffic through topology A and video traffic through topology B.

Router B does not belong to topology A. In topology B, the links between Router A and Router D and the links between Router B and Router C do not exist. Route calculation and traffic forwarding are performed in each topology independently.

**Configuration prerequisites**

Before you configure IPv4 IS-IS MTR, complete the following tasks:

- Configure basic IS-IS to establish IS-IS neighbor relationships.
- Configure MTR. For more information, see "Configuring MTR."

**Configuration procedure**

To configure IS-IS MTR:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter IS-IS view.</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td></td>
<td>isis [ process-id ] [ vpn-instance ] [ vpn-instance-name ]</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>3.</td>
<td>Specify an IS-IS cost style.</td>
<td><strong>cost-style</strong> { <strong>wide</strong></td>
</tr>
<tr>
<td>4.</td>
<td>Enter IPv4 address family view.</td>
<td><strong>address-family ipv4</strong> [ <strong>unicast</strong> ] &lt;br&gt; N/A</td>
</tr>
<tr>
<td>5.</td>
<td>Create a IS-IS IPv4 unicast topology and enter its view.</td>
<td><strong>topology</strong> <strong>topo-name</strong> <strong>tid</strong> <strong>tid</strong> &lt;br&gt; By default, no IS-IS IPv4 unicast topologies exist. By default, IS-IS does not support any IPv4 unicast topology.</td>
</tr>
<tr>
<td>6.</td>
<td>Return to system view.</td>
<td><strong>quit</strong> &lt;br&gt; To return to system view from IPv4 address family view, execute the <strong>quit</strong> command three times.</td>
</tr>
<tr>
<td>7.</td>
<td>Enter interface view.</td>
<td><strong>interface</strong> <strong>interface-type</strong> <strong>interface-number</strong> &lt;br&gt; N/A</td>
</tr>
<tr>
<td>8.</td>
<td>Enter IPv4 unicast topology view.</td>
<td><strong>topology ipv4</strong> [ <strong>unicast</strong> ] <strong>topo-name</strong> &lt;br&gt; N/A</td>
</tr>
<tr>
<td>9.</td>
<td>Enable IS-IS for the specified topology on the interface.</td>
<td><strong>isis topology enable</strong> &lt;br&gt; By default, IS-IS is disabled for the topology.</td>
</tr>
</tbody>
</table>

### Displaying and maintaining IS-IS

Execute **display** commands in any view and the **reset** command in user view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display IS-IS process information.</td>
<td><strong>display isis</strong> [ <strong>process-id</strong> ]</td>
</tr>
<tr>
<td>Display IS-IS GR log information (centralized devices in standalone mode).</td>
<td><strong>display isis graceful-restart event-log</strong></td>
</tr>
<tr>
<td>Display IS-IS GR log information (distributed devices in standalone mode/centralized devices in IRF mode).</td>
<td><strong>display isis graceful-restart event-log slot</strong> <strong>slot-number</strong></td>
</tr>
<tr>
<td>Display IS-IS GR log information (distributed devices in IRF mode).</td>
<td><strong>display isis graceful-restart event-log chassis</strong> <strong>chassis-number</strong> <strong>slot</strong> <strong>slot-number</strong></td>
</tr>
<tr>
<td>Display the IS-IS GR status.</td>
<td><strong>display isis graceful-restart status</strong> [ <strong>level-1</strong></td>
</tr>
<tr>
<td>Display IS-IS interface information.</td>
<td><strong>display isis interface</strong> [ [ <strong>interface-type</strong> <strong>interface-number</strong> ] [ <strong>verbose</strong> ]</td>
</tr>
<tr>
<td>Display IS-IS LSDB information.</td>
<td><strong>display isis lsdb</strong> [ [ <strong>level-1</strong></td>
</tr>
<tr>
<td>Display IS-IS mesh group information.</td>
<td><strong>display isis mesh-group</strong> [ <strong>process-id</strong> ]</td>
</tr>
<tr>
<td>Display the host name to system ID mapping table.</td>
<td><strong>display isis name-table</strong> [ <strong>process-id</strong> ]</td>
</tr>
<tr>
<td>Display IS-IS NSR log information (distributed devices in standalone mode/centralized devices in IRF mode).</td>
<td><strong>display isis non-stop-routing event-log slot</strong> <strong>slot-number</strong></td>
</tr>
<tr>
<td>Task</td>
<td>Command</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Display IS-IS NSR log information (distributed devices in IRF mode).</td>
<td><code>display isis non-stop-routing event-log chassis chassis-number slot slot-number</code></td>
</tr>
<tr>
<td>Display the IS-IS NSR status.</td>
<td><code>display isis non-stop-routing status</code></td>
</tr>
<tr>
<td>Display IS-IS neighbor information.</td>
<td>`display isis neighbor [ statistics</td>
</tr>
<tr>
<td>Display IS-IS redistributed route information.</td>
<td>`display isis redistribute [ ipv4 [ topology topo-name ] [ ip-address mask-length ] ] [ level-1</td>
</tr>
<tr>
<td>Display IS-IS IPv4 routing information.</td>
<td>`display isis route [ ipv4 [ topology topo-name ] [ ip-address mask-length ] ] [ [ level-1</td>
</tr>
<tr>
<td>Display IS-IS IPv4 topology information.</td>
<td>`display isis spf-tree [ ipv4 [ topology topo-name ] ] [ [ level-1</td>
</tr>
<tr>
<td>Display IS-IS statistics.</td>
<td>`display isis statistics [ ipv4 [ topology topo-name ] ] [ [ level-1</td>
</tr>
<tr>
<td>Display OSI connection information (centralized devices in standalone mode).</td>
<td><code>display osi</code></td>
</tr>
<tr>
<td>Display OSI connection information (distributed devices in standalone mode/centralized devices in IRF mode).</td>
<td><code>display osi [ slot slot-number ]</code></td>
</tr>
<tr>
<td>Display OSI connection information (distributed devices in IRF mode).</td>
<td><code>display osi [ chassis chassis-number slot slot-number ]</code></td>
</tr>
<tr>
<td>Display OSI connection statistics (centralized devices in standalone mode).</td>
<td><code>display osi statistics</code></td>
</tr>
<tr>
<td>Display OSI connection statistics (distributed devices in standalone mode/centralized devices in IRF mode).</td>
<td><code>display osi statistics [ slot slot-number ]</code></td>
</tr>
<tr>
<td>Display OSI connection statistics (distributed devices in IRF mode).</td>
<td><code>display osi statistics [ chassis chassis-number slot slot-number ]</code></td>
</tr>
<tr>
<td>Clear IS-IS process data structure information.</td>
<td><code>reset isis all [ process-id ] [ graceful-restart ]</code></td>
</tr>
<tr>
<td>Clear IS-IS GR log information (distributed devices in standalone mode).</td>
<td><code>reset isis graceful-restart event-log</code></td>
</tr>
<tr>
<td>Clear IS-IS GR log information (distributed devices in standalone mode/centralized devices in IRF mode).</td>
<td><code>reset isis graceful-restart event-log slot slot-number</code></td>
</tr>
<tr>
<td>Clear IS-IS GR log information (distributed devices in IRF mode).</td>
<td><code>reset isis graceful-restart event-log chassis chassis-number slot slot-number</code></td>
</tr>
<tr>
<td>Clear IS-IS NSR log information (distributed devices in IRF mode).</td>
<td><code>reset isis non-stop-routing event-log slot slot-number</code></td>
</tr>
<tr>
<td>Clear IS-IS NSR log information (distributed devices in IRF mode).</td>
<td><code>reset isis non-stop-routing event-log chassis chassis-number slot slot-number</code></td>
</tr>
<tr>
<td>Clear the data structure information of an IS-IS neighbor.</td>
<td><code>reset isis peer system-id [ process-id ]</code></td>
</tr>
<tr>
<td>Clear OSI connection statistics.</td>
<td><code>reset osi statistics</code></td>
</tr>
</tbody>
</table>
IS-IS configuration examples

Basic IS-IS configuration example

Network requirements

As shown in Figure 44, Router A, Router B, Router C, and Router D reside in an AS.

Router A and Router B are Level-1 routers, Router D is a Level-2 router, and Router C is a Level-1-2 router connecting two areas. Router A, Router B, and Router C are in area 10, and Router D is in area 20.

Figure 44 Network diagram

Configuration procedure

1. Configure IP addresses for interfaces. (Details not shown.)
2. Configure IS-IS:
   # Configure Router A
   <RouterA> system-view
   [RouterA] isis 1
   [RouterA-isis-1] is-level level-1
   [RouterA-isis-1] network-entity 10.0000.0000.0001.00
   [RouterA-isis-1] quit
   [RouterA] interface gigabitethernet 1/0/1
   [RouterA-GigabitEthernet1/0/1] isis enable 1
   [RouterA-GigabitEthernet1/0/1] quit
   # Configure Router B.
   <RouterB> system-view
   [RouterB] isis 1
   [RouterB-isis-1] is-level level-1
   [RouterB-isis-1] network-entity 10.0000.0000.0002.00
   [RouterB-isis-1] quit
   [RouterB] interface gigabitethernet 1/0/1
   [RouterB-GigabitEthernet1/0/1] isis enable 1
   [RouterB-GigabitEthernet1/0/1] quit
   # Configure Router C.
<RouterC> system-view
[RouterC] isis 1
[RouterC-isis-1] network-entity 10.0000.0000.0003.00
[RouterC-isis-1] quit
[RouterC] interface gigabitethernet 1/0/3
[RouterC-GigabitEthernet1/0/3] isis enable 1
[RouterC-GigabitEthernet1/0/3] quit
[RouterC] interface gigabitethernet 1/0/1
[RouterC-GigabitEthernet1/0/1] isis enable 1
[RouterC-GigabitEthernet1/0/1] quit
[RouterC] interface gigabitethernet 1/0/2
[RouterC-GigabitEthernet1/0/2] isis enable 1
[RouterC-GigabitEthernet1/0/2] quit

# Configure Router D
<RouterD> system-view
[RouterD] isis 1
[RouterD-isis-1] is-level level-2
[RouterD-isis-1] network-entity 20.0000.0000.0004.00
[RouterD-isis-1] quit
[RouterD] interface gigabitethernet 1/0/1
[RouterD-GigabitEthernet1/0/1] isis enable 1
[RouterD-GigabitEthernet1/0/1] quit
[RouterD] interface gigabitethernet 1/0/2
[RouterD-GigabitEthernet1/0/2] isis enable 1
[RouterD-GigabitEthernet1/0/2] quit

Verifying the configuration

# Display the IS-IS LSDB information.
[RouterA] display isis lsdb

Database information for ISIS(1)
---------------------------------
Level-1 Link State Database
---------------------------------

<table>
<thead>
<tr>
<th>LSPID</th>
<th>Seq Num</th>
<th>Checksum</th>
<th>Holdtime</th>
<th>Length</th>
<th>ATT/P/OL</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000.0000.0000.0001.00-00*</td>
<td>0x000000004</td>
<td>0xdf5e</td>
<td>1096</td>
<td>68</td>
<td>0/0/0</td>
</tr>
<tr>
<td>0000.0000.0000.0000.00-00</td>
<td>0x000000004</td>
<td>0xee4d</td>
<td>1102</td>
<td>68</td>
<td>0/0/0</td>
</tr>
<tr>
<td>0000.0000.0000.0002.01-00</td>
<td>0x000000001</td>
<td>0xdaaf</td>
<td>1102</td>
<td>55</td>
<td>0/0/0</td>
</tr>
<tr>
<td>0000.0000.0000.0003.00-00</td>
<td>0x000000009</td>
<td>0xc3a3</td>
<td>1161</td>
<td>111</td>
<td>1/0/0</td>
</tr>
<tr>
<td>0000.0000.0000.0003.01-00</td>
<td>0x000000001</td>
<td>0xaadda</td>
<td>1112</td>
<td>55</td>
<td>0/0/0</td>
</tr>
</tbody>
</table>

*-Self LSP, +-Self LSP(Extended), ATT-Attached, P-Partition, OL-Overload

[RouterB] display isis lsdb

Database information for ISIS(1)
---------------------------------
**Level-1 Link State Database**

<table>
<thead>
<tr>
<th>LSPID</th>
<th>Seq Num</th>
<th>Checksum</th>
<th>Holdtime</th>
<th>Length</th>
<th>ATT/P/OL</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000.0000.0001.00-00</td>
<td>0x00000006</td>
<td>0xdb60</td>
<td>988</td>
<td>68</td>
<td>0/0/0</td>
</tr>
<tr>
<td>0000.0000.0002.00-00*</td>
<td>0x00000008</td>
<td>0xe651</td>
<td>1189</td>
<td>68</td>
<td>0/0/0</td>
</tr>
<tr>
<td>0000.0000.0002.01-00*</td>
<td>0x00000005</td>
<td>0xd2b3</td>
<td>1188</td>
<td>55</td>
<td>0/0/0</td>
</tr>
<tr>
<td>0000.0000.0003.00-00</td>
<td>0x00000014</td>
<td>0x194a</td>
<td>1190</td>
<td>111</td>
<td>1/0/0</td>
</tr>
<tr>
<td>0000.0000.0003.01-00</td>
<td>0x00000002</td>
<td>0xabdb</td>
<td>995</td>
<td>55</td>
<td>0/0/0</td>
</tr>
</tbody>
</table>

*Self LSP, +Self LSP(Extended), ATT-Attached, P-Partition, OL-Overload

[RouterC] display isis lsdb

**Database information for ISIS(1)**

**Level-1 Link State Database**

<table>
<thead>
<tr>
<th>LSPID</th>
<th>Seq Num</th>
<th>Checksum</th>
<th>Holdtime</th>
<th>Length</th>
<th>ATT/P/OL</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000.0000.0001.00-00</td>
<td>0x00000006</td>
<td>0xdb60</td>
<td>847</td>
<td>68</td>
<td>0/0/0</td>
</tr>
<tr>
<td>0000.0000.0002.00-00</td>
<td>0x00000008</td>
<td>0xe651</td>
<td>1053</td>
<td>68</td>
<td>0/0/0</td>
</tr>
<tr>
<td>0000.0000.0002.01-00</td>
<td>0x00000005</td>
<td>0xd2b3</td>
<td>1052</td>
<td>55</td>
<td>0/0/0</td>
</tr>
<tr>
<td>0000.0000.0003.00-00*</td>
<td>0x00000014</td>
<td>0x194a</td>
<td>1051</td>
<td>111</td>
<td>1/0/0</td>
</tr>
<tr>
<td>0000.0000.0003.01-00*</td>
<td>0x00000002</td>
<td>0xabdb</td>
<td>854</td>
<td>55</td>
<td>0/0/0</td>
</tr>
</tbody>
</table>

*Self LSP, +Self LSP(Extended), ATT-Attached, P-Partition, OL-Overload

**Level-2 Link State Database**

<table>
<thead>
<tr>
<th>LSPID</th>
<th>Seq Num</th>
<th>Checksum</th>
<th>Holdtime</th>
<th>Length</th>
<th>ATT/P/OL</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000.0000.0003.00-00*</td>
<td>0x00000012</td>
<td>0xc93c</td>
<td>842</td>
<td>100</td>
<td>0/0/0</td>
</tr>
<tr>
<td>0000.0000.0004.00-00</td>
<td>0x00000026</td>
<td>0x331</td>
<td>1173</td>
<td>84</td>
<td>0/0/0</td>
</tr>
<tr>
<td>0000.0000.0004.01-00</td>
<td>0x00000001</td>
<td>0xee95</td>
<td>668</td>
<td>55</td>
<td>0/0/0</td>
</tr>
</tbody>
</table>

*Self LSP, +Self LSP(Extended), ATT-Attached, P-Partition, OL-Overload

[RouterD] display isis lsdb

**Database information for ISIS(1)**

**Level-2 Link State Database**

177
LSPID                 Seq Num      Checksum      Holdtime      Length  ATT/P/OL
-------------------------------------------------------------------------
0000.0000.0003.00-00  0x00000013   0xc73d        1003          100     0/0/0
0000.0000.0004.00-00* 0x0000003c   0xd647        1194          84      0/0/0
0000.0000.0004.01-00* 0x00000002   0xec96        1007          55      0/0/0

*-Self LSP, +Self LSP(Extended), ATT-Attached, P-Partition, OL-Overload

# Display the IS-IS routing information on each router.

[RouterA] display isis route

Route information for IS-IS(1)
-------------------------------

Level-1 IPv4 Forwarding Table
-------------------------------

IPv4 Destination     IntCost    ExtCost ExitInterface   NextHop         Flags
-------------------------------------------------------------------------------
10.1.1.0/24          10         NULL    GE1/0/1         Direct          D/L/-
10.1.2.0/24          20         NULL    GE1/0/1         10.1.1.1        R/-/-
192.168.0.0/24       20         NULL    GE1/0/1         10.1.1.1        R/-/-
0.0.0.0/0            10         NULL    GE1/0/1         10.1.1.1        R/-/-

Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set

[RouterC] display isis route

Route information for IS-IS(1)
-------------------------------

Level-1 IPv4 Forwarding Table
-------------------------------

IPv4 Destination     IntCost    ExtCost ExitInterface   NextHop         Flags
-------------------------------------------------------------------------------
10.1.1.0/24          10         NULL    GE1/0/1         Direct          D/L/-
10.1.2.0/24          10         NULL    GE1/0/3         Direct          D/L/-
192.168.0.0/24       10         NULL    GE1/0/2         Direct          D/L/-

Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set

Level-2 IPv4 Forwarding Table
-------------------------------

IPv4 Destination     IntCost    ExtCost ExitInterface   NextHop         Flags
-------------------------------------------------------------------------------
10.1.1.0/24          10         NULL      Direct          D/L/-
10.1.2.0/24          10         NULL      Direct          D/L/-
10.1.2.0/24          10         NULL      Direct          D/L/-
192.168.0.0/24  10       NULL      D/L/-
172.16.0.0/16   20       NULL      GE1/0/2  192.168.0.2  R/-/-

Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set

[RouterD] display isis route

Route information for IS-IS(1)

-------------------------------

Level-2 IPv4 Forwarding Table
-------------------------------

<table>
<thead>
<tr>
<th>IPv4 Destination</th>
<th>IntCost</th>
<th>ExtCost</th>
<th>ExitInterface</th>
<th>NextHop</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.0/24</td>
<td>10</td>
<td>NULL</td>
<td>GE1/0/2</td>
<td>Direct</td>
<td>D/L/-</td>
</tr>
<tr>
<td>10.1.1.0/24</td>
<td>20</td>
<td>NULL</td>
<td>GE1/0/2</td>
<td>192.168.0.1</td>
<td>R/-/-</td>
</tr>
<tr>
<td>10.1.2.0/24</td>
<td>20</td>
<td>NULL</td>
<td>GE1/0/2</td>
<td>192.168.0.1</td>
<td>R/-/-</td>
</tr>
<tr>
<td>172.16.0.0/16</td>
<td>10</td>
<td>NULL</td>
<td>GE1/0/1</td>
<td>Direct</td>
<td>D/L/-</td>
</tr>
</tbody>
</table>

Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set

The output shows that the routing table of Level-1 routers contains a default route with the next hop as the Level-1-2 router. The routing table of Level-2 router contains all Level-1 and Level-2 routes.

DIS election configuration example

Network requirements

As shown in Figure 45, on a broadcast network (Ethernet), Router A, Router B, Router C, and Router D reside in IS-IS Area 10. Router A and Router B are Level-1-2 routers, Router C is a Level-1 router, and Router D is a Level-2 router.

Change the DIS priority of Router A to make it elected as the Level-1-2 DIS router.

Figure 45 Network diagram
Configuration procedure

1. Configure IP addresses for interfaces. (Details not shown.)

2. Enable IS-IS:

   # Configure Router A.
   <RouterA> system-view
   [RouterA] isis 1
   [RouterA-isis-1] network-entity 10.0000.0000.0001.00
   [RouterA-isis-1] quit
   [RouterA] interface gigabitethernet 1/0/1
   [RouterA-GigabitEthernet1/0/1] isis enable 1
   [RouterA-GigabitEthernet1/0/1] quit

   # Configure Router B.
   <RouterB> system-view
   [RouterB] isis 1
   [RouterB-isis-1] network-entity 10.0000.0000.0002.00
   [RouterB-isis-1] quit
   [RouterB] interface gigabitethernet 1/0/1
   [RouterB-GigabitEthernet1/0/1] isis enable 1
   [RouterB-GigabitEthernet1/0/1] quit

   # Configure Router C.
   <RouterC> system-view
   [RouterC] isis 1
   [RouterC-isis-1] network-entity 10.0000.0000.0003.00
   [RouterC-isis-1] is-level level-1
   [RouterC-isis-1] quit
   [RouterC] interface gigabitethernet 1/0/1
   [RouterC-GigabitEthernet1/0/1] isis enable 1
   [RouterC-GigabitEthernet1/0/1] quit

   # Configure Router D.
   <RouterD> system-view
   [RouterD] isis 1
   [RouterD-isis-1] network-entity 10.0000.0000.0004.00
   [RouterD-isis-1] is-level level-2
   [RouterD-isis-1] quit
   [RouterD] interface gigabitethernet 1/0/1
   [RouterD-GigabitEthernet1/0/1] isis enable 1
   [RouterD-GigabitEthernet1/0/1] quit

   # Display information about IS-IS neighbors of Router A.
   [RouterA] display isis peer

       Peer information for IS-IS(1)
                        ------------------------
        System Id: 0000.0000.0002
       Interface: GigabitEthernet1/0/1          Circuit Id: 0000.0000.0003.01
                      State: Up       HoldTime: 21s      Type: L1(L1L2)    PRI: 64
        System Id: 0000.0000.0003
Interface: GigabitEthernet1/0/1              Circuit Id: 0000.0000.0003.01
State: Up     HoldTime: 6s     Type: L1     PRI: 64
System Id: 0000.0000.0002

Interface: GigabitEthernet1/0/1              Circuit Id: 0000.0000.0004.01
State: Up     HoldTime: 23s    Type: L2(L1L2)     PRI: 64
System Id: 0000.0000.0004

# Display information about IS-IS interfaces of Router A.
[RouterA] display isis interface

Interface information for IS-IS(1)
---------------------------------
Interface: GigabitEthernet1/0/1
Index     IPv4.State      IPv6.State     CircuitID   MTU   Type   DIS
00001     Up              Down           1           1497  L1/L2  No/No

# Display IS-IS interfaces of Router C.
[RouterC] display isis interface

Interface information for IS-IS(1)
---------------------------------
Interface: GigabitEthernet1/0/1
Index     IPv4.State      IPv6.State     CircuitID   MTU   Type   DIS
00001     Up              Down           1           1497  L1/L2  Yes/No

# Display information about IS-IS interfaces of Router D.
[RouterD] display isis interface

Interface information for IS-IS(1)
---------------------------------
Interface: GigabitEthernet1/0/1
Index     IPv4.State      IPv6.State     CircuitID   MTU   Type   DIS
00001     Up              Down           1           1497  L1/L2  No/Yes

The output shows that when the default DIS priority is used, Router C is the DIS for Level-1, and Router D is the DIS for Level-2. The pseudonodes of Level-1 and Level-2 are 0000.0000.0003.01 and 0000.0000.0004.01.

# Configure the DIS priority of Router A.
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] isis dis-priority 100

# Display information about IS-IS neighbors of Router A.
[RouterA] display isis peer

Peer information for IS-IS(1)
-----------------------------

181
System Id: 0000.0000.0002
Interface: GigabitEthernet1/0/1                  Circuit Id: 0000.0000.0001.01
State: Up            HoldTime: 29s          Type: L1(L1L2)   PRI: 64

System Id: 0000.0000.0003
Interface: GigabitEthernet1/0/1                  Circuit Id: 0000.0000.0001.01
State: Up            HoldTime: 22s          Type: L1          PRI: 64

System Id: 0000.0000.0004
Interface: GigabitEthernet1/0/1                  Circuit Id: 0000.0000.0001.01
State: Up            HoldTime: 22s          Type: L2          PRI: 64

# Display information about IS-IS interfaces of Router A.
[RouterA] display isis interface

    Interface information for IS-IS(1)
    ---------------------------------
    Interface: GigabitEthernet1/0/1
    Index  IPv4.State  IPv6.State  CircuitID  MTU  Type DIS
    00001     Up        Down           1       1497  L1/L2 Yes/Yes

The output shows that after the DIS priority configuration, Router A becomes the DIS for Level-1-2, and the pseudonode is 0000.0000.0001.01.

# Display information about IS-IS neighbors and interfaces of Router C.
[RouterC] display isis peer

    Peer information for IS-IS(1)
    -----------------------------
    System Id: 0000.0000.0001
    Interface: GigabitEthernet1/0/1                  Circuit Id: 0000.0000.0001.01
    State: Up            HoldTime: 7s          Type: L1          PRI: 100

    System Id: 0000.0000.0002
    Interface: GigabitEthernet1/0/1                  Circuit Id: 0000.0000.0001.01
    State: Up            HoldTime: 23s          Type: L1          PRI: 64

[RouterC] display isis interface

    Interface information for IS-IS(1)
    ---------------------------------
    Interface: GigabitEthernet1/0/1
    Index  IPv4.State  IPv6.State  CircuitID  MTU  Type DIS
    00  1     Up        Down           1       1497  L1/L2 No/No
IS-IS route redistribution configuration example

Network requirements

As shown in Figure 46, Router A, Router B, Router C, and Router D reside in the same AS. They use IS-IS to interconnect. Router A and Router B are Level-1 routers, Router D is a Level-2 router, and Router C is a Level-1-2 router.

Redistribute RIP routes into IS-IS on Router D.

Figure 46 Network diagram
Configure Router A.

```
<RouterA> system-view
[RouterA] isis 1
[RouterA-isis-1] is-level level-1
[RouterA-isis-1] network-entity 10.0000.0000.0001.00
[RouterA-isis-1] quit
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] isis enable 1
[RouterA-GigabitEthernet1/0/1] quit
```

# Configure Router B.

```
<RouterB> system-view
[RouterB] isis 1
[RouterB-isis-1] is-level level-1
[RouterB-isis-1] network-entity 10.0000.0000.0002.00
[RouterB-isis-1] quit
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] isis enable 1
[RouterB-GigabitEthernet1/0/1] quit
```

# Configure Router C.

```
<RouterC> system-view
[RouterC] isis 1
[RouterC-isis-1] network-entity 10.0000.0000.0003.00
[RouterC-isis-1] quit
[RouterC] interface gigabitethernet 1/0/1
[RouterC-GigabitEthernet1/0/1] isis enable 1
[RouterC-GigabitEthernet1/0/1] quit
[RouterC] interface gigabitethernet 1/0/2
[RouterC-GigabitEthernet1/0/2] isis enable 1
[RouterC-GigabitEthernet1/0/2] quit
[RouterC] interface gigabitethernet 1/0/3
[RouterC-GigabitEthernet1/0/3] isis enable 1
[RouterC-GigabitEthernet1/0/3] quit
```

# Configure Router D.

```
<RouterD> system-view
[RouterD] isis 1
[RouterD-isis-1] is-level level-2
[RouterD-isis-1] network-entity 20.0000.0000.0004.00
[RouterD-isis-1] quit
[RouterD] interface gigabitethernet 1/0/1
[RouterD-GigabitEthernet1/0/1] isis enable 1
[RouterD-GigabitEthernet1/0/1] quit
[RouterD] interface gigabitethernet 1/0/2
[RouterD-GigabitEthernet1/0/2] isis enable 1
[RouterD-GigabitEthernet1/0/2] quit
[RouterD] interface gigabitethernet 1/0/2
[RouterD-GigabitEthernet1/0/2] isis enable 1
[RouterD-GigabitEthernet1/0/2] quit
```

# Display IS-IS routing information on each router.

```
[RouterA] display isis route
```
Route information for IS-IS(1)
-------------------------------

**Level-1 IPv4 Forwarding Table**
-------------------------------

<table>
<thead>
<tr>
<th>IPv4 Destination</th>
<th>IntCost</th>
<th>ExtCost</th>
<th>ExitInterface</th>
<th>NextHop</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.1.0/24</td>
<td>10</td>
<td>NULL</td>
<td>GE1/0/1</td>
<td>Direct</td>
<td>D/L/-</td>
</tr>
<tr>
<td>10.1.2.0/24</td>
<td>20</td>
<td>NULL</td>
<td>GE1/0/1</td>
<td>10.1.1.1</td>
<td>R/-/-</td>
</tr>
<tr>
<td>192.168.0.0/24</td>
<td>20</td>
<td>NULL</td>
<td>GE1/0/1</td>
<td>10.1.1.1</td>
<td>R/-/-</td>
</tr>
<tr>
<td>0.0.0.0/0</td>
<td>10</td>
<td>NULL</td>
<td>GE1/0/1</td>
<td>10.1.1.1</td>
<td>R/-/-</td>
</tr>
</tbody>
</table>

Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set

[RouterC] display isis route

Route information for IS-IS(1)
-------------------------------

**Level-1 IPv4 Forwarding Table**
-------------------------------

<table>
<thead>
<tr>
<th>IPv4 Destination</th>
<th>IntCost</th>
<th>ExtCost</th>
<th>ExitInterface</th>
<th>NextHop</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.1.0/24</td>
<td>10</td>
<td>NULL</td>
<td>GE1/0/1</td>
<td>Direct</td>
<td>D/L/-</td>
</tr>
<tr>
<td>10.1.2.0/24</td>
<td>10</td>
<td>NULL</td>
<td>GE1/0/3</td>
<td>Direct</td>
<td>D/L/-</td>
</tr>
<tr>
<td>192.168.0.0/24</td>
<td>10</td>
<td>NULL</td>
<td>GE1/0/2</td>
<td>Direct</td>
<td>D/L/-</td>
</tr>
</tbody>
</table>

Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set

Level-2 IPv4 Forwarding Table
-------------------------------

<table>
<thead>
<tr>
<th>IPv4 Destination</th>
<th>IntCost</th>
<th>ExtCost</th>
<th>ExitInterface</th>
<th>NextHop</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.1.0/24</td>
<td>10</td>
<td>NULL</td>
<td></td>
<td>D/L/-</td>
<td></td>
</tr>
<tr>
<td>10.1.2.0/24</td>
<td>10</td>
<td>NULL</td>
<td></td>
<td>D/L/-</td>
<td></td>
</tr>
<tr>
<td>192.168.0.0/24</td>
<td>10</td>
<td>NULL</td>
<td></td>
<td>D/L/-</td>
<td></td>
</tr>
</tbody>
</table>

Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set

[RouterD] display isis route

Route information for IS-IS(1)
-------------------------------

Level-2 IPv4 Forwarding Table
-------------------------------
3. Configure RIPv2 on Router D and Router E, and configure IS-IS to redistribute RIP routes on Router D:

# Configure RIPv2 on Router D.
[RouterD] rip 1
[RouterD-rip-1] network 10.0.0.0
[RouterD-rip-1] version 2
[RouterD-rip-1] undo summary

# Configure RIPv2 on Router E.
[RouterE] rip 1
[RouterE-rip-1] network 10.0.0.0
[RouterE-rip-1] version 2
[RouterE-rip-1] undo summary

# On Router D, configure IS-IS to redistribute routes from RIP.
[RouterD-rip-1] quit
[RouterD] isis 1
[RouterD-isis-1] address-family ipv4

# Display IS-IS routing information on Router C.
[RouterC] display isis route

Route information for IS-IS(1)

Level-1 IPv4 Forwarding Table

<table>
<thead>
<tr>
<th>IPv4 Destination</th>
<th>IntCost</th>
<th>ExtCost</th>
<th>ExitInterface</th>
<th>NextHop</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.1.0/24</td>
<td>10</td>
<td>NULL</td>
<td>GE1/0/1</td>
<td>Direct</td>
<td>D/L/-</td>
</tr>
<tr>
<td>10.1.2.0/24</td>
<td>10</td>
<td>NULL</td>
<td>GE1/0/3</td>
<td>Direct</td>
<td>D/L/-</td>
</tr>
<tr>
<td>192.168.0.0/24</td>
<td>10</td>
<td>NULL</td>
<td>GE1/0/2</td>
<td>Direct</td>
<td>D/L/-</td>
</tr>
</tbody>
</table>

Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set

Level-2 IPv4 Forwarding Table

<table>
<thead>
<tr>
<th>IPv4 Destination</th>
<th>IntCost</th>
<th>ExtCost</th>
<th>ExitInterface</th>
<th>NextHop</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.1.0/24</td>
<td>10</td>
<td>NULL</td>
<td></td>
<td></td>
<td>D/L/-</td>
</tr>
</tbody>
</table>

Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set
IS-IS authentication configuration example

Network requirements

As shown in Figure 47, Router A, Router B, Router C, and Router D reside in the same IS-IS routing domain.

Router A, Router B, and Router C belong to Area 10, and Router D belongs to Area 20.

- Configure neighbor relationship authentication between neighbors.
- Configure area authentication in Area 10 to prevent untrusted routes from entering into the area.
- Configure routing domain authentication on Router C and Router D to prevent untrusted routes from entering the routing domain.

Figure 47 Network diagram

Configuration procedure

1. Configure IP addresses for interfaces. (Details not shown.)
2. Configure basic IS-IS:
   # Configure Router A.
   <RouterA> system-view
   [RouterA] isis 1
   [RouterA-isis-1] network-entity 10.0000.0000.0001.00
   [RouterA-isis-1] is-level level-1
   [RouterA-isis-1] quit
   [RouterA] interface gigabitethernet 1/0/1
   [RouterA-GigabitEthernet1/0/1] isis enable 1
   [RouterA-GigabitEthernet1/0/1] quit
   # Configure Router B.
<RouterB> system-view
[RouterB] isis 1
[RouterB-isis-1] network-entity 10.0000.0000.0002.00
[RouterB-isis-1] is-level level-1
[RouterB-isis-1] quit
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] isis enable 1
[RouterB-GigabitEthernet1/0/1] quit

# Configure Router C.
<RouterC> system-view
[RouterC] isis 1
[RouterC-isis-1] network-entity 10.0000.0000.0003.00
[RouterC-isis-1] quit
[RouterC] interface gigabitethernet 1/0/1
[RouterC-GigabitEthernet1/0/1] isis enable 1
[RouterC-GigabitEthernet1/0/1] quit
[RouterC] interface gigabitethernet 1/0/2
[RouterC-GigabitEthernet1/0/2] isis enable 1
[RouterC-GigabitEthernet1/0/2] quit
[RouterC] interface gigabitethernet 1/0/3
[RouterC-GigabitEthernet1/0/3] isis enable 1
[RouterC-GigabitEthernet1/0/3] quit

# Configure Router D.
<RouterD> system-view
[RouterD] isis 1
[RouterD-isis-1] network-entity 20.0000.0000.0001.00
[RouterD-isis-1] quit
[RouterD] interface gigabitethernet 1/0/1
[RouterD-GigabitEthernet1/0/1] isis enable 1
[RouterD-GigabitEthernet1/0/1] quit

3. Configure neighbor relationship authentication between neighbors:

# Set the authentication mode to MD5 and set the plaintext key to eRq on GigabitEthernet 1/0/1
of Router A and on GigabitEthernet 1/0/3 of Router C.
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] isis authentication-mode md5 plain eRg
[RouterA-GigabitEthernet1/0/1] quit
[RouterC] interface gigabitethernet 1/0/3
[RouterC-GigabitEthernet1/0/3] isis authentication-mode md5 plain eRg
[RouterC-GigabitEthernet1/0/3] quit

# Set the authentication mode to MD5 and set the plaintext key to t5Hr on GigabitEthernet 1/0/1
of Router B and on GigabitEthernet 1/0/1 of Router C.
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] isis authentication-mode md5 plain t5Hr
[RouterB-GigabitEthernet1/0/1] quit
[RouterC] interface gigabitethernet 1/0/1
[RouterC-GigabitEthernet1/0/1] isis authentication-mode md5 plain t5Hr
[RouterC-GigabitEthernet1/0/1] quit
# Set the authentication mode to MD5 and set the plaintext key to hSec on GigabitEthernet 1/0/1 of Route D and on GigabitEthernet 1/0/2 of Router C.

[RouterC-GigabitEthernet1/0/2] isis authentication-mode md5 plain hSec
[RouterD-GigabitEthernet1/0/1] isis authentication-mode md5 plain hSec

4. Set the area authentication mode to MD5 and set the plaintext key to 10Sec on Router A, Router B, and Router C.

[RouterA-isis-1] area-authentication-mode md5 plain 10Sec
[RouterB-isis-1] area-authentication-mode md5 plain 10Sec
[RouterC-isis-1] area-authentication-mode md5 plain 10Sec

5. Set routing domain authentication mode to MD5 and set the plaintext key to 1020Sec on Router C and Router D.

[RouterC-isis-1] domain-authentication-mode md5 plain 1020Sec
[RouterD-isis-1] domain-authentication-mode md5 plain 1020Sec

IS-IS GR configuration example

Network requirements

As shown in Figure 48, Router A, Router B, and Router C belong to the same IS-IS routing domain. Run IS-IS on all the routers to interconnect them with each other.

Figure 48 Network diagram

Configuration procedure

1. Configure the IP addresses and subnet masks for interfaces on the routers. (Details not shown.)
2. Configure IS-IS on the routers to make sure Router A, Router B, and Router C can communicate with each other at Layer 3 and dynamic route update can be implemented among them with IS-IS. (Details not shown.)

3. Enable IS-IS GR on Router A.

   <RouterA> system-view
   [RouterA] isis 1
   [RouterA-isis-1] graceful-restart
   [RouterA-isis-1] return

Verifying the configuration

   # Restart the IS-IS process on Router A.
   <RouterA> reset isis all 1 graceful-restart
   Reset IS-IS process? [Y/N]: y

   # Check the GR state of the IS-IS process on Router A.
   <RouterA> display isis graceful-restart status

   Restart information for IS-IS(1)
   --------------------------------
   Restart status: COMPLETE
   Restart phase: Finish
   Restart t1: 3, count 10; Restart t2: 60; Restart t3: 300
   SA Bit: supported

   Level-1 restart information
   ---------------------------
   Total number of interfaces: 1
   Number of waiting LSPs: 0

   Level-2 restart information
   ---------------------------
   Total number of interfaces: 1
   Number of waiting LSPs: 0

IS-IS NSR configuration example

Network requirements

As shown in Figure 49, Router S, Router A, and Router B belong to the same IS-IS routing domain.
- Run IS-IS on all the routers to interconnect them with each other.
- Enable IS-IS NSR on Router S to ensure forwarding continuity between Router A and Router B when an active/standby switchover occurs on Router S.

Figure 49 Network diagram
Configuration procedure

1. Configure the IP addresses and subnet masks for interfaces on the routers. (Details not shown.)

2. Configure IS-IS on the routers to make sure Router S, Router A, and Router B can communicate with each other at Layer 3 and dynamic route update can be implemented among them with IS-IS. (Details not shown.)

3. Enable IS-IS NSR on Router S.

   <RouterS> system-view
   [RouterS] isis 1
   [RouterS-isis-1] non-stop-routing
   [RouterS-isis-1] return

Verifying the configuration

# Reoptimize process placement on Router S to trigger an active/standby switchover.

   <RouterS> system-view
   [RouterS] placement reoptimize

Predicted changes to the placement

<table>
<thead>
<tr>
<th>Program</th>
<th>Current location</th>
<th>New location</th>
</tr>
</thead>
<tbody>
<tr>
<td>syslog</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>diagusageratio</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>l3vpn</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>fc</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>dns</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>lauth</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>aaa</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>lsm</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>rm</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>rm6</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>track</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>ip6addr</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>ipaddr</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>rpm</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>trange</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>tunnel</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>lagg</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>bfd</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>acl</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>slsp</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>usr6</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>usr</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>qos</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>fczone</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>ethbase</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>ipcim</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>ip6base</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>ipbase</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>eth</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>eviisis</td>
<td>0/0</td>
<td>0/0</td>
</tr>
</tbody>
</table>
ifnet                           NA                     NA
isis                              0/0                    1/0
Continue? [y/n]: y
Re-optimization of the placement start. You will be notified on completion
Re-optimization of the placement complete. Use 'display placement' to view the new placement

# During the switchover period, display IS-IS neighbor information on Router A to verify the neighborhood between Router A and Router S.
<RouterA> display isis peer

Peer information for IS-IS(1)
-----------------------------

System Id: 0000.0000.0001
Interface: GE1/0/1            Circuit Id: 0000.0000.0001.01
State: Up    HoldTime:  23s   Type: L1(L1L2)    PRI: 64

System Id: 0000.0000.0001
Interface: GE1/0/1            Circuit Id: 0000.0000.0001.01
State: Up    HoldTime:  28s   Type: L2(L1L2)    PRI: 64

# Display IS-IS routing information on Router A to verify that Router A has a route to the loopback interface of Router B.
<RouterA> display isis route

Route information for IS-IS(1)
-------------------------------

Level-1 IPv4 Forwarding Table
-------------------------------

IPv4 Destination     IntCost ExtCost ExitInterface   NextHop          Flags
-------------------------------------------------------------------------------
12.12.12.0/24        10      NULL    GE1/0/1         Direct          D/L/-
22.22.22.22/32       10      NULL    Loop0           Direct          D/-/-
44.44.44.44/32       10      NULL    GE1/0/1         12.12.12.2      R/L/-

Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set

Level-2 IPv4 Forwarding Table
-------------------------------

IPv4 Destination     IntCost ExtCost ExitInterface   NextHop          Flags
-------------------------------------------------------------------------------
12.12.12.0/24        10      NULL    GE1/0/1         Direct          D/L/-
22.22.22.22/32       10      NULL    Loop0           Direct          D/-/-
44.44.44.44/32        10      NULL
# Display IS-IS neighbor information on Router B to verify the neighborship between Router B and Router S.

```bash
<RouterB> display isis peer

Peer information for IS-IS(1)
---------------------------
System Id: 0000.0000.0001
Interface: GE1/0/1                  Circuit Id: 0000.0000.0001.01
State: Up     HoldTime:  23s       Type: L1(L1L2)     PRI: 64

System Id: 0000.0000.0001
Interface: GE1/0/1                  Circuit Id: 0000.0000.0001.01
State: Up     HoldTime:  28s       Type: L2(L1L2)     PRI: 64
```

# Display IS-IS routing information on Router B to verify that Router B has a route to the loopback interface of Router A.

```bash
<RouterB> display isis route

Route information for IS-IS(1)
-----------------------------
Level-1 IPv4 Forwarding Table
-----------------------------
IPv4 Destination     IntCost    ExtCost ExitInterface   NextHop         Flags
-------------------------------------------------------------------------------
14.14.14.0/24        10         NULL    GE1/0/1         Direct          D/L/-
44.44.44.44/32       10         NULL    Loop0           Direct          D/-/-
22.22.22.22/32       10         NULL    GE1/0/1         14.14.14.4      R/L/-

Level-2 IPv4 Forwarding Table
-------------------------------
IPv4 Destination     IntCost    ExtCost ExitInterface   NextHop         Flags
-------------------------------------------------------------------------------
14.14.14.0/24        10         NULL    GE1/0/1         Direct          D/L/-
44.44.44.44/32       10         NULL    Loop0           Direct          D/-/-
12.12.12.0/32        10         NULL
22.22.22.22/32       10         NULL
```

Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set
The output shows that the neighbor information and routing information on Router A and Router B have not changed during the active/standby switchover on Router S. The neighbors are unaware of the switchover.

BFD for IS-IS configuration example

Network requirements

- As shown in Figure 50, run IS-IS on Router A, Router B and Router C so that they can reach each other at the network layer.
- After the link over which Router A and Router B communicate through the Layer 2 switch fails, BFD can quickly detect the failure and notify IS-IS of the failure. Router A and Router B then communicate through Router C.

Figure 50 Network diagram

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router A</td>
<td>GE1/0/1</td>
<td>192.168.0.102/24</td>
<td>Router B</td>
<td>GE1/0/1</td>
<td>192.168.0.100/24</td>
</tr>
<tr>
<td></td>
<td>GE1/0/2</td>
<td>10.1.1.102/24</td>
<td></td>
<td>GE1/0/2</td>
<td>13.1.1.1/24</td>
</tr>
<tr>
<td></td>
<td>Loop0</td>
<td>121.1.1.1/32</td>
<td></td>
<td>Loop0</td>
<td>120.1.1.1/32</td>
</tr>
<tr>
<td>Router C</td>
<td>GE1/0/1</td>
<td>10.1.1.100/24</td>
<td></td>
<td>GE1/0/2</td>
<td>13.1.1.2/24</td>
</tr>
</tbody>
</table>

Configuration procedure

1. Configure IP addresses for interfaces. (Details not shown.)
2. Configure basic IS-IS:
   
   # Configure Router A.
   
   <RouterA> system-view
   [RouterA] isis
   [RouterA-isis-1] network-entity 10.0000.0000.0001.00
   [RouterA-isis-1] quit
   [RouterA] interface loopback 0
   [RouterA-LoopBack0] isis enable
   [RouterA-LoopBack0] quit
   [RouterA] interface gigabitethernet 1/0/1
   [RouterA-GigabitEthernet1/0/1] isis enable
   [RouterA-GigabitEthernet1/0/1] quit
   [RouterA] interface gigabitethernet 1/0/2
# Configure Router B.

<RouterB> system-view
[RouterB] isis
[RouterB-isis-1] network-entity 10.0000.0000.0002.00
[RouterB-isis-1] quit
[RouterB] interface loopback 0
[RouterB-LoopBack0] isis enable
[RouterB-LoopBack0] quit
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] isis enable
[RouterB-GigabitEthernet1/0/1] quit
[RouterB] interface gigabitethernet 1/0/2
[RouterB-GigabitEthernet1/0/2] isis enable
[RouterB-GigabitEthernet1/0/2] quit

# Configure Router C.

<RouterC> system-view
[RouterC] isis
[RouterC-isis-1] network-entity 10.0000.0000.0003.00
[RouterC-isis-1] quit
[RouterC] interface gigabitethernet 1/0/1
[RouterC-GigabitEthernet1/0/1] isis enable
[RouterC-GigabitEthernet1/0/1] quit
[RouterC] interface gigabitethernet 1/0/2
[RouterC-GigabitEthernet1/0/2] isis enable
[RouterC-GigabitEthernet1/0/2] quit

3. Configure BFD functions:

# Enable BFD and configure BFD parameters on Router A.

[RouterA] bfd session init-mode active
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] isis bfd enable
[RouterA-GigabitEthernet1/0/1] bfd min-receive-interval 500
[RouterA-GigabitEthernet1/0/1] bfd min-transmit-interval 500
[RouterA-GigabitEthernet1/0/1] bfd detect-multiplier 7

# Enable BFD and configure BFD parameters on Router B.

[RouterB] bfd session init-mode active
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] isis bfd enable
[RouterB-GigabitEthernet1/0/1] bfd min-receive-interval 500
[RouterB-GigabitEthernet1/0/1] bfd min-transmit-interval 500
[RouterB-GigabitEthernet1/0/1] bfd detect-multiplier 8

Verifying the configuration

# Display the BFD session information on Router A.

<RouterA> display bfd session

Total Session Num: 1     Up Session Num: 1     Init Mode: Active
IPv4 Session Working Under Ctrl Mode:

<table>
<thead>
<tr>
<th>LD/RD</th>
<th>SourceAddr</th>
<th>DestAddr</th>
<th>State</th>
<th>Holdtime</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>3/1</td>
<td>192.168.0.102</td>
<td>192.168.0.100</td>
<td>Up</td>
<td>1700ms</td>
<td>GE1/0/1</td>
</tr>
</tbody>
</table>

# Display routes destined for 120.1.1.1/32 on Router A.

```
<RouterA> display ip routing-table 120.1.1.1 verbose
```

Summary Count : 1

Destination: 120.1.1.1/32
Protocol: IS_L1
Process ID: 1

SubProtID: 0x1   Age: 04h20m37s
Cost: 10        Preference: 10
IpPre: N/A      QosLocalID: N/A
Tag: 0          State: Active Adv
OrigTblID: 0x0  OrigVrf: default-vrf
TableID: 0x2
NibID: 0x26000002  LastAs: 0
AttrID: 0xffffffff Neighbor: 0.0.0.0
Flags: 0x1008c  OrigNextHop: 192.168.0.100
Label: NULL     RealNextHop: 192.168.0.100
BkLabel: NULL   BkNextHop: N/A
Tunnel ID: Invalid Interface: GigabitEthernet1/0/1
BkTunnel ID: Invalid BkInterface: N/A
FtnIndex: 0x0   TrafficIndex: N/A
Connector: N/A

The output shows that Router A and Router B communicate through Ethernet 1/1. Then the link over Ethernet 1/1 fails.

# Display routes destined for 120.1.1.1/32 on Router A.

```
<RouterA> display ip routing-table 120.1.1.1 verbose
```

Summary Count : 1

Destination: 120.1.1.1/32
Protocol: IS_L1
Process ID: 1

SubProtID: 0x1   Age: 04h20m37s
Cost: 20        Preference: 10
IpPre: N/A      QosLocalID: N/A
Tag: 0          State: Active Adv
OrigTblID: 0x0  OrigVrf: default-vrf
TableID: 0x2
NibID: 0x26000002  LastAs: 0
AttrID: 0xffffffff Neighbor: 0.0.0.0
Flags: 0x1008c  OrigNextHop: 10.1.1.100
Label: NULL     RealNextHop: 10.1.1.100
BkLabel: NULL   BkNextHop: N/A
Tunnel ID: Invalid Interface: GigabitEthernet1/0/1
BkTunnel ID: Invalid BkInterface: N/A
FtnIndex: 0x0   TrafficIndex: N/A
Connector: N/A
The output shows that Router A and Router B communicate through Ethernet 1/2.

IS-IS FRR configuration example

Network requirements

As shown in Figure 51, Router A, Router B, and Router C reside in the same IS-IS routing domain.

- Run IS-IS on all the routers to interconnect them with each other.
- Configure IS-IS FRR so that when Link A fails, traffic can be switched to Link B immediately.

Figure 51 Network diagram

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router A</td>
<td>GE1/0/1</td>
<td>12.12.12.1/24</td>
<td>Router B</td>
<td>GE1/0/1</td>
<td>24.24.24.4/24</td>
</tr>
<tr>
<td></td>
<td>GE1/0/2</td>
<td>13.13.13.1/24</td>
<td></td>
<td>GE1/0/2</td>
<td>13.13.13.2/24</td>
</tr>
<tr>
<td></td>
<td>Loop0</td>
<td>1.1.1.1/32</td>
<td></td>
<td>Loop0</td>
<td>4.4.4.4/32</td>
</tr>
<tr>
<td>Router C</td>
<td>GE1/0/1</td>
<td>12.12.12.2/24</td>
<td></td>
<td>GE1/0/2</td>
<td>24.24.24.2/24</td>
</tr>
</tbody>
</table>

Configuration procedure

1. Configure IP addresses and subnet masks for interfaces on the routers. (Details not shown.)
2. Configure IS-IS on the routers to make sure Router A, Router B, and Router C can communicate with each other at the network layer. (Details not shown.)
3. Configure IS-IS FRR:
   - Enable IS-IS FRR to calculate a backup next hop through LFA calculation, or designate a backup next hop by using a routing policy.
   - (Method 1.) Enable IS-IS FRR to calculate a backup next hop through LFA calculation:
     
     ```
     # Configure Router A.
     <RouterA> system-view
     [RouterA] isis 1
     [RouterA-isis-1] address-family ipv4
     [RouterA-isis-1-ipv4] fast-reroute lfa
     [RouterA-isis-1-ipv4] quit
     [RouterA-isis-1] quit
     ```
   - # Configure Router B.
(Method 2.) Enable IS-IS FRR to designate a backup next hop by using a routing policy:

# Configure Router A.

```
<RouterA> system-view
[RouterA] ip prefix-list abc index 10 permit 4.4.4.4 32
[RouterA] route-policy frr permit node 10
[RouterA-route-policy-frr-10] if-match ip address prefix-list abc
[RouterA-route-policy-frr-10] quit
[RouterA] isis 1
[RouterA-isis-1] address-family ipv4
[RouterA-isis-1-ipv4] quit
[RouterA-isis-1] quit
```

# Configure Router B.

```
<RouterB> system-view
[RouterB] ip prefix-list abc index 10 permit 1.1.1.1 32
[RouterB] route-policy frr permit node 10
[RouterB-route-policy-frr-10] if-match ip address prefix-list abc
[RouterB-route-policy-frr-10] apply fast-reroute backup-interface gigabitethernet 1/0/1 backup-nexthop 24.24.24.2
[RouterB-route-policy-frr-10] quit
[RouterB] isis 1
[RouterB-isis-1] address-family ipv4
[RouterB-isis-1-ipv4] fast-reroute route-policy frr
[RouterB-isis-1-ipv4] quit
[RouterB-isis-1] quit
```

Verifying the configuration

# Display route 4.4.4.4/32 on Router A to view the backup next hop information.

```
[RouterA] display ip routing-table 4.4.4.4 verbose

Summary Count : 1

Destination: 4.4.4.4/32
 Protocol: IS_L1
 Process ID: 1
 SubProtID: 0x1 Age: 04h20m37s
 Cost: 10 Preference: 10
 IpPre: N/A QosLocalID: N/A
 Tag: 0 State: Active Adv
 OrigTb1ID: 0x0 OrigVrf: default-vrf
 TableID: 0x2 OrigAs: 0
```
<table>
<thead>
<tr>
<th>NibID</th>
<th>0x26000002</th>
<th>LastAs: 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>AttrID</td>
<td>0xffffffff</td>
<td>Neighbor: 0.0.0.0</td>
</tr>
<tr>
<td>Flags</td>
<td>0x1008c</td>
<td>OrigNextHop: 13.13.13.2</td>
</tr>
<tr>
<td>Label</td>
<td>NULL</td>
<td>RealNextHop: 13.13.13.2</td>
</tr>
<tr>
<td>BkLabel</td>
<td>NULL</td>
<td>BkNextHop: 12.12.12.2</td>
</tr>
<tr>
<td>Tunnel ID</td>
<td>Invalid</td>
<td>Interface: GigabitEthernet1/0/2</td>
</tr>
<tr>
<td>BkTunnel ID</td>
<td>Invalid</td>
<td>BkInterface: GigabitEthernet1/0/1</td>
</tr>
<tr>
<td>FtnIndex</td>
<td>0x0</td>
<td>TrafficIndex: N/A</td>
</tr>
<tr>
<td>Connector</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

# Display route 1.1.1.1/32 on Router B to view the backup next hop information.

[RouterB] display ip routing-table 1.1.1.1 verbose

Summary Count : 1

Destination: 1.1.1.1/32
  Protocol: IS_L1
  Process ID: 1
  SubProtID: 0x1  Age: 04h20m37s
  Cost: 10  Preference: 10
  IpPre: N/A  QosLocalID: N/A
  Tag: 0  State: Active Adv
  OrigTblID: 0x0  OrigVrf: default-vrf
  TableID: 0x2  OrigAs: 0
  NibID: 0x26000002  LastAs: 0
  AttrID: 0xffffffff  Neighbor: 0.0.0.0
  Flags: 0x1008c  OrigNextHop: 13.13.13.1
  Label: NULL  RealNextHop: 13.13.13.1
  BkLabel: NULL  BkNextHop: 24.24.24.2
  Tunnel ID: Invalid  Interface: GigabitEthernet1/0/2
  BkTunnel ID: Invalid  BkInterface: GigabitEthernet1/0/1
  FtnIndex: 0x0  TrafficIndex: N/A
  Connector: N/A
Configuring BGP

Overview

Border Gateway Protocol (BGP) is an exterior gateway protocol (EGP). It is called internal BGP (IBGP) when it runs within an AS and called external BGP (EBGP) when it runs between ASs. The current version in use is BGP-4 (RFC 4271).

BGP has the following characteristics:
- Focuses on route control and selection rather than route discovery and calculation.
- Uses TCP to enhance reliability.
- Measures the distance of a route by using a list of ASs that the route must travel through to reach the destination. BGP is also called a path-vector protocol.
- Supports CIDR.
- Reduces bandwidth consumption by advertising only incremental updates. BGP is very suitable to advertise large numbers of routes on the Internet.
- Eliminates routing loops by adding AS path information to BGP route updates.
- Uses policies to implement flexible route filtering and selection.
- Has good scalability.

BGP speaker and BGP peer

A router running BGP is a BGP speaker. A BGP speaker establishes peer relationships with other BGP speakers to exchange routing information over TCP connections.

BGP peers include the following types:
- IBGP peers—Reside in the same AS as the local router.
- EBGP peers—Reside in different ASs from the local router.

BGP message types

BGP uses the following message types:
- Open—After establishing a TCP connection, BGP sends an Open message to establish a session to the peer.
- Update—BGP sends update messages to exchange routing information between peers. Each update message can advertise a group of feasible routes with identical attributes and multiple withdrawn routes.
- Keepalive—BGP sends Keepalive messages between peers to maintain connectivity.
- Route-refresh—BGP sends a Route-refresh message to request the routing information for a specific address family from a peer.
- Notification—BGP sends a Notification message upon detecting an error and immediately closes the connection.

BGP path attributes

BGP uses the following path attributes in update messages for route filtering and selection:
- ORIGIN
The ORIGIN attribute specifies the origin of BGP routes. This attribute has the following types:

- **IGP**—Has the highest priority. Routes generated in the local AS have the IGP attribute.
- **EGP**—Has the second highest priority. Routes obtained through EGP have the EGP attribute.
- **INCOMPLETE**—Has the lowest priority. The source of routes with this attribute is unknown. Routes redistributed from other routing protocols have the INCOMPLETE attribute.

**AS_PATH**

The AS_PATH attribute identifies the ASs through which a route has passed. Before advertising a route to another AS, BGP adds the local AS number into the AS_PATH attribute, so the receiver can determine ASs to route the message back.

The AS_PATH attribute has the following types:

- **AS_SEQUENCE**—Arranges AS numbers in sequence. As shown in Figure 52, the number of the AS closest to the receiver's AS is leftmost.
- **AS_SET**—Arranges AS numbers randomly.

Figure 52 AS_PATH attribute

BGP uses the AS_PATH attribute to implement the following functions:

- **Avoid routing loops**—A BGP router does not receive routes containing the local AS number to avoid routing loops.
- **Affect route selection**—BGP gives priority to the route with the shortest AS_PATH length if other factors are the same. As shown in Figure 52, the BGP router in AS 50 gives priority to the route passing AS 40 for sending data to the destination 8.0.0.0. In some applications, you can apply a routing policy to control BGP route selection by modifying the AS_PATH length. For more information about routing policy, see "Configuring routing policies."
- **Filter routes**—By using an AS path list, you can filter routes based on AS numbers contained in the AS_PATH attribute. For more information about AS path list, see "Configuring routing policies."

**NEXT_HOP**

The NEXT_HOP attribute may not be the IP address of a directly connected router. Its value is determined as follows:
When a BGP speaker advertises a self-originated route to a BGP peer, it sets the address of the sending interface as the NEXT_HOP.

When a BGP speaker sends a received route to an EBGP peer, it sets the address of the sending interface as the NEXT_HOP.

When a BGP speaker sends a route received from an EBGP peer to an IBGP peer, it does not modify the NEXT_HOP attribute. If load balancing is configured, BGP modifies the NEXT_HOP attribute for the equal-cost routes. For load balancing information, see "BGP load balancing."

Figure 53 NEXT_HOP attribute

![Diagram](image)

- MED (MULTI_EXIT_DISC)
  BGP advertises the MED attribute between two neighboring ASs, each of which does not advertise the attribute to any other AS.

  Similar to metrics used by IGPs, MED is used to determine the optimal route for traffic going into an AS. When a BGP router obtains multiple routes to the same destination but with different next hops, it considers the route with the smallest MED value as the optimal route. As shown in Figure 54, traffic from AS 10 to AS 20 travels through Router B that is selected according to MED.
Generally BGP only compares MEDs of routes received from the same AS. You can also use the `compare-different-as-med` command to force BGP to compare MED values of routes received from different ASs.

- **LOCAL_PREF**

  The LOCAL_PREF attribute is exchanged between IBGP peers only, and is not advertised to any other AS. It indicates the priority of a BGP router.

  BGP uses LOCAL_PREF to determine the optimal route for traffic leaving the local AS. When a BGP router obtains multiple routes to the same destination but with different next hops, it considers the route with the highest LOCAL_PREF value as the optimal route. As shown in Figure 55, traffic from AS 20 to AS 10 travels through Router C that is selected according to LOCAL_PREF.
COMMUNITY

The COMMUNITY attribute identifies the community of BGP routes. A BGP community is a group of routes with the same characteristics. It has no geographical boundaries. Routes of different ASs can belong to the same community.

A route can carry one or more COMMUNITY attribute values (each of which is represented by a 4-byte integer). A router uses the COMMUNITY attribute to determine whether to advertise the route and the advertising scope without using complex filters such as ACLs. This mechanism simplifies routing policy configuration, management, and maintenance.

Well-known COMMUNITY attributes involve the following:

- **INTERNET**—By default, all routes belong to the Internet community. Routes with this attribute can be advertised to all BGP peers.
- **NO_EXPORT**—Routes with this attribute cannot be advertised out of the local AS or out of the local confederation, but can be advertised to other sub-ASs in the confederation. For confederation information, see "Settlements for problems in large-scale BGP networks."
- **No_ADVERTISE**—Routes with this attribute cannot be advertised to other BGP peers.
- **No_EXPORT_SUBCONFED**—Routes with this attribute cannot be advertised out of the local AS or other sub-ASs in the local confederation.

You can configure BGP community lists to filter BGP routes based on the BGP COMMUNITY attribute.

Extended community attribute

To meet new demands, BGP defines the extended community attribute. The extended community attribute has the following advantages over the COMMUNITY attribute:

- Provides more attribute values by extending the attribute length to eight bytes.
- Allows for using different types of extended community attributes in different scenarios to enhance route filtering and control and simplify configuration and management.

The device supports the route target and Site of Origin (SoO) extended community attributes. For information about route target, see MPLS Configuration Guide.
The SoO attribute specifies the site where the route originated. It prevents advertising a route back to the originating site. If the AS-path attribute is lost, the router can use the SoO attribute to avoid routing loops.

The SoO attribute has the following formats:
- 16-bit AS number:32-bit user-defined number. For example, 100:3.
- 32-bit IP address:16-bit user-defined number. For example, 192.168.122.15:1.
- 32-bit AS number:16-bit user-defined number, where the minimum value of the AS number is 65536. For example, 65536:1.

BGP route selection

BGP discards routes with unreachable NEXT_HOPs. If multiple routes to the same destination are available, BGP selects the optimal route in the following sequence:

1. The route with the highest Preferred_value.
2. The route with the highest LOCAL_PREF.
3. The route generated by the network command, the route redistributed by the import-route command, or the summary route in turn.
4. The route with the shortest AS_PATH.
5. The IGP, EGP, or INCOMPLETE route in turn.
6. The route with the lowest MED value.
7. The route learned from EBGP, confederation EBGP, confederation IBGP, or IBGP in turn.
8. The route with the smallest IGP metric.
9. The route with the smallest recursion depth.
10. If all routes are received from EBGP peers and the peers have different router IDs, the route that used to be an optimal route becomes the optimal route.
11. The route advertised by the router with the smallest router ID.
   If one of the routes is advertised by a route reflector, BGP compares the ORIGINATOR_ID of the route with the router IDs of other routers. Then, BGP selects the route with the smallest ID as the optimal route.
12. The route with the shortest CLUSTER_LIST.
13. The route advertised by the peer with the lowest IP address.

The CLUSTER_IDs of route reflectors form a CLUSTER_LIST. If a route reflector receives a route that contains its own CLUSTER ID in the CLUSTER_LIST, the router discards the route to avoid routing loops.

If load balancing is configured, the system selects available routes to implement load balancing.

BGP route advertisement rules

BGP follows these rules for route advertisement:

- When multiple feasible routes to a destination exist, BGP advertises only the optimal route to its peers. If the advertise-rib-active command is configured, BGP advertises the optimal route in the IP routing table. If not, BGP advertises the optimal route in the BGP routing table.
- BGP advertises only routes that it uses.
- BGP advertises routes learned from an EBGP peer to all BGP peers, including both EBGP and IBGP peers.
- BGP advertises routes learned from an IBGP peer to EBGP peers, rather than other IBGP peers.
After establishing a session to a new BGP peer, BGP advertises all the routes matching the above rules to the peer. After that, BGP advertises only incremental updates to the peer.

**BGP load balancing**

BGP load balancing is applicable between EBGP peers, between IBGP peers, and between confederations.

BGP implements load balancing through route recursion and route selection.

**BGP load balancing through route recursion**

The next hop of a BGP route might not be directly connected. One of the reasons is that the next hop information exchanged between IBGP peers is not modified. The BGP router must find the directly connected next hop through IGP. The matching route with the direct next hop is called the recursive route. The process of finding a recursive route is route recursion.

If multiple recursive routes to the same destination are load balanced, BGP generates the same number of next hops to forward packets.

BGP load balancing based on route recursion is always enabled in the system.

**BGP load balancing through route selection**

IGP routing protocols, such as RIP and OSPF, can use route metrics as criteria to load balance between routes that have the same metric. BGP cannot load balance between routes by route metrics as an IGP protocol does, because BGP does not have a route computation algorithm.

BGP uses the following load balancing criteria to determine load balanced routes:

- The routes have the same ORIGIN, LOCAL_PREF, and MED attributes. If the `balance as-path-neglect` command is not configured, the routes must also have the same AS_PATH attribute.
- The routes have the same MPLS label assignment status (labeled or not labeled).

BGP does not use the route selection rules described in "BGP route selection" for load balancing.

As shown in Figure 56, Router A and Router B are IBGP peers of Router C. Router C allows a maximum number of two ECMP routes for load balancing.

Router D and Router E both advertise a route 9.0.0.0 to Router C. Router C installs the two routes to its routing table for load balancing if the routes meet the BGP load balancing criteria. After that, Router C forwards to Router A and Router B a single route whose attributes are changed as follows:

- AS_PATH attribute:
  - If the `balance as-path-neglect` command is not configured, the AS_PATH attribute does not change.
  - If the `balance as-path-neglect` command is configured, the AS_PATH attribute is changed to the attribute of the optimal route.
- The NEXT_HOP attribute is changed to the IP address of Router C.
- Other attributes are changed to be the same as the optimal route.
Settlements for problems in large-scale BGP networks

You can use the following methods to facilitate management and improve route distribution efficiency on a large-scale BGP network.

- Route summarization
  Route summarization can reduce the BGP routing table size by advertising summary routes rather than more specific routes.

  The system supports both manual and automatic route summarization. Manual route summarization allows you to determine the attribute of a summary route and whether to advertise more specific routes.

- Route dampening
  Route flapping (a route comes up and disappears in the routing table frequently) causes BGP to send many routing updates. It can consume too many resources and affect other operations.

  In most cases, BGP runs in complex networks where route changes are more frequent. To solve the problem caused by route flapping, you can use BGP route dampening to suppress unstable routes.

  BGP route dampening uses a penalty value to judge the stability of a route. The bigger the value, the less stable the route. Each time a route state changes from reachable to unreachable, or a reachable route’s attribute changes, BGP adds a penalty value of 1000 to the route. When the penalty value of the route exceeds the suppress value, the route is suppressed and cannot become the optimal route. When the penalty value reaches the upper limit, no penalty value is added.

  If the suppressed route does not flap, its penalty value gradually decreases to half of the suppress value after a period of time. This period is called "Half-life." When the value decreases to the reusable threshold value, the route is usable again.
• Peer group
You can organize BGP peers with the same attributes into a group to simplify their configurations.
When a peer joins the peer group, the peer obtains the same configuration as the peer group. If the configuration of the peer group is changed, the configuration of group members is changed.

• Community
You can apply a community list or an extended community list to a routing policy for route control. For more information, see "BGP path attributes."

• Route reflector
IBGP peers must be fully meshed to maintain connectivity. If n routers exist in an AS, the number of IBGP connections is n(n-1)/2. If a large number of IBGP peers exist, large amounts of network and CPU resources are consumed to maintain sessions.
Using route reflectors can solve this issue. In an AS, a router acts as a route reflector, and other routers act as clients connecting to the route reflector. The route reflector forwards routing information received from a client to other clients. In this way, all clients can receive routing information from one another without establishing BGP sessions.
A router that is neither a route reflector nor a client is a non-client, which, as shown in Figure 58, must establish BGP sessions to the route reflector and other non-clients.

Figure 58 Network diagram for a route reflector
The route reflector and clients form a cluster. Typically a cluster has one route reflector. The ID of the route reflector is the Cluster_ID. You can configure more than one route reflector in a cluster to improve availability, as shown in Figure 59. The configured route reflectors must have the same Cluster_ID to avoid routing loops.

**Figure 59 Network diagram for route reflectors**

When the BGP routers in an AS are fully meshed, route reflection is unnecessary because it consumes more bandwidth resources. You can use commands to disable route reflection instead of modifying network configuration or changing network topology.

After route reflection is disabled between clients, routes can still be reflected between a client and a non-client.

- **Confederation**

  Confederation is another method to manage growing IBGP connections in an AS. It splits an AS into multiple sub-ASs. In each sub-AS, IBGP peers are fully meshed. As shown in Figure 60, intra-confederation EBGP connections are established between sub-ASs in AS 200.

**Figure 60 Confederation network diagram**
A non-confederation BGP speaker does not need to know sub-ASs in the confederation. It considers the confederation as one AS, and the confederation ID as the AS number. In the above figure, AS 200 is the confederation ID.

Confederation has a deficiency. When you change an AS into a confederation, you must reconfigure the routers, and the topology will be changed.

In large-scale BGP networks, you can use both route reflector and confederation.

**MP-BGP**

BGP-4 can only advertise IPv4 unicast routing information. Multiprotocol Extensions for BGP-4 (MP-BGP) can advertise routing information for the following address families:

- IPv6 unicast address family.
- IPv4 multicast and IPv6 multicast address families.
- IPv4 unicast and IPv6 unicast address families.

PIM uses static and dynamic unicast routes to perform RPF check before creating multicast routing entries. When the multicast and unicast topologies are different, you can use MP-BGP to advertise the routes for RPF check. MP-BGP stores the routes in the BGP multicast routing table. For more information about PIM and RPF check, see [IP Multicast Configuration Guide](#).

- VPNv4 and VPNv6 address families.

For more information about VPNv4 and VPNv6, see [MPLS Configuration Guide](#).

- Labeled IPv4 unicast and IPv6 unicast address families.

MP-BGP advertises IPv4 unicast/IPv6 unicast routes and MPLS labels assigned for the routes. Labeled IPv4 unicast routes apply to inter-AS Option C for MPLS L3VPN. Labeled IPv6 unicast routes apply to 6PE and inter-AS Option C for MPLS L3VPN. For more information about inter-AS Option C, see [MPLS Configuration Guide](#).

- L2VPN address family.

L2VPN information includes label block information and remote peer information. For more information about L2VPN and VPLS, see [MPLS Configuration Guide](#).

- IPv4 MDT address family.

MP-BGP advertises MDT information including the PE address and default group so that multicast VPN can create a default MDT that uses the PE as the root on the public network. For more information about multicast VPN, see [IP Multicast Configuration Guide](#).

**MP-BGP extended attributes**

Prefixes and next hops are key routing information. BGP-4 uses update messages to carry the following information:

- Feasible route prefixes in the Network Layer Reachability Information (NLRI) field.
- Unfeasible route prefixes in the withdrawn routes field.
- Next hops in the NEXT_HOP attribute.

BGP-4 cannot carry routing information for multiple network layer protocols.

To support multiple network layer protocols, MP-BGP defines the following path attributes:

- **MP_REACH_NLRI**—Carries feasible route prefixes and next hops for multiple network layer protocols.
- **MP_UNREACH_NLRI**—Carries unfeasible route prefixes for multiple network layer protocols.

MP-BGP uses these two attributes to advertise feasible and unfeasible routes for different network layer protocols. BGP speakers not supporting MP-BGP ignore updates containing these attributes and do not forward them to its peers.
Address family

MP-BGP uses address families and subsequent address families to identify different network layer protocols for routes contained in the MP_REACH_NLRI and MP_UNREACH_NLRI attributes. For example, an Address Family Identifier (AFI) of 2 and a Subsequent Address Family Identifier (SAFI) of 1 identify IPv6 unicast routing information carried in the MP_REACH_NLRI attribute. For address family values, see RFC 1700.

BGP multi-instance

A BGP router can run multiple BGP processes. Each BGP process corresponds to a BGP instance. BGP maintains an independent routing table for each BGP instance.

You can create multiple public address families for a BGP instance. However, each public address family (except for public VPNv4 and VPNv6 address families) can belong to only one BGP instance.

You can create multiple VPN instances for a BGP instance, and each VPN instance can have multiple address families. A VPN instance can belong to only one BGP instance.

Different BGP instances can have the same AS number but cannot have the same name.

BGP configuration views

BGP uses different views to manage routing information for different BGP instances, address families, and VPN instances. Most BGP commands are available in all BGP views. BGP supports multiple VPN instances by establishing a separate routing table for each VPN instance.

Table 14 describes different BGP configuration views.

Table 14 BGP configuration views

<table>
<thead>
<tr>
<th>View names</th>
<th>Ways to enter the views</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP instance view</td>
<td><code>&lt;Sysname&gt; system-view</code> [Sysname] bgp 100 instance abc [Sysname-bgp-abc]</td>
<td>You can create a BGP instance and enter its view by specifying the instance keyword in the bgp command. Configurations in this view apply to all public address families for the specified BGP instance and all VPN instances (such as confederation, GR, and logging configurations), or apply to all public address families for the specified BGP instance.</td>
</tr>
<tr>
<td>BGP IPv4 multicast address family view</td>
<td><code>&lt;Sysname&gt; system-view</code> [Sysname] bgp 100 instance abc [Sysname-bgp-abc] address-family ipv4 multicast</td>
<td>Configurations in this view apply to IPv4 multicast routes and peers of the specified BGP instance.</td>
</tr>
<tr>
<td>View names</td>
<td>Ways to enter the views</td>
<td>Remarks</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| BGP IPv6 multicast address     | <Sysname> system-view  
| family view                    | [Sysname] bgp 100 instance abc  
|                               | [Sysname-bgp-abc] address-family ipv6 multicast  
|                               | [Sysname-bgp-abc-mul-ipv6]                                                               | Configurations in this view apply to IPv6 multicast routes and peers of the specified BGP instance. |
| BGP VPNv4 address family view  | <Sysname> system-view  
|                               | [Sysname] bgp 100 instance abc  
|                               | [Sysname-bgp-abc] address-family vpnv4  
|                               | [Sysname-bgp-abc-vpnv4]                                                                | Configurations in this view apply to VPNv4 routes and peers of the specified BGP instance.  
|                               |                                                                                         | For more information about BGP VPNv4 address family view, see MPLS Configuration Guide.            |
| BGP VPNv6 address family view  | <Sysname> system-view  
|                               | [Sysname] bgp 100 instance abc  
|                               | [Sysname-bgp-abc] address-family vpnv6  
|                               | [Sysname-bgp-abc-vpnv6]                                                               | Configurations in this view apply to VPNv6 routes and peers of the specified BGP instance.  
|                               |                                                                                         | For more information about BGP VPNv6 address family view, see MPLS Configuration Guide.            |
| BGP L2VPN address family view  | <Sysname> system-view  
|                               | [Sysname] bgp 100 instance abc  
|                               | [Sysname-bgp-abc] address-family 12vpn  
|                               | [Sysname-bgp-abc-12vpn]                                                                  | Configurations in this view apply to L2VPN information and L2VPN peers of the specified BGP instance.  
|                               |                                                                                         | For more information about BGP L2VPN address family view, see MPLS Configuration Guide.            |
| BGP-VPN instance view          | <Sysname> system-view  
|                               | [Sysname] bgp 100 instance abc  
|                               | [Sysname-bgp-abc] ip vpn-instance vpn1  
|                               | [Sysname-bgp-abc-vpn1]                                                                  | Configurations in this view apply to all address families in the specified VPN instance of the specified BGP instance.  |
| BGP-VPN IPv4 unicast address   | <Sysname> system-view  
| family view                    | [Sysname] bgp 100 instance abc  
|                               | [Sysname-bgp-abc] ip vpn-instance vpn1  
|                               | [Sysname-bgp-abc-vpn1] address-family ipv4 unicast  
|                               | [Sysname-bgp-abc-ipv4-vpn1]                                                              | Configurations in this view apply to IPv4 unicast routes and peers in the specified VPN instance of the specified BGP instance.  |
| BGP-VPN IPv6 unicast address   | <Sysname> system-view  
| family view                    | [Sysname] bgp 100 instance abc  
|                               | [Sysname-bgp-abc] ip vpn-instance vpn1  
|                               | [Sysname-bgp-abc-vpn1] address-family ipv6 unicast  
|                               | [Sysname-bgp-abc-ipv6-vpn1]                                                              | Configurations in this view apply to IPv6 unicast routes and peers in the specified VPN instance of the specified BGP instance.  |
| BGP-VPN VPNv4 address family   | <Sysname> system-view  
| view                           | [Sysname] bgp 100 instance abc  
|                               | [Sysname-bgp-abc] ip vpn-instance vpn1  
|                               | [Sysname-bgp-abc-vpn1] address-family vpnv4  
|                               | [Sysname-bgp-abc-vpnv4-vpn1]                                                              | Configurations in this view apply to VPNv4 routes and peers in the specified VPN instance of the specified BGP instance.  
|                               |                                                                                         | For more information about BGP-VPN VPNv4 address family view, see MPLS Configuration Guide.            |
Protocols and standards

- RFC 1700, ASSIGNED NUMBERS
- RFC 1771, A Border Gateway Protocol 4 (BGP-4)
- RFC 1997, BGP Communities Attribute
- RFC 2439, BGP Route Flap Damping
- RFC 2796, BGP Route Reflection
- RFC 2858, Multiprotocol Extensions for BGP-4
- RFC 2918, Route Refresh Capability for BGP-4
- RFC 3065, Autonomous System Confederations for BGP
- RFC 3392, Capabilities Advertisement with BGP-4
- RFC 4271, A Border Gateway Protocol 4 (BGP-4)
- RFC 4360, BGP Extended Communities Attribute
- RFC 4724, Graceful Restart Mechanism for BGP
- RFC 4760, Multiprotocol Extensions for BGP-4
- RFC 5082, The Generalized TTL Security Mechanism (GTSM)
- RFC 6037, Cisco Systems’ Solution for Multicast in BGP MPLS IP VPNs

BGP configuration task list

On a basic BGP network, perform the following configuration tasks:

- Enable BGP.
- Configure BGP peers or peer groups. If you configure a BGP setting at both the peer group and the peer level, the most recent configuration takes effect on the peer.
- Control BGP route generation.

To control BGP route distribution and path selection, you must perform additional configuration tasks.

To configure BGP, perform the following tasks (IPv4 unicast/IPv4 multicast):

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring basic BGP:</td>
<td>As a best practice, configure BGP peer groups on large scale BGP networks for easy configuration and maintenance.</td>
</tr>
<tr>
<td>(Required.) Enabling BGP</td>
<td></td>
</tr>
<tr>
<td>(Required.) Perform one of the following tasks:</td>
<td></td>
</tr>
<tr>
<td>o Configuring a BGP peer</td>
<td></td>
</tr>
<tr>
<td>o Configuring dynamic BGP peers</td>
<td></td>
</tr>
<tr>
<td>o Configuring a BGP peer group</td>
<td></td>
</tr>
<tr>
<td>(Optional.) Specifying the source address of TCP connections</td>
<td></td>
</tr>
<tr>
<td>Tasks at a glance</td>
<td>Remarks</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>Perform at least one of the following tasks to generate BGP routes:</td>
<td></td>
</tr>
<tr>
<td>• Injecting a local network</td>
<td>N/A</td>
</tr>
<tr>
<td>• Redistributing IGP routes</td>
<td></td>
</tr>
<tr>
<td><em>(Optional.)</em> Controlling route distribution and reception:</td>
<td>BGP cannot advertise optimal routes in the IP routing table for IPv4 multicast address family.</td>
</tr>
<tr>
<td>• Configuring BGP route summarization</td>
<td></td>
</tr>
<tr>
<td>• Advertising optimal routes in the IP routing table</td>
<td></td>
</tr>
<tr>
<td>• Advertising a default route to a peer or peer group</td>
<td></td>
</tr>
<tr>
<td>• Limiting routes received from a peer or peer group</td>
<td></td>
</tr>
<tr>
<td>• Configuring BGP route filtering policies</td>
<td></td>
</tr>
<tr>
<td>• Configuring BGP route update delay</td>
<td></td>
</tr>
<tr>
<td>• Configuring BGP route dampening</td>
<td></td>
</tr>
<tr>
<td><em>(Optional.)</em> Controlling BGP path selection:</td>
<td></td>
</tr>
<tr>
<td>• Setting a preferred value for routes received</td>
<td>N/A</td>
</tr>
<tr>
<td>• Configuring preferences for BGP routes</td>
<td></td>
</tr>
<tr>
<td>• Configuring the default local preference</td>
<td></td>
</tr>
<tr>
<td>• Configuring the MED attribute</td>
<td></td>
</tr>
<tr>
<td>• Configuring the NEXT_HOP attribute</td>
<td></td>
</tr>
<tr>
<td>• Configuring the AS_PATH attribute</td>
<td></td>
</tr>
<tr>
<td>• Ignoring IGP metrics during optimal route selection</td>
<td></td>
</tr>
<tr>
<td>• Configuring the SoO attribute</td>
<td></td>
</tr>
<tr>
<td><em>(Optional.)</em> Tuning and optimizing BGP networks;</td>
<td></td>
</tr>
<tr>
<td>• Configuring the keepalive interval and hold time</td>
<td>N/A</td>
</tr>
<tr>
<td>• Configuring the interval for sending updates for the same route</td>
<td></td>
</tr>
<tr>
<td>• Enabling BGP to establish an EBGP session over multiple hops</td>
<td></td>
</tr>
<tr>
<td>• Enabling immediate re-establishment of direct EBGP connections upon link failure</td>
<td></td>
</tr>
<tr>
<td>• Enabling 4-byte AS number suppression</td>
<td></td>
</tr>
<tr>
<td>• Enabling MD5 authentication for BGP peers</td>
<td></td>
</tr>
<tr>
<td>• Configuring BGP load balancing</td>
<td>N/A</td>
</tr>
<tr>
<td>• Configuring IPSec for IPv6 BGP</td>
<td></td>
</tr>
<tr>
<td>• Disabling BGP to establish a session to a peer or peer group</td>
<td></td>
</tr>
<tr>
<td>• Configuring GTSM for BGP</td>
<td></td>
</tr>
<tr>
<td>• Configuring BGP soft-reset</td>
<td></td>
</tr>
<tr>
<td>• Protecting an EBGP peer when memory usage reaches level 2 threshold</td>
<td></td>
</tr>
<tr>
<td>• Configuring an update delay for local MPLS labels</td>
<td></td>
</tr>
<tr>
<td>• Flushing the suboptimal BGP route to the RIB</td>
<td></td>
</tr>
<tr>
<td><em>(Optional.)</em> Configuring a large-scale BGP network:</td>
<td>N/A</td>
</tr>
<tr>
<td>• Configuring BGP community</td>
<td></td>
</tr>
<tr>
<td>• Configuring BGP route reflection</td>
<td></td>
</tr>
<tr>
<td>• Configuring a BGP confederation</td>
<td></td>
</tr>
<tr>
<td><em>(Optional.)</em> Configuring BGP GR</td>
<td>N/A</td>
</tr>
<tr>
<td><em>(Optional.)</em> Configuring BGP NSR</td>
<td>N/A</td>
</tr>
<tr>
<td><em>(Optional.)</em> Enabling SNMP notifications for BGP</td>
<td>N/A</td>
</tr>
<tr>
<td><em>(Optional.)</em> Enabling logging for session state changes</td>
<td>N/A</td>
</tr>
<tr>
<td>Tasks at a glance</td>
<td>Remarks</td>
</tr>
<tr>
<td>------------------------------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>(Optional.) Configuring BFD for BGP</td>
<td>N/A</td>
</tr>
<tr>
<td>(Optional.) Configuring BGP FRR</td>
<td>BGP does not support FRR for IPv4 multicast routes.</td>
</tr>
<tr>
<td>(Optional.) Configuring BGP policy accounting</td>
<td>BGP does not support policy accounting for IPv4 multicast routes.</td>
</tr>
</tbody>
</table>

To configure BGP, perform the following tasks (IPv6 unicast/IPv6 multicast):

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring basic BGP:</td>
<td>As a best practice, configure BGP peer groups on large scale BGP networks for easy configuration and maintenance.</td>
</tr>
<tr>
<td>• (Required.) Enabling BGP</td>
<td></td>
</tr>
<tr>
<td>• (Required.) Perform one of the following tasks:</td>
<td></td>
</tr>
<tr>
<td>o Configuring a BGP peer</td>
<td></td>
</tr>
<tr>
<td>o Configuring dynamic BGP peers</td>
<td></td>
</tr>
<tr>
<td>o Configuring a BGP peer group</td>
<td></td>
</tr>
<tr>
<td>• (Optional.) Specifying the source address of TCP connections</td>
<td></td>
</tr>
<tr>
<td>Perform at least one of the following tasks to generate BGP routes:</td>
<td>N/A</td>
</tr>
<tr>
<td>• Injecting a local network</td>
<td></td>
</tr>
<tr>
<td>• Redistributing IGP routes</td>
<td></td>
</tr>
<tr>
<td>(Optional.) Controlling route distribution and reception:</td>
<td></td>
</tr>
<tr>
<td>• Configuring BGP route summarization</td>
<td>BGP cannot advertise optimal routes in the IP routing table for IPv6 multicast address family.</td>
</tr>
<tr>
<td>• Advertising optimal routes in the IP routing table</td>
<td></td>
</tr>
<tr>
<td>• Advertising a default route to a peer or peer group</td>
<td></td>
</tr>
<tr>
<td>• Limiting routes received from a peer or peer group</td>
<td></td>
</tr>
<tr>
<td>• Configuring BGP route filtering policies</td>
<td></td>
</tr>
<tr>
<td>• Configuring BGP route dampening</td>
<td></td>
</tr>
<tr>
<td>(Optional.) Controlling BGP path selection:</td>
<td></td>
</tr>
<tr>
<td>• Setting a preferred value for routes received</td>
<td>N/A</td>
</tr>
<tr>
<td>• Configuring preferences for BGP routes</td>
<td></td>
</tr>
<tr>
<td>• Configuring the default local preference</td>
<td></td>
</tr>
<tr>
<td>• Configuring the MED attribute</td>
<td></td>
</tr>
<tr>
<td>• Configuring the NEXT_HOP attribute</td>
<td></td>
</tr>
<tr>
<td>• Configuring the AS_PATH attribute</td>
<td></td>
</tr>
<tr>
<td>• Configuring the SoO attribute</td>
<td></td>
</tr>
</tbody>
</table>
### Tasks at a glance

<table>
<thead>
<tr>
<th>Remarks</th>
</tr>
</thead>
</table>

(Optional.) Tuning and optimizing BGP networks:
- Configuring the keepalive interval and hold time
- Configuring the interval for sending updates for the same route
- Enabling BGP to establish an EBGP session over multiple hops
- Enabling immediate re-establishment of direct EBGP connections upon link failure
- Enabling 4-byte AS number suppression
- Enabling MD5 authentication for BGP peers
- Configuring BGP load balancing
- Configuring IPSec for IPv6 BGP
- Disabling BGP to establish a session to a peer or peer group
- Configuring GTSM for BGP
- Configuring BGP soft-reset
- Protecting an EBGP peer when memory usage reaches level 2 threshold
- Configuring an update delay for local MPLS labels

(Optional.) Configuring a large-scale BGP network:
- Configuring BGP community
- Configuring BGP route reflection
- Configuring a BGP confederation

(Optional.) Configuring BGP GR

(Optional.) Configuring BGP NSR

(Optional.) Enabling SNMP notifications for BGP

(Optional.) Enabling logging for session state changes

(Optional.) Configuring BFD for BGP

(Optional.) Configuring BGP FRR

(Optional.) Configuring BGP policy accounting

(Optional.) Configuring 6PE

### Configuring basic BGP

This section describes the basic settings required for a BGP network to run.

### Enabling BGP

A router ID is the unique identifier of a BGP router in an AS.

- To ensure the uniqueness of a router ID and enhance availability, specify in BGP instance view the IP address of a local loopback interface as the router ID. Different BGP instances can have the same router ID.
- If no router ID is specified in BGP instance view, the global router ID is used.
• To modify a non-zero router ID of a BGP instance, use the `router-id` command in BGP instance view, rather than the `router id` command in system view.

• If you specify a router ID in BGP instance view and then remove the interface that owns the router ID, the router does not select a new router ID. To select a new router ID, use the `undo router-id` command in BGP instance view.

To enable BGP:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure a global router ID.</td>
<td><code>router-id</code></td>
</tr>
<tr>
<td>3.</td>
<td>Enable BGP and enter BGP instance view.</td>
<td><code>bgp as-number [ instance instance-name ]</code></td>
</tr>
<tr>
<td>4.</td>
<td>(Optional.) Configure an SNMP context for the BGP instance.</td>
<td><code>snmp context-name context-name</code></td>
</tr>
<tr>
<td>5.</td>
<td>(Optional.) Configure a router ID for the BGP instance.</td>
<td><code>router-id</code></td>
</tr>
<tr>
<td>6.</td>
<td>(Optional.) Enter BGP-VPN instance view.</td>
<td><code>ip vpn-instance vpn-instance-name</code></td>
</tr>
<tr>
<td>7.</td>
<td>(Optional.) Configure a router ID for the BGP VPN instance.</td>
<td>`router-id { router-id</td>
</tr>
</tbody>
</table>

**Configuring a BGP peer**

**Configuring a BGP peer (IPv4 unicast address family)**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
### Configuring a BGP peer (IPv4 unicast address family)

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP instance view or BGP-VPN instance view.</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>Create an IPv4 BGP peer and specify its AS number.</td>
<td>peer ipv4-address as-number By default, no IPv4 BGP peers exist.</td>
</tr>
<tr>
<td>4.</td>
<td>(Optional.) Configure a description for a peer.</td>
<td>peer ipv4-address description text By default, no description is configured for a peer.</td>
</tr>
<tr>
<td>5.</td>
<td>Create the BGP IPv4 unicast address family or BGP-VPN IPv4 unicast address family and enter its view.</td>
<td>address-family ipv4 [ unicast ] By default, no BGP IPv4 unicast address family or BGP-VPN IPv4 unicast address family exists.</td>
</tr>
<tr>
<td>6.</td>
<td>Enable the router to exchange IPv4 unicast routing information with the specified peer.</td>
<td>peer ipv4-address enable By default, the router cannot exchange IPv4 unicast routing information with the peer.</td>
</tr>
</tbody>
</table>

### Configuring a BGP peer (IPv6 unicast address family)

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP instance view or BGP-VPN instance view.</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>Create an IPv6 BGP peer and specify its AS number.</td>
<td>peer ipv6-address as-number By default, no IPv6 BGP peers exist.</td>
</tr>
<tr>
<td>4.</td>
<td>(Optional.) Configure a description for a peer.</td>
<td>peer ipv6-address description text By default, no description is configured for a peer.</td>
</tr>
<tr>
<td>5.</td>
<td>Create the BGP IPv6 unicast address family or BGP-VPN IPv6 unicast address family and enter its view.</td>
<td>address-family ipv6 [ unicast ] By default, no BGP IPv6 unicast address family or BGP-VPN IPv6 unicast address family exists.</td>
</tr>
<tr>
<td>6.</td>
<td>Enable the router to exchange IPv6 unicast routing information with the specified peer.</td>
<td>peer ipv6-address enable By default, the router cannot exchange IPv6 unicast routing information with the peer.</td>
</tr>
</tbody>
</table>
Configuring a BGP peer (IPv4 multicast address family)

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP instance view</td>
<td>bgp as-number [ instance instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Create an IPv4 BGP peer and specify its AS number.</td>
<td>peer ipv4-address as-number</td>
</tr>
<tr>
<td>4.</td>
<td>(Optional.) Configure a description for the peer.</td>
<td>peer ipv4-address description text</td>
</tr>
<tr>
<td>5.</td>
<td>Create the BGP IPv4 multicast address family and enter its view.</td>
<td>address-family ipv4 multicast</td>
</tr>
<tr>
<td>6.</td>
<td>Enable the router to exchange IPv4 unicast routing information used for RPF check with the specified peer.</td>
<td>peer ipv4-address enable</td>
</tr>
</tbody>
</table>

Configuring a BGP peer (IPv6 multicast address family)

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP instance view</td>
<td>bgp as-number [ instance instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Create an IPv6 BGP peer and specify its AS number.</td>
<td>peer ipv6-address as-number as-number</td>
</tr>
<tr>
<td>4.</td>
<td>(Optional.) Configure a description for the peer.</td>
<td>peer ipv6-address description text</td>
</tr>
<tr>
<td>5.</td>
<td>Create the BGP IPv6 multicast address family and enter its view.</td>
<td>address-family ipv6 multicast</td>
</tr>
<tr>
<td>6.</td>
<td>Enable the router to exchange IPv6 unicast routing information used for RPF check with the specified peer.</td>
<td>peer ipv6-address enable</td>
</tr>
</tbody>
</table>

Configuring dynamic BGP peers

This feature enables BGP to establish dynamic BGP peer relationships with devices in a network. BGP accepts connection requests from the network but it does not initiate connection requests to the network.

After a device in the network initiates a connection request, BGP establishes a dynamic peer relationship with the device.

If multiple BGP peers reside in the same network, you can use this feature to simplify BGP peer configuration.
### Configuring dynamic BGP peers (IPv4 unicast address family)

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
| 2. | Enter BGP instance view or BGP-VPN instance view. | - Enter BGP instance view: `bgp as-number [ instance instance-name ]`  
- Enter BGP-VPN instance view:  
  a. `bgp as-number [ instance instance-name ]`  
  b. `ip vpn-instance vpn-instance-name` | N/A |
| 3. | Specify devices in a network as dynamic BGP peers and specify an AS number for the peers. | `peer ipv4-address mask-length as-number` | By default, no dynamic BGP peers exist. |
| 4. | (Optional.) Configure a description for dynamic BGP peers. | `peer ipv4-address mask-length description text` | By default, no description is configured for dynamic BGP peers. |
| 5. | Create the BGP IPv4 unicast address family or BGP-VPN IPv4 unicast address family and enter its view. | `address-family ipv4 [ unicast ]` | By default, no BGP IPv4 unicast address family or BGP-VPN IPv4 unicast address family exists. |
| 6. | Enable BGP to exchange IPv4 unicast routing information with dynamic BGP peers in the specified network. | `peer ipv4-address mask-length enable` | By default, BGP cannot exchange IPv4 unicast routing information with dynamic BGP peers. |

### Configuring dynamic BGP peers (IPv6 unicast address family)

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
| 2. | Enter BGP instance view or BGP-VPN instance view. | - Enter BGP instance view: `bgp as-number [ instance instance-name ]`  
- Enter BGP-VPN instance view:  
  a. `bgp as-number [ instance instance-name ]`  
  b. `ip vpn-instance vpn-instance-name` | N/A |
<p>| 3. | Specify devices in a network as dynamic BGP peers and specify an AS number for the peers. | <code>peer ipv6-address prefix-length as-number as-number</code> | By default, no dynamic BGP peers exist. |
| 4. | (Optional.) Configure a description for dynamic BGP peers. | <code>peer ipv6-address prefix-length description text</code> | By default, no description is configured for dynamic BGP peers. |
| 5. | Create the BGP IPv6 unicast address family or BGP-VPN IPv6 unicast address family and enter its view. | <code>address-family ipv6 [ unicast ]</code> | By default, no BGP IPv6 unicast address family or BGP-VPN IPv6 unicast address family exists. |</p>
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.</td>
<td><strong>peer ipv6-address prefix-length enable</strong></td>
<td>By default, BGP cannot exchange IPv6 unicast routing information with dynamic BGP peers.</td>
</tr>
</tbody>
</table>

**Configuring dynamic BGP peers (IPv4 multicast address family)**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><strong>system-view</strong></td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td><strong>bgp as-number [ instance instance-name ]</strong></td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td><strong>peer ipv4-address mask-length as-number as-number</strong></td>
<td>By default, no dynamic BGP peers exist.</td>
</tr>
<tr>
<td>4.</td>
<td><strong>peer ipv4-address mask-length description text</strong></td>
<td>By default, no description is configured for dynamic BGP peers.</td>
</tr>
<tr>
<td>5.</td>
<td><strong>address-family ipv4 multicast</strong></td>
<td>By default, no BGP IPv4 multicast address family exists.</td>
</tr>
<tr>
<td>6.</td>
<td><strong>peer ipv4-address mask-length enable</strong></td>
<td>By default, BGP cannot exchange IPv4 unicast routing information used for RPF check with dynamic BGP peers.</td>
</tr>
</tbody>
</table>

**Configuring dynamic BGP peers (IPv6 multicast address family)**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><strong>system-view</strong></td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td><strong>bgp as-number [ instance instance-name ]</strong></td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td><strong>peer ipv6-address prefix-length as-number as-number</strong></td>
<td>By default, no dynamic BGP peers exist.</td>
</tr>
<tr>
<td>4.</td>
<td><strong>peer ipv6-address prefix-length description text</strong></td>
<td>By default, no description is configured for dynamic BGP peers.</td>
</tr>
<tr>
<td>5.</td>
<td><strong>address-family ipv6 multicast</strong></td>
<td>By default, no BGP IPv6 multicast address family exists.</td>
</tr>
<tr>
<td>6.</td>
<td><strong>peer ipv6-address prefix-length enable</strong></td>
<td>By default, BGP cannot exchange IPv6 unicast routing information used for RPF check with dynamic BGP peers.</td>
</tr>
</tbody>
</table>
Configuring a BGP peer group

The peers in a peer group use the same route selection policy.

In a large-scale network, many peers can use the same route selection policy. You can configure a peer group and add these peers into this group. When you change the policy for the group, the modification also applies to the peers in the group.

A peer group is an IBGP peer group if peers in it belong to the local AS, and is an EBGP peer group if peers in it belong to different ASs.

Configuring an IBGP peer group

After you create an IBGP peer group and then add a peer into it, the system creates the peer in BGP instance view and specifies the local AS number for the peer.

To configure an IBGP peer group (IPv4 unicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
| 2.   | Enter BGP instance view or BGP-VPN instance view. | • Enter BGP instance view: bgp as-number [ instance instance-name ]  
      • Enter BGP-VPN instance view:  
        a. bgp as-number [ instance instance-name ]  
        b. ip vpn-instance vpn-instance-name | N/A |
| 3.   | Create an IBGP peer group. | group group-name [ internal ] | By default, no IBGP peer groups exist. |
| 4.   | Add a peer into the IBGP peer group. | peer ipv4-address [ mask-length ] group group-name [ as-number as-number ] | By default, no peer exists in the peer group.  
    The as-number option must specify the local AS number. |
| 5.   | (Optional.) Configure a description for the peer group. | peer group-name description text | By default, no description is configured for the peer group. |
| 6.   | Create the BGP IPv4 unicast address family or BGP-VPN IPv4 unicast address family and enter its view. | address-family ipv4 [ unicast ] | By default, no BGP IPv4 unicast address family or BGP-VPN IPv4 unicast address family exists. |
| 7.   | Enable the router to exchange IPv4 unicast routing information with peers in the specified peer group. | peer group-name enable | By default, the router cannot exchange IPv4 unicast routing information with the peers. |

To configure an IBGP peer group (IPv6 unicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP instance view or BGP-VPN instance view.</td>
<td>N/A</td>
</tr>
</tbody>
</table>
|     | • Enter BGP instance view: `bgp as-number [ instance instance-name ]`  
     |     | • Enter BGP-VPN instance view:  
     |     |   a. `bgp as-number [ instance instance-name ]`  
     |     |   b. `ip vpn-instance vpn-instance-name` | |
| 3. | Create an IBGP peer group. | By default, no IBGP peer groups exist. |
|     | `group group-name [ internal ]` | |
| 4. | Add a peer into the IBGP peer group. | By default, no peer exists in the peer group.  
    | `peer ipv6-address [ prefix-length ]`  
    |     | `group group-name [ as-number ]` | The `as-number` option must specify the local AS number. |
| 5. | (Optional.) Configure a description for the peer group. | By default, no description is configured for the peer group. |
|     | `peer group-name description text` | |
| 6. | Create the BGP IPv6 unicast address family or BGP-VPN IPv6 unicast address family and enter its view. | By default, no BGP IPv6 unicast address family exists. |
|     | `address-family ipv6 [ unicast ]` | |
| 7. | Enable the router to exchange IPv6 unicast routing information with peers in the specified peer group. | By default, the router cannot exchange IPv6 unicast routing information with the peers. |
|     | `peer group-name enable` | |

To configure an IBGP peer group (IPv4 multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td><code>system-view</code></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP instance view.</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td><code>bgp as-number [ instance instance-name ]</code></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Create an IBGP peer group.</td>
<td>By default, no IBGP peer groups exist.</td>
</tr>
<tr>
<td></td>
<td><code>group group-name [ internal ]</code></td>
<td></td>
</tr>
</tbody>
</table>
| 4. | Add an IPv4 peer into the IBGP peer group. | By default, no peer exists in the peer group.  
    | `peer ipv4-address [ mask-length ]`  
    |     | `group group-name [ as-number ]` | The `as-number` option must specify the local AS number. |
| 5. | (Optional.) Configure a description for the peer group. | By default, no description is configured for the peer group. |
|     | `peer group-name description text` | |
| 6. | Create the BGP IPv4 multicast address family and enter its view. | By default, no BGP IPv4 multicast address family exists. |
|     | `address-family ipv4 multicast` | |
### Configuring an IBGP peer group

To configure an IBGP peer group (IPv6 multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>bgp as-number [ instance instance-name ]</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>group group-name [ internal ]</td>
<td>By default, no IBGP peer groups exist.</td>
</tr>
<tr>
<td>4.</td>
<td>peer ipv6-address [ prefix-length ] group group-name [ as-number as-number ]</td>
<td>By default, no peer exists in the peer group. The as-number as-number option must specify the local AS number.</td>
</tr>
<tr>
<td>5.</td>
<td>peer group-name description text</td>
<td>By default, no description is configured for the peer group.</td>
</tr>
<tr>
<td>6.</td>
<td>address-family ipv6 multicast</td>
<td>By default, no BGP IPv6 multicast address family exists.</td>
</tr>
<tr>
<td>7.</td>
<td>peer group-name enable</td>
<td>By default, the router cannot exchange IPv6 unicast routing information used for RPF check with the peers in the peer group.</td>
</tr>
</tbody>
</table>

### Configuring an EBGP peer group

If peers in an EBGP group belong to the same external AS, the EBGP peer group is a pure EBGP peer group. If not, it is a mixed EBGP peer group.

Use one of the following methods to configure an EBGP peer group:

- **Method 1**—Create an EBGP peer group, specify its AS number, and add peers into it. All the added peers have the same AS number. All peers in the peer group have the same AS number as the peer group. You can specify an AS number for a peer before adding it into the peer group. The AS number must be the same as that of the peer group.

- **Method 2**—Create an EBGP peer group, specify an AS number for a peer, and add the peer into the peer group. Peers added in the group can have different AS numbers.

- **Method 3**—Create an EBGP peer group and add a peer with an AS number into it. Peers added in the group can have different AS numbers.

To configure an EBGP peer group by using Method 1 (IPv4 unicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
</tbody>
</table>
### Step 2. Enter BGP instance view or BGP-VPN instance view.

- **Enter BGP instance view:**
  
  ```
  bgp as-number [ instance instance-name ]
  ```

- **Enter BGP-VPN instance view:**
  
  a. ```bgp as-number [ instance instance-name ]```  
  
  b. ```ip vpn-instance vpn-instance-name```  

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>Enter BGP instance view or BGP-VPN instance view.</td>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td>Create an EBGP peer group.</td>
<td>By default, no EBGP peer groups exist.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.</td>
<td>Specify the AS number of the group.</td>
<td>By default, no AS number is specified. If a peer group contains peers, you cannot remove or change its AS number.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.</td>
<td>Add a peer into the EBGP peer group.</td>
<td>By default, no peers exist in the peer group. The <strong>as-number as-number</strong> option, if used, must specify the same AS number as the peer group-name <strong>as-number as-number</strong> command.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.</td>
<td>(Optional.) Configure a description for the peer group.</td>
<td>By default, no description is configured for the peer group.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.</td>
<td>Create the BGP IPv4 unicast address family or BGP-VPN IPv4 unicast address family and enter its view.</td>
<td>By default, no BGP IPv4 unicast address family or BGP-VPN IPv4 unicast address family exists.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.</td>
<td>Enable the router to exchange IPv4 unicast routing information with peers in the specified peer group.</td>
<td>By default, the router cannot exchange IPv4 unicast routing information with the peers.</td>
</tr>
</tbody>
</table>

### To configure an EBGP peer group by using Method 1 (IPv6 unicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>Enter BGP instance view or BGP-VPN instance view.</td>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td>Create an EBGP peer group.</td>
<td>By default, no EBGP peer groups exist.</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| 4.   | Specify the AS number of the group. | **peer group-name as-number**  
*as-number*  
By default, no AS number is specified. If a peer group contains peers, you cannot remove or change its AS number. |
| 5.   | Add a peer into the EBGP peer group. | **peer ipv6-address [ prefix-length ]**  
**group group-name [ as-number as-number ]**  
By default, no peers exist in the peer group. The **as-number** option, if used, must specify the same AS number as the **peer group-name as-number** command. |
| 6.   | (Optional.) Configure a description for the peer group. | **peer group-name description**  
*text*  
By default, no description is configured for the peer group. |
| 7.   | Create the BGP IPv6 unicast address family or BGP-VPN IPv6 unicast address family and enter its view. | **address-family ipv6 [ unicast ]**  
By default, no BGP IPv6 unicast address family or BGP-VPN IPv6 unicast address family exists. |
| 8.   | Enable the router to exchange IPv6 unicast routing information with peers in the specified peer group. | **peer group-name enable**  
By default, the router cannot exchange IPv6 unicast routing information with the peers. |

To configure an EBGP peer group by using Method 1 (IPv4 multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
</table>
| 1.   | Enter system view. | **system-view**  
N/A |
| 2.   | Enter BGP instance view. | **bgp as-number [ instance instance-name ]**  
N/A |
| 3.   | Create an EBGP peer group. | **group group-name external**  
By default, no EBGP peer groups exist. |
| 4.   | Specify the AS number of the group. | **peer group-name as-number as-number**  
By default, no AS number is specified. If a peer group contains peers, you cannot remove or change its AS number. |
| 5.   | Add an IPv4 BGP peer into the EBGP peer group. | **peer ipv4-address [ mask-length ]**  
**group group-name [ as-number as-number ]**  
By default, no peers exist in the peer group. The **as-number** option, if used, must specify the same AS number as the **peer group-name as-number** command. |
| 6.   | (Optional.) Configure a description for the peer group. | **peer group-name description**  
*text*  
By default, no description is configured for the peer group. |
| 7.   | Create the BGP IPv4 multicast address family and enter its view. | **address-family ipv4 multicast**  
By default, no BGP IPv4 multicast address family exists. |
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.</td>
<td>Enable the router to exchange IPv4 unicast routing information used for RPF check with peers in the specified peer group.</td>
<td>peer group-name enable</td>
</tr>
</tbody>
</table>

To configure an EBGP peer group by using Method 1 (IPv6 multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP instance view.</td>
<td>bgp [ instance instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Create an EBGP peer group.</td>
<td>group group-name external</td>
</tr>
<tr>
<td>4.</td>
<td>Specify the AS number of the group.</td>
<td>peer group-name as-number as-number</td>
</tr>
<tr>
<td>5.</td>
<td>Add an IPv6 BGP peer into the EBGP peer group.</td>
<td>peer ipv6-address [ prefix-length ] group group-name [ as-number as-number ]</td>
</tr>
<tr>
<td>6.</td>
<td>(Optional.) Configure a description for the peer group.</td>
<td>peer group-name description text</td>
</tr>
<tr>
<td>7.</td>
<td>Create the BGP IPv6 multicast address family and enter its view.</td>
<td>address-family ipv6 multicast</td>
</tr>
<tr>
<td>8.</td>
<td>Enable the router to exchange IPv6 unicast routing information used for RPF check with peers in the specified peer group.</td>
<td>peer group-name enable</td>
</tr>
</tbody>
</table>

To configure an EBGP peer group by using Method 2 (IPv4 unicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP instance view or BGP-VPN instance view.</td>
<td></td>
</tr>
<tr>
<td>a.</td>
<td>Enter BGP instance view:</td>
<td>bgp [ instance instance-name ]</td>
</tr>
<tr>
<td>b.</td>
<td>Enter BGP-VPN instance view:</td>
<td>bgp [ instance instance-name ]</td>
</tr>
<tr>
<td>c.</td>
<td>ip vpn-instance</td>
<td>vpn-instance-name</td>
</tr>
</tbody>
</table>
### Step 3. Create an EBGP peer group.

<table>
<thead>
<tr>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>group group-name external</code></td>
<td>By default, no EBGP peer groups exist.</td>
</tr>
</tbody>
</table>

### Step 4. Create an IPv4 BGP peer and specify its AS number.

<table>
<thead>
<tr>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>peer ipv4-address [ mask-length ] as-number as-number</code></td>
<td>By default, no IPv4 BGP peers exist.</td>
</tr>
</tbody>
</table>

### Step 5. Add the peer into the EBGP peer group.

<table>
<thead>
<tr>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>peer ipv4-address [ mask-length ] group group-name [ as-number as-number ]</code></td>
<td>By default, no peers exist in the peer group. The <code>as-number</code> option, if used, must specify the same AS number as the <code>peer ipv4-address [ mask-length ] as-number as-number</code> command.</td>
</tr>
</tbody>
</table>

### Step 6. (Optional.) Configure a description for the peer group.

<table>
<thead>
<tr>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>peer group-name description text</code></td>
<td>By default, no description is configured for the peer group.</td>
</tr>
</tbody>
</table>

### Step 7. Create the BGP IPv4 unicast address family or BGP-VPN IPv4 unicast address family and enter its view.

<table>
<thead>
<tr>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>address-family ipv4 [ unicast ]</code></td>
<td>By default, no BGP IPv4 unicast address family or BGP-VPN IPv4 unicast address family exists.</td>
</tr>
</tbody>
</table>

### Step 8. Enable the router to exchange IPv4 unicast routing information with peers in the specified peer group.

<table>
<thead>
<tr>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>peer group-name enable</code></td>
<td>By default, the router cannot exchange IPv4 unicast routing information with the peers.</td>
</tr>
</tbody>
</table>

To configure an EBGP peer group by using Method 2 (IPv6 unicast address family):

### Step 1. Enter system view.

<table>
<thead>
<tr>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
</tbody>
</table>

### Step 2. Enter BGP instance view or BGP-VPN instance view.

<table>
<thead>
<tr>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>- Enter BGP instance view: </code></td>
<td>N/A</td>
</tr>
<tr>
<td><code>- Enter BGP-VPN instance view:</code></td>
<td></td>
</tr>
<tr>
<td><code>- a. bgp as-number [ instance instance-name ]</code></td>
<td></td>
</tr>
<tr>
<td><code>- b. ip vpn-instance vpn-instance-name</code></td>
<td></td>
</tr>
</tbody>
</table>

### Step 3. Create an EBGP peer group.

<table>
<thead>
<tr>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>group group-name external</code></td>
<td>By default, no EBGP peer groups exist.</td>
</tr>
</tbody>
</table>

### Step 4. Create an IPv6 BGP peer and specify its AS number.

<table>
<thead>
<tr>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>peer ipv6-address [ prefix-length ] as-number as-number</code></td>
<td>By default, no IPv6 BGP peers exist.</td>
</tr>
</tbody>
</table>

### Step 5. Add the peer into the EBGP peer group.

<table>
<thead>
<tr>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>peer ipv6-address [ prefix-length ] group group-name [ as-number as-number ]</code></td>
<td>By default, no peers exist in the peer group. The <code>as-number</code> option, if used, must specify the same AS number as the <code>peer ipv4-address [ mask-length ] as-number as-number</code> command.</td>
</tr>
</tbody>
</table>
### To configure an EBGP peer group by using Method 2 (IPv4 multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP instance view.</td>
<td>bgp as-number [ instance instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Create an EBGP peer group.</td>
<td>group group-name external</td>
</tr>
<tr>
<td>4.</td>
<td>Create an IPv4 BGP peer and specify its AS number.</td>
<td>peer ipv4-address [ mask-length ] as-number as-number</td>
</tr>
<tr>
<td>5.</td>
<td>Add the peer into the EBGP peer group.</td>
<td>peer ipv4-address [ mask-length ] group group-name [ as-number as-number ]</td>
</tr>
<tr>
<td>6.</td>
<td>(Optional.) Configure a description for the peer group.</td>
<td>peer group-name description text</td>
</tr>
<tr>
<td>7.</td>
<td>Create the BGP IPv4 multicast address family and enter its view.</td>
<td>address-family ipv4 multicast</td>
</tr>
<tr>
<td>8.</td>
<td>Enable the router to exchange IPv4 unicast routing information used for RPF check with peers in the specified peer group.</td>
<td>peer group-name enable</td>
</tr>
</tbody>
</table>

### To configure an EBGP peer group by using Method 2 (IPv6 multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP instance view.</td>
<td>bgp as-number [ instance instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Create an EBGP peer group.</td>
<td>group group-name external</td>
</tr>
</tbody>
</table>
### Step 4: Create an IPv6 BGP peer and specify its AS number.

<table>
<thead>
<tr>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
</table>
| peer ipv6-address [ prefix-length ]
  as-number as-number     | By default, no IPv6 BGP peers exist.         |

### Step 5: Add the peer into the EBGP peer group.

<table>
<thead>
<tr>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
</table>
| peer ipv6-address [ prefix-length ]
  group group-name [ as-number as-number ] | By default, no peers exist in the peer group. The as-number as-number option, if used, must specify the same AS number as the peer ipv6-address [ prefix-length ] as-number as-number command. |

### Step 6: (Optional.) Configure a description for the peer group.

<table>
<thead>
<tr>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer group-name description text</td>
<td>By default, no description is configured for the peer group.</td>
</tr>
</tbody>
</table>

### Step 7: Create the BGP IPv6 multicast address family and enter its view.

<table>
<thead>
<tr>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>address-family ipv6 multicast</td>
<td>By default, no BGP IPv6 multicast address family exists.</td>
</tr>
</tbody>
</table>

### Step 8: Enable the router to exchange IPv6 unicast routing information used for RPF check with peers in the specified peer group.

<table>
<thead>
<tr>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer group-name enable</td>
<td>By default, the router cannot exchange IPv6 unicast routing information used for RPF check with the peers in the group.</td>
</tr>
</tbody>
</table>

### To configure an EBGP peer group by using Method 3 (IPv4 unicast address family):

#### Step 1: Enter system view.

<table>
<thead>
<tr>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>system-view</td>
<td>N/A</td>
</tr>
</tbody>
</table>

#### Step 2: Enter BGP instance view or BGP-VPN instance view.

<table>
<thead>
<tr>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>group group-name external</td>
<td>N/A</td>
</tr>
</tbody>
</table>
| • Enter BGP instance view: bgp as-number [ instance instance-name ]
  • Enter BGP-VPN instance view:
    a. bgp as-number [ instance instance-name ]
    b. ip vpn-instance
    vpn-instance-name | N/A     |

#### Step 3: Create an EBGP peer group.

<table>
<thead>
<tr>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
</table>
| peer ipv4-address [ mask-length ]
  group group-name as-number | By default, no peers exist in the peer group. |

#### Step 5: (Optional.) Configure a description for the peer group.

<table>
<thead>
<tr>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer group-name description text</td>
<td>By default, no description is configured for the peer group.</td>
</tr>
</tbody>
</table>

#### Step 6: Create the BGP IPv4 unicast address family or BGP-VPN IPv4 unicast address family and enter its view.

<table>
<thead>
<tr>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>address-family ipv4 [ unicast ]</td>
<td>By default, no BGP IPv4 unicast address family or BGP-VPN IPv4 unicast address family exists.</td>
</tr>
</tbody>
</table>

#### Step 7: Enable the router to exchange IPv4 unicast routing information with peers in the specified peer group.

<table>
<thead>
<tr>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer group-name enable</td>
<td>By default, the router cannot exchange IPv4 unicast routing information with the peers.</td>
</tr>
</tbody>
</table>
To configure an EBGP peer group by using Method 3 (IPv6 unicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view N/A</td>
</tr>
</tbody>
</table>
| 2.   | Enter BGP instance view or BGP-VPN instance view. | - Enter BGP instance view: `bgp as-number [ instance instance-name ]`  
- Enter BGP-VPN instance view:  
  a. `bgp as-number [ instance instance-name ]`  
  b. `ip vpn-instance vpn-instance-name` | N/A |
| 3.   | Create an EBGP peer group. | `group group-name external` By default, no EBGP peer groups exist. |
| 4.   | Add a peer into the EBGP peer group. | `peer ipv6-address [ prefix-length ] group group-name as-number` By default, no peers exist in the peer group. |
| 5.   | (Optional.) Configure a description for the peer group. | `peer group-name description text` By default, no description is configured for the peer group. |
| 6.   | Create the BGP IPv6 unicast address family or BGP-VPN IPv6 unicast address family and enter its view. | `address-family ipv6 [ unicast ]` By default, no BGP IPv6 unicast address family or BGP-VPN IPv6 unicast address family exists. |
| 7.   | Enable the router to exchange IPv6 unicast routing information with peers in the specified peer group. | `peer group-name enable` By default, the router cannot exchange IPv6 unicast routing information with the peers. |

To configure an EBGP peer group by using Method 3 (IPv4 multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP instance view.</td>
<td><code>bgp as-number [ instance instance-name ]</code> N/A</td>
</tr>
<tr>
<td>3.</td>
<td>Create an EBGP peer group.</td>
<td><code>group group-name external</code> By default, no EBGP peer groups exist.</td>
</tr>
<tr>
<td>4.</td>
<td>Add an IPv4 BGP peer into the EBGP peer group.</td>
<td><code>peer ipv4-address [ mask-length ] group group-name as-number</code> By default, no peers exist in the peer group.</td>
</tr>
<tr>
<td>5.</td>
<td>(Optional.) Configure a description for the peer group.</td>
<td><code>peer group-name description text</code> By default, no description is configured for the peer group.</td>
</tr>
<tr>
<td>6.</td>
<td>Create the BGP IPv4 multicast address family and enter its view.</td>
<td><code>address-family ipv4 multicast</code> By default, no BGP IPv4 multicast address family exists.</td>
</tr>
<tr>
<td>7.</td>
<td>Enable the router to exchange IPv4 unicast routing information used for RPF check with peers in the specified peer group.</td>
<td><code>peer group-name enable</code> By default, the router cannot exchange IPv4 unicast routing information used for RPF check with the peers.</td>
</tr>
</tbody>
</table>
To configure an EBGP peer group by using Method 3 (IPv6 multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP instance view.</td>
<td>bgp as-number [ instance instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Create an EBGP peer group.</td>
<td>group group-name external</td>
</tr>
<tr>
<td>4.</td>
<td>Add an IPv6 BGP peer into the EBGP peer group.</td>
<td>peer ipv6-address [ prefix-length ] group group-name as-number as-number</td>
</tr>
<tr>
<td>5.</td>
<td>(Optional.) Configure a description for the peer group.</td>
<td>peer group-name description text</td>
</tr>
<tr>
<td>6.</td>
<td>Create the BGP IPv6 multicast address family and enter its view.</td>
<td>address-family ipv6 multicast</td>
</tr>
<tr>
<td>7.</td>
<td>Enable the router to exchange IPv6 unicast routing information used for RPF check with peers in the specified peer group.</td>
<td>peer group-name enable</td>
</tr>
</tbody>
</table>

Specifying the source address of TCP connections

By default, BGP uses the primary IPv4/IPv6 address of the egress interface in the optimal route to a peer or peer group as the source address of TCP connections to the peer or peer group. You can change the source address in the following scenarios:

- If the peer's IPv4/IPv6 address belongs to an interface indirectly connected to the local router, specify that interface as the source interface for TCP connections on the peer. For example, interface A on the local end is directly connected to interface B on the peer. If you use the peer x.x.x.x as-number as-number command on the local end, and x.x.x.x is not the IPv4 address of interface B, you must do the following:
  a. Use the peer connect-interface command on the peer.
  b. Specify the interface whose IPv4 address is x.x.x.x as the source interface.

- If the source interface fails on a BGP router that has multiple links to a peer, BGP must re-establish TCP connections. To avoid this problem, use a loopback interface as the source interface or use the IP address of a loopback interface as the source address.

- If the BGP sessions use the IP addresses of different interfaces, specify a source address or source interface for each peer to establish multiple BGP sessions to a router. Specify a source address for each peer if the BGP sessions use the different addresses of the same interface. Otherwise, the local BGP router might fail to establish a TCP connection to a peer when it uses the optimal route to determine the source address.

To specify the source address of TCP connections (IPv4 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
### Generating BGP routes

BGP can generate routes in the following ways:
- Advertise local networks.
- Redistribute IGP routes.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP instance view or BGP-VPN instance view.</td>
<td>* Enter BGP instance view: &lt;br&gt;<code>bgp as-number [ instance instance-name ]</code>&lt;br&gt;* Enter BGP-VPN instance view:&lt;br&gt;a. <code>bgp as-number [ instance instance-name ]</code>&lt;br&gt;b. <code>ip vpn-instance vpn-instance-name</code></td>
</tr>
<tr>
<td>3.</td>
<td>Specify the source address of TCP connections to a peer or peer group.</td>
<td>peer (group-name</td>
</tr>
<tr>
<td>4.</td>
<td>Specify the source interface of TCP connections to a peer or peer group.</td>
<td>peer (group-name</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP instance view or BGP-VPN instance view.</td>
<td>* Enter BGP instance view: &lt;br&gt;<code>bgp as-number [ instance instance-name ]</code>&lt;br&gt;* Enter BGP-VPN instance view:&lt;br&gt;a. <code>bgp as-number [ instance instance-name ]</code>&lt;br&gt;b. <code>ip vpn-instance vpn-instance-name</code></td>
</tr>
<tr>
<td>3.</td>
<td>Specify the source IPv6 address of TCP connections to a peer or peer group.</td>
<td>peer (group-name</td>
</tr>
<tr>
<td>4.</td>
<td>Specify the source interface of TCP connections to a peer or peer group.</td>
<td>peer (group-name</td>
</tr>
</tbody>
</table>
Injecting a local network

Perform this task to inject a network in the local routing table to the BGP routing table, so BGP can advertise the network to BGP peers. The ORIGIN attribute of BGP routes advertised in this way is IGP. You can also use a routing policy to control route advertisement.

The specified network must be available and active in the local IP routing table.

To inject a local network (IPv4 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP IPv4 unicast address family view, BGP-VPN IPv4 unicast address family view, or BGP IPv4 multicast address family view.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enter BGP IPv4 unicast address family view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>a. bgp as-number [ instance instance-name ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. address-family ipv4 [ unicast ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enter BGP-VPN IPv4 unicast address family view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>c. bgp as-number [ instance instance-name ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>d. ip vpn-instance vpn-instance-name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>e. address-family ipv4 [ unicast ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enter BGP IPv4 multicast address family view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>f. bgp as-number [ instance instance-name ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>g. address-family ipv4 multicast</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Configure BGP to advertise a local network.</td>
<td>network ipv4-address [ mask</td>
</tr>
</tbody>
</table>

To inject a local network (IPv6 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
Step | Command | Remarks
--- | --- | ---
2. | Enter BGP IPv6 unicast address family view, BGP-VPN IPv6 unicast address family view, or BGP IPv6 multicast address family view. | • Enter BGP IPv6 unicast address family view:  
  a. `bgp as-number`
  b. `address-family ipv6`  
  • Enter BGP-VPN IPv6 unicast address family view:  
  c. `bgp as-number`
  d. `ip vpn-instance`
  e. `address-family ipv6`
  • Enter BGP IPv6 multicast address family view:  
  f. `bgp as-number`
  g. `address-family ipv6` multicast | N/A
3. | Configure BGP to advertise a local network. | `network ipv6-address prefix-length [ route-policy route-policy-name ]`  
  By default, BGP does not advertise local networks.

Redistributing IGP routes

Perform this task to configure route redistribution from an IGP to BGP.

By default, BGP does not redistribute default IGP routes. You can use the `default-route imported` command to redistribute default IGP routes into the BGP routing table.

Only active routes can be redistributed. To view route state information, use the `display ip routing-table protocol` or `display ipv6 routing-table protocol` command.

The ORIGIN attribute of BGP routes redistributed from IGPs is INCOMPLETE.

To configure BGP to redistribute IGP routes (IPv4 unicast/multicast address family):

Step | Command | Remarks
--- | --- | ---
1. | Enter system view. | `system-view` | N/A
### Step Command Remarks

2. Enter BGP IPv4 unicast address family view, BGP-VPN IPv4 unicast address family view, or BGP IPv4 multicast address family view.

- Enter BGP IPv4 unicast address family view:
  a. `bgp as-number`
     - `instance instance-name`
  b. `address-family ipv4 [ unicast ]`
- Enter BGP-VPN IPv4 unicast address family view:
  c. `bgp as-number`
     - `instance instance-name`
  d. `ip vpn-instance vpn-instance-name`
  e. `address-family ipv4 [ unicast ]`
- Enter BGP IPv4 multicast address family view:
  f. `bgp as-number`
     - `instance instance-name`
  g. `address-family ipv4 multicast`

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
</tr>
</tbody>
</table>
| 2.   | Enter BGP IPv4 unicast address family view, BGP-VPN IPv4 unicast address family view, or BGP IPv4 multicast address family view. | - Enter BGP IPv4 unicast address family view:  
  a. `bgp as-number`
     - `instance instance-name`
  b. `address-family ipv4 [ unicast ]`
  - Enter BGP-VPN IPv4 unicast address family view:  
  c. `bgp as-number`
     - `instance instance-name`
  d. `ip vpn-instance vpn-instance-name`
  e. `address-family ipv4 [ unicast ]`
  - Enter BGP IPv4 multicast address family view:  
  f. `bgp as-number`
     - `instance instance-name`
  g. `address-family ipv4 multicast` | N/A |
| 3.   | Enable route redistribution from the specified IGP into BGP. | `import-route protocol`
  - `{ process-id | all-processes }
    - `{ allow-direct | med med-value | route-policy route-policy-name }
  *` | By default, BGP does not redistribute IGP routes. |
| 4.   | (Optional.) Enable default route redistribution into BGP. | `default-route imported` | By default, BGP does not redistribute default routes. |

To configure BGP to redistribute IGP routes (IPv6 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
</tr>
</tbody>
</table>
Controlling route distribution and reception

This section describes how to control route distribution and reception.

Configuring BGP route summarization

Route summarization can reduce the number of redistributed routes and the routing table size. IPv4 BGP supports automatic route summarization and manual route summarization. Manual summarization takes precedence over automatic summarization. IPv6 BGP supports only manual route summarization.

The egress interface of a BGP summary route is Null 0 on the originating router. Therefore, a summary route must not be an optimal route on the originating router. Otherwise, BGP will fail to forward packets matching the route. If a summarized specific route has the same mask as the summary route, but has a lower priority, the summary route becomes the optimal route. To ensure correct packet forwarding, change the priority of the summary or specific route to make the specific route the optimal route.

Configuring automatic route summarization

Automatic route summarization enables BGP to summarize IGP subnet routes redistributed by the `import-route` command so BGP advertises only natural network routes.

To configure automatic route summarization (IPv4 unicast/multicast address family):
### Configuring BGP Address Family

#### Step 1. Enter system view.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>

- **Enter BGP IPv4 unicast address family view:**
  - bgp as-number
    - instance instance-name
  - address-family ipv4
    - unicast

- **Enter BGP-VPN IPv4 unicast address family view:**
  - bgp as-number
    - instance instance-name
  - ip vpn-instance
    - vpn-instance-name
  - address-family ipv4
    - unicast

- **Enter BGP IPv4 multicast address family view:**
  - bgp as-number
    - instance instance-name
  - address-family ipv4
    - multicast

#### Step 2. Enter BGP IPv4 unicast address family view, BGP-VPN IPv4 unicast address family view, or BGP IPv4 multicast address family view.

- Configure automatic route summarization.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>Configure automatic route summarization.</td>
<td>summary automatic</td>
</tr>
</tbody>
</table>

#### Configuring manual route summarization

By configuring manual route summarization, you can do the following:

- Summarize both redistributed routes and routes injected using the network command.
- Determine the mask length for a summary route.

To configure BGP manual route summarization (IPv4 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
### Step 2. Enter BGP IPv4 unicast address family view, BGP-VPN IPv4 unicast address family view, or BGP IPv4 multicast address family view.

- **Enter BGP IPv4 unicast address family view:**
  - `bgp as-number`
    - `[ instance instance-name ]`
  - `address-family ipv4`
    - `[ unicast ]`

- **Enter BGP-VPN IPv4 unicast address family view:**
  - `bgp as-number`
    - `[ instance instance-name ]`
  - `ip vpn-instance`
    - `vpn-instance-name`
  - `address-family ipv4`
    - `[ unicast ]`

- **Enter BGP IPv4 multicast address family view:**
  - `bgp as-number`
    - `[ instance instance-name ]`
  - `address-family ipv4`
    - `[ multicast ]`

### Step 3. Create a summary route in the BGP routing table.

- **aggregate ipv4-address**
  - `( mask | mask-length )`
  - `[ as-set ]`
  - `attribute-policy route-policy-name`
  - `detail-suppressed`
  - `origin-policy route-policy-name`
  - `suppress-policy route-policy-name`

By default, no summary routes are configured.

To configure BGP manual route summarization (IPv6 unicast/multicast address family):

### Step 1. Enter system view.

- `system-view`

### Step 2. Enter BGP IPv6 unicast address family view, or BGP IPv6 multicast address family view.

- **Enter BGP IPv6 unicast address family view:**
  - `bgp as-number`
    - `[ instance instance-name ]`
  - `address-family ipv6`
    - `[ unicast ]`

- **Enter BGP IPv6 multicast address family view:**
  - `bgp as-number`
    - `[ instance instance-name ]`
  - `address-family ipv6`
    - `[ multicast ]`
Step | Command | Remarks |
--- | --- | --- |
3. | Create a summary route in the IPv6 BGP routing table. **aggregate ipv6-address prefix-length [ as-set | attribute-policy route-policy-name | detail-suppressed | origin-policy route-policy-name | suppress-policy route-policy-name ]** | By default, no summary routes are configured. |

### Advertising optimal routes in the IP routing table

By default, BGP advertises optimal routes in the BGP routing table, which may not be optimal in the IP routing table. This task allows you to advertise BGP routes that are optimal in the IP routing table.

To enable BGP to advertise optimal routes in the IP routing table (IPv4 unicast):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP instance view.</td>
<td>bgp as-number [ instance instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Enable BGP to advertise optimal routes in the IP routing table.</td>
<td>advertise-rib-active</td>
</tr>
</tbody>
</table>

- Enter BGP IPv4 unicast address family view: **address-family ipv4 [ unicast ]**
- Enter BGP-VPN IPv4 unicast address family view:
  - a. *ip vpn-instance vpn-instance-name*
  - b. **address-family ipv4 [ unicast ]**

To enable BGP to advertise optimal routes in the IPv6 routing table (IPv6 unicast):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP instance view.</td>
<td>bgp as-number [ instance instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Enable BGP to advertise optimal routes in the IPv6 routing table.</td>
<td>advertise-rib-active</td>
</tr>
</tbody>
</table>
### Advertising a default route to a peer or peer group

Perform this task to advertise a default BGP route with the next hop being the advertising router to a peer or peer group.

To advertise a default route to a peer or peer group (IPv4 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td></td>
<td>• Enter BGP IPv4 unicast address family view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>a. bgp as-number [ instance instance-name ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. address-family ipv4 [ unicast ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter BGP-VPN IPv4 unicast address family view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>c. bgp as-number [ instance instance-name ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>d. ip vpn-instance vpn-instance-name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>e. address-family ipv4 [ unicast ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter BGP IPv4 multicast address family view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>f. bgp as-number [ instance instance-name ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>g. address-family ipv4 multicast</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP IPv4 unicast address family view, BGP-VPN IPv4 unicast address family view, or BGP IPv4 multicast address family view.</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Advertise a default route to a peer or peer group.</td>
<td>peer { group-name</td>
</tr>
</tbody>
</table>
### Limiting routes received from a peer or peer group

This feature can prevent attacks that send a large number of BGP routes to the router.

If the number of routes received from a peer or peer group exceeds the upper limit, the router takes one of the following actions based on your configuration:

- Tears down the BGP session to the peer or peer group and does not attempt to re-establish the session.
- Continues to receive routes from the peer or peer group and generates a log message.
- Retains the session to the peer or peer group, but it discards excess routes and generates a log message.
- Tears down the BGP session to the peer or peer group and, after a specific period of time, re-establishes a BGP session to the peer or peer group.

You can specify a percentage threshold for the router to generate a log message. When the ratio of the number of received routes to the maximum number reaches the percentage value, the router generates a log message.

To limit routes that a router can receive from a peer or peer group (IPv4 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP IPv6 unicast address family view, or BGP IPv6 multicast address family view.</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>Advertise a default route to a peer or peer group.</td>
<td>By default, no default route is advertised.</td>
</tr>
</tbody>
</table>
### 2. Enter BGP IPv4 unicast address family view, BGP-VPN IPv4 unicast address family view, or BGP IPv4 multicast address family view.

- **Enter BGP IPv4 unicast address family view:**
  - bgp as-number [ instance instance-name ]
  - address-family ipv4 [ unicast ]

- **Enter BGP-VPN IPv4 unicast address family view:**
  - bgp as-number [ instance instance-name ]
  - ip vpn-instance vpn-instance-name
  - address-family ipv4 [ unicast ]

- **Enter BGP IPv4 multicast address family view:**
  - bgp as-number [ instance instance-name ]
  - address-family ipv4 multicast

### 3. Specify the maximum number of routes that a router can receive from a peer or peer group.

- **peer**
  - group-name | ipv4-address [ mask-length ]
  - route-limit prefix-number [ { alert-only | discard | reconnect reconnect-time } | percentage-value ] *

By default, the number of routes that a router can receive from a peer or peer group is not limited.

---

To limit routes that a router can receive from a peer or peer group (IPv6 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
</tbody>
</table>

- **Enter BGP IPv6 unicast address family view, or BGP IPv6 multicast address family view.**

- **Enter BGP IPv6 unicast address family view:**
  - bgp as-number [ instance instance-name ]
  - address-family ipv6 [ unicast ]

- **Enter BGP IPv6 multicast address family view:**
  - bgp as-number [ instance instance-name ]
  - address-family ipv6 multicast

N/A
3. Specify the maximum number of routes that a router can receive from a peer or peer group.

```
peer { group-name | ipv6-address [ prefix-length ] } route-limit prefix-number [ { alert-only | discard | reconnect reconnect-time } | percentage-value ] *
```

By default, the number of routes that a router can receive from a peer or peer group is not limited.

### Configuring BGP route filtering policies

#### Configuration prerequisites

Before you configure BGP routing filtering policies, configure the following filters used for route filtering as needed:

- ACL (see *ACL and QoS Configuration Guide*).
- Prefix list (see "Configuring routing policies").
- Routing policy (see "Configuring routing policies").
- AS path list (see "Configuring routing policies").

#### Configuring BGP route distribution filtering policies

To configure BGP route distribution filtering policies, use the following methods:

- Use an ACL or prefix list to filter routing information advertised to all peers.
- Use a routing policy, ACL, AS path list, or prefix list to filter routing information advertised to a peer or peer group.

If you configure multiple filtering policies, apply them in the following sequence:

1. `filter-policy export`
2. `peer filter-policy export`
3. `peer as-path-acl export`
4. `peer prefix-list export`
5. `peer route-policy export`

Only routes passing all the configured policies can be advertised.

To configure BGP route distribution filtering policies (IPv4 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>2.</td>
<td>• Enter BGP IPv4 unicast address family view:</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>a. <code>bgp as-number</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>[ instance <code>instance-name</code> ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. <code>address-family ipv4</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>[ <code>unicast</code> ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter BGP-VPN IPv4 unicast address family view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>c. <code>bgp as-number</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>[ instance <code>instance-name</code> ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>d. <code>ip vpn-instance</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>vpn-instance-name</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>e. <code>address-family ipv4</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>[ <code>unicast</code> ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter BGP IPv4 multicast address family view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>f. <code>bgp as-number</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>[ instance <code>instance-name</code> ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>g. <code>address-family ipv4</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>multicast</code></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>• Reference an ACL or IP prefix list to filter advertised BGP routes:</td>
<td>Use at least one method.</td>
</tr>
<tr>
<td></td>
<td><code>filter-policy</code></td>
<td>By default, no BGP distribution filtering policy is configured.</td>
</tr>
<tr>
<td></td>
<td>`{ ipv4-acl-number</td>
<td>prefix-list prefix-list-name }`</td>
</tr>
<tr>
<td></td>
<td>export `direct</td>
<td>isis process-id</td>
</tr>
<tr>
<td></td>
<td>• Reference a routing policy to filter BGP routes advertised to a peer</td>
<td></td>
</tr>
<tr>
<td></td>
<td>or peer group:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>peer</code> `{ group-name</td>
<td>ipv4-address [ mask-length ] }`</td>
</tr>
<tr>
<td></td>
<td><code>route-policy route-policy-name export</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Reference an ACL to filter BGP routes advertised to a peer or peer</td>
<td></td>
</tr>
<tr>
<td></td>
<td>group: <code>peer</code> `{ group-name</td>
<td>ipv4-address [ mask-length ] } <code>filter-policy ipv4-acl-number export</code></td>
</tr>
<tr>
<td></td>
<td>• Reference an AS path list to filter BGP routes advertised to a peer</td>
<td></td>
</tr>
<tr>
<td></td>
<td>or peer group:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>peer</code> `{ group-name</td>
<td>ipv4-address [ mask-length ] } <code>as-path-acl as-path-acl-number export</code></td>
</tr>
<tr>
<td></td>
<td>• Reference an IPv4 prefix list to filter BGP routes advertised to a</td>
<td></td>
</tr>
<tr>
<td></td>
<td>peer or peer group:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>peer</code> `{ group-name</td>
<td>}`</td>
</tr>
</tbody>
</table>
To configure BGP route distribution filtering policies (IPv6 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td></td>
<td>• Enter BGP IPv6 unicast address family view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>a. bgp as-number</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. address-family ipv6</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter BGP-VPN IPv6 unicast address family view:</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>c. bgp as-number</td>
<td></td>
</tr>
<tr>
<td></td>
<td>d. ip vpn-instance</td>
<td></td>
</tr>
<tr>
<td></td>
<td>e. address-family ipv6</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter BGP IPv6 multicast address family view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>f. bgp as-number</td>
<td></td>
</tr>
<tr>
<td></td>
<td>g. address-family ipv6 multicast</td>
<td></td>
</tr>
</tbody>
</table>

• ipv4-address
  [ mask-length ] \) prefix-list
  prefix-list-name export
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td>Configure BGP route distribution filtering policies.</td>
<td>Use at least one method. Not configured by default.</td>
</tr>
</tbody>
</table>

### Configuring BGP route reception filtering policies

You can use the following methods to configure BGP route reception filtering policies:

- Use an ACL or prefix list to filter routing information received from all peers.
- Use a routing policy, ACL, AS path list, or prefix list to filter routing information received from a peer or peer group.

If you configure multiple filtering policies, apply them in the following sequence:

1. `filter-policy import`
2. `peer filter-policy import`
3. `peer as-path-acl import`
4. `peer prefix-list import`
5. `peer route-policy import`

Only routes passing all the configured policies can be received.

To configure BGP route reception filtering policies (IPv4 unicast/multicast address family):
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td></td>
<td>• Enter BGP IPv4 unicast address family view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>a. bgp as-number [ instance instance-name ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. address-family ipv4 [ unicast ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter BGP-VPN IPv4 unicast address family view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>c. bgp as-number [ instance instance-name ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>d. ip vpn-instance vpn-instance-name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>e. address-family ipv4 [ unicast ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter BGP IPv4 multicast address family view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>f. bgp as-number [ instance instance-name ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>g. address-family ipv4 multicast</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP IPv4 unicast address family view, BGP-VPN IPv4 unicast address family view, or BGP IPv4 multicast address family view.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Reference an ACL or IP prefix list to filter BGP routes received from all peers:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>filter-policy { ipv4-acl-number</td>
<td>prefix-list prefix-list-name } import</td>
</tr>
<tr>
<td></td>
<td>• Reference a routing policy to filter BGP routes received from a peer or peer group:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>peer { group-name</td>
<td>ipv4-address [ mask-length ] } route-policy route-policy-name import</td>
</tr>
<tr>
<td></td>
<td>• Reference an ACL to filter BGP routes received from a peer or peer group:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>peer { group-name</td>
<td>ipv4-address [ mask-length ] } filter-policy ipv4-acl-number import</td>
</tr>
<tr>
<td></td>
<td>• Reference an AS path list to filter BGP routes received from a peer or peer group:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>peer { group-name</td>
<td>ipv4-address [ mask-length ] } as-path-acl as-path-acl-number import</td>
</tr>
<tr>
<td></td>
<td>• Reference an IPv4 prefix list to filter BGP routes received from a peer or peer group:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>peer { group-name</td>
<td>ipv4-address [ mask-length ] } prefix-list prefix-list-name import</td>
</tr>
</tbody>
</table>

To configure BGP route reception filtering policies (IPv6 unicast/multicast address family):
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP IPv6 unicast address family view, BGP-VPN IPv6 unicast address family view, or BGP IPv6 multicast address family view.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter BGP IPv6 unicast address family view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>a. bgp as-number [ instance instance-name ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. address-family ipv6 [ unicast ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter BGP-VPN IPv6 unicast address family view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>c. bgp as-number [ instance instance-name ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>d. ip vpn-instance vpn-instance-name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>e. address-family ipv6 [ unicast ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter BGP IPv6 multicast address family view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>f. bgp as-number [ instance instance-name ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>g. address-family ipv6 multicast</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Configure BGP route reception filtering policies.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Reference ACL or IPv6 prefix list to filter BGP routes received from all peers:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>filter-policy { ipv6-acl-number</td>
<td>prefix-list ipv6-prefix-name }</td>
</tr>
<tr>
<td></td>
<td>• Reference a routing policy to filter BGP routes received from a peer or peer group:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>peer { group-name</td>
<td>ipv6-address [ prefix-length ] } route-policy route-policy-name import</td>
</tr>
<tr>
<td></td>
<td>• Reference an ACL to filter BGP routes received from a peer or peer group:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>peer { group-name</td>
<td>ipv6-address [ prefix-length ] } filter-policy ipv6-acl-number import</td>
</tr>
<tr>
<td></td>
<td>• Reference an AS path list to filter BGP routes received from a peer or peer group:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>peer { group-name</td>
<td>ipv6-address [ prefix-length ] } as-path-acl as-path-acl-number import</td>
</tr>
<tr>
<td></td>
<td>• Reference an IPv6 prefix list to filter BGP routes received from a peer or peer group:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>peer { group-name</td>
<td>ipv6-address [ prefix-length ] } prefix-list ipv6-prefix-name import</td>
</tr>
</tbody>
</table>
Configuring BGP route update delay

Perform this task to configure BGP to delay sending route updates on reboot to reduce traffic loss. With this feature enabled, BGP redistributes all routes from other neighbors on reboot, selects the optimal route, and then advertises it.

To configure BGP route update delay:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>bgp as-number [ instance instance-name ]</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>bgp update-delay on-startup seconds</td>
<td>By default, BGP immediately sends route updates on reboot.</td>
</tr>
<tr>
<td>4.</td>
<td>bgp update-delay on-startup prefix-list prefix-list-name</td>
<td>By default, no prefix list is specified to filter routes. Use this command when the updates for the specified routes must be immediately sent. This command is available only to IPv4 prefix lists.</td>
</tr>
</tbody>
</table>

Configuring BGP route dampening

Route dampening enables BGP to not select unstable routes as optimal routes. This feature applies to EBGP routes but not to IBGP routes.

To configure BGP route dampening (IPv4 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>bgp as-number [ instance instance-name ]</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>address-family ipv4 [ unicast ]</td>
<td>N/A</td>
</tr>
<tr>
<td>4.</td>
<td>bgp as-number [ instance instance-name ]</td>
<td>N/A</td>
</tr>
<tr>
<td>5.</td>
<td>ip vpn-instance vpn-instance-name</td>
<td>N/A</td>
</tr>
<tr>
<td>6.</td>
<td>address-family ipv4 [ unicast ]</td>
<td>N/A</td>
</tr>
<tr>
<td>7.</td>
<td>bgp as-number [ instance instance-name ]</td>
<td>N/A</td>
</tr>
<tr>
<td>8.</td>
<td>address-family ipv4 multicast</td>
<td>N/A</td>
</tr>
</tbody>
</table>
To configure BGP route dampening (IPv6 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP IPv6 unicast address family view, BGP-VPN IPv6 unicast address family view, or BGP IPv6 multicast address family view.</td>
<td>system-view</td>
</tr>
<tr>
<td>3.</td>
<td>Configure IPv6 BGP route dampening.</td>
<td>system-view</td>
</tr>
</tbody>
</table>

**Controlling BGP path selection**

By configuring BGP path attributes, you can control BGP path selection.

**Setting a preferred value for routes received**

Perform this task to set a preferred value for specific routes to control BGP path selection.

Among multiple routes that have the same destination/mask and are learned from different peers, the one with the greatest preferred value is selected as the optimal route.

To set a preferred value for routes from a peer or peer group (IPv4 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
### Step 1: Enter system view.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
</tbody>
</table>

### Step 2: Enter BGP IPv4 unicast address family view, BGP-VPN IPv4 unicast address family view, or BGP IPv4 multicast address family view.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
</table>
| 2.   | • Enter BGP IPv4 unicast address family view:  
   a. `bgp as-number [ instance instance-name ]`  
   b. `address-family ipv4 [ unicast ]`  
   • Enter BGP-VPN IPv4 unicast address family view:  
   c. `bgp as-number [ instance instance-name ]`  
   d. `ip vpn-instance vpn-instance-name`  
   e. `address-family ipv4 [ unicast ]`  
   • Enter BGP IPv4 multicast address family view:  
   f. `bgp as-number [ instance instance-name ]`  
   g. `address-family ipv4 multicast` | N/A |

### Step 3: Set a preferred value for routes received from a peer or peer group.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td>`peer { group-name</td>
<td>ipv4-address [ mask-length ] } preferred-value value`</td>
</tr>
</tbody>
</table>

To set a preferred value for routes from a peer or peer group (IPv6 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
</tbody>
</table>

### Step 2: Enter BGP IPv6 unicast address family view, BGP-VPN IPv6 unicast address family view, or BGP IPv6 multicast address family view.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
</table>
| 2.   | • Enter BGP IPv6 unicast address family view:  
   a. `bgp as-number [ instance instance-name ]`  
   b. `address-family ipv6 [ unicast ]`  
   • Enter BGP-VPN IPv6 unicast address family view:  
   c. `bgp as-number [ instance instance-name ]`  
   d. `ip vpn-instance vpn-instance-name`  
   e. `address-family ipv6 [ unicast ]`  
   • Enter BGP IPv6 multicast address family view:  
   f. `bgp as-number [ instance instance-name ]`  
   g. `address-family ipv6 multicast` | N/A |
### Configuring preferences for BGP routes

Routing protocols each have a default preference. If they find multiple routes destined for the same network, the route found by the routing protocol with the highest preference is selected as the optimal route.

You can use the `preference` command to modify preferences for EBGP, IBGP, and local BGP routes, or use a routing policy to set a preference for matching routes. For routes not matching the routing policy, the default preference applies.

If a device has an EBGP route and a local BGP route to reach the same destination, it does not select the EBGP route because the EBGP route has a lower preference than the local BGP route by default. You can use the `network short-cut` command to configure the EBGP route as a shortcut route that has the same preference as the local BGP route. The EBGP route will more likely become the optimal route.

To configure preferences for BGP routes (IPv4 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>• Enter BGP IPv4 unicast address family view:</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>a. <code>bgp as-number [ instance instance-name ]</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. <code>address-family ipv4 [ unicast ]</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter BGP-VPN IPv4 unicast address family view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>c. <code>bgp as-number [ instance instance-name ]</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>d. <code>ip vpn-instance vpn-instance-name</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>e. <code>address-family ipv4 [ unicast ]</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter BGP IPv4 multicast address family view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>f. <code>bgp as-number [ instance instance-name ]</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>g. <code>address-family ipv4 multicast</code></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td><code>preference { external-preference internal-preference local-preference [ route-policy route-policy-name ] }</code></td>
<td>The default preferences for EBGP, IBGP, and local BGP routes are 255, 255, and 130.</td>
</tr>
<tr>
<td>4.</td>
<td>`network ipv4-address [ mask</td>
<td>mask-length ] short-cut`</td>
</tr>
</tbody>
</table>
To configure preferences for BGP routes (IPv6 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP IPv6 unicast address family view, BGP-VPN IPv6 unicast address family view, or BGP IPv6 multicast address family view.</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• Enter BGP IPv6 unicast address family view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>a. bgp as-number [instance instance-name]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. address-family ipv6 [unicast]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter BGP-VPN IPv6 unicast address family view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>c. bgp as-number [instance instance-name]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>d. ip vpn-instance vpn-instance-name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>e. address-family ipv6 [unicast]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter BGP IPv6 multicast address family view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>f. bgp as-number [instance instance-name]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>g. address-family ipv6 multicast</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Configure preferences for EBGP, IBGP, and local BGP routes.</td>
<td>preference {external-preference internal-preference local-preference</td>
</tr>
<tr>
<td>4.</td>
<td>Configure an EBGP route as a shortcut route.</td>
<td>network ipv6-address prefix-length short-cut</td>
</tr>
</tbody>
</table>

Configuring the default local preference

The local preference is used to determine the optimal route for traffic leaving the local AS. When a BGP router obtains from several IBGP peers multiple routes to the same destination, but with different next hops, it considers the route with the highest local preference as the optimal route.

This task allows you to specify the default local preference for routes sent to IBGP peers.

To specify the default local preference (IPv4 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP IPv4 unicast address family view, BGP-VPN IPv4 unicast address family view, or BGP IPv4 multicast address family view.</td>
<td>N/A</td>
</tr>
</tbody>
</table>
|      | • Enter BGP IPv4 unicast address family view:  
  a. `bgp as-number [ instance instance-name ]`  
  b. `address-family ipv4 [ unicast ]`  
  • Enter BGP-VPN IPv4 unicast address family view:  
  c. `bgp as-number [ instance instance-name ]`  
  d. `ip vpn-instance vpn-instance-name`  
  e. `address-family ipv4 [ unicast ]`  
  • Enter BGP IPv4 multicast address family view:  
  f. `bgp as-number [ instance instance-name ]`  
  g. `address-family ipv4 multicast` | |
| 3.   | Configure the default local preference. | `default local-preference value`  
  The default local preference is 100. |

To specify the default local preference (IPv6 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
</table>
| 1.   | Enter system view. | `system-view`  
  N/A |
| 2.   | Enter BGP IPv6 unicast address family view, BGP-VPN IPv6 unicast address family view, or BGP IPv6 multicast address family view. | N/A |
|      | • Enter BGP IPv6 unicast address family view:  
  a. `bgp as-number [ instance instance-name ]`  
  b. `address-family ipv6 [ unicast ]`  
  • Enter BGP-VPN IPv6 unicast address family view:  
  c. `bgp as-number [ instance instance-name ]`  
  d. `ip vpn-instance vpn-instance-name`  
  e. `address-family ipv6 [ unicast ]`  
  • Enter BGP IPv6 multicast address family view:  
  f. `bgp as-number [ instance instance-name ]`  
  g. `address-family ipv6 multicast` | |
### Configuring the MED attribute

BGP uses MED to determine the optimal route for traffic going into an AS. When a BGP router obtains multiple routes with the same destination but with different next hops, it considers the route with the smallest MED value as the optimal route if other conditions are the same.

#### Configuring the default MED value

To configure the default MED value (IPv4 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP IPv4 unicast address family view, BGP-VPN IPv4 unicast address family view, or BGP IPv4 multicast address family view.</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• Enter BGP IPv4 unicast address family view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>a. bgp as-number [ instance instance-name ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. address-family ipv4 [ unicast ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter BGP-VPN IPv4 unicast address family view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>c. bgp as-number [ instance instance-name ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>d. ip vpn-instance vpn-instance-name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>e. address-family ipv4 [ unicast ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter BGP IPv4 multicast address family view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>f. bgp as-number [ instance instance-name ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>g. address-family ipv4 multicast</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Configure the default MED value.</td>
<td>default med med-value</td>
</tr>
</tbody>
</table>

To configure the default MED value (IPv6 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Step | Command | Remarks
--- | --- | ---
2. | Enter BGP IPv6 unicast address family view, BGP-VPN IPv6 unicast address family view, or BGP IPv6 multicast address family view. | • Enter BGP IPv6 unicast address family view:
  a. `bgp as-number [ instance instance-name ]`
  b. `address-family ipv6 [ unicast ]`
• Enter BGP-VPN IPv6 unicast address family view:
  c. `bgp as-number [ instance instance-name ]`
  d. `ip vpn-instance vpn-instance-name`
  e. `address-family ipv6 [ unicast ]`
• Enter BGP IPv6 multicast address family view:
  f. `bgp as-number [ instance instance-name ]`
  g. `address-family ipv6 multicast`
| N/A | 
3. | Configure the default MED value. | `default med med-value`
The default MED value is 0.

Enabling MED comparison for routes from different ASs
This task enables BGP to compare the MEDs of routes from different ASs.
To enable MED comparison for routes from different ASs:

Step | Command | Remarks
--- | --- | ---
1. | Enter system view. | `system-view`
| | | N/A

2. | Enter BGP instance view or BGP-VPN instance view. | • Enter BGP instance view:
  `bgp as-number [ instance instance-name ]`
• Enter BGP-VPN instance view:
  a. `bgp as-number [ instance instance-name ]`
  b. `ip vpn-instance vpn-instance-name`
| | N/A

3. | Enable MED comparison for routes from different ASs. | `compare-different-as-med`
| | By default, MED comparison for routes from different ASs is disabled.

Enabling MED comparison for routes on a per-AS basis
This task enables BGP to compare the MEDs of routes from an AS.
As shown in Figure 61, Router D establishes indirect EIGP peer relationships with Router A, Router B, and Router C, and learns addresses 1.1.1.1/32, 2.2.2.2/32, and 3.3.3.3/32 through OSPF. The following output shows the routing information on Router D.

<table>
<thead>
<tr>
<th>Destination/Mask</th>
<th>Proto</th>
<th>Pre</th>
<th>Cost</th>
<th>NextHop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.1/32</td>
<td>O_INTRA</td>
<td>10</td>
<td>10</td>
<td>11.1.1.2</td>
<td>GE1/0/1</td>
</tr>
<tr>
<td>2.2.2.2/32</td>
<td>O_INTRA</td>
<td>10</td>
<td>20</td>
<td>12.1.1.2</td>
<td>GE1/0/2</td>
</tr>
<tr>
<td>3.3.3.3/32</td>
<td>O_INTRA</td>
<td>10</td>
<td>30</td>
<td>13.1.1.2</td>
<td>GE1/0/3</td>
</tr>
</tbody>
</table>

Router D learns network 10.0.0.0 from both Router A and Router B. Because the route learned from Router B has a smaller IGP metric, the route is optimal. The following output shows the BGP routing table on Router D.

<table>
<thead>
<tr>
<th>Network</th>
<th>NextHop</th>
<th>MED</th>
<th>LocPrf</th>
<th>PrefVal</th>
<th>Path/Ogn</th>
</tr>
</thead>
<tbody>
<tr>
<td>*e 10.0.0.0</td>
<td>2.2.2.2</td>
<td>50</td>
<td>0</td>
<td>300</td>
<td>400e</td>
</tr>
<tr>
<td>* e 10.0.0.0</td>
<td>3.3.3.3</td>
<td>50</td>
<td>0</td>
<td>200</td>
<td>400e</td>
</tr>
</tbody>
</table>

When Router D learns network 10.0.0.0 from Router C, it compares the route with the optimal route in its routing table. Because Router C and Router B reside in different ASs, BGP does not compare the MEDs of the two routes. The route from Router C has a smaller IGP metric than the route from Router B, so the route from Router C becomes optimal. The following output shows the BGP routing table on Router D.

<table>
<thead>
<tr>
<th>Network</th>
<th>NextHop</th>
<th>MED</th>
<th>LocPrf</th>
<th>PrefVal</th>
<th>Path/Ogn</th>
</tr>
</thead>
<tbody>
<tr>
<td>*e 10.0.0.0</td>
<td>1.1.1.1</td>
<td>60</td>
<td>0</td>
<td>200</td>
<td>400e</td>
</tr>
<tr>
<td>* e 10.0.0.0</td>
<td>2.2.2.2</td>
<td>50</td>
<td>0</td>
<td>300</td>
<td>400e</td>
</tr>
<tr>
<td>* e 10.0.0.0</td>
<td>3.3.3.3</td>
<td>50</td>
<td>0</td>
<td>200</td>
<td>400e</td>
</tr>
</tbody>
</table>

However, Router C and Router A reside in the same AS, and Router C has a greater MED, so network 10.0.0.0 learned from Router C should not be optimal.

To avoid this problem, you can configure the `bestroute compare-med` command to enable MED comparison for routes from the same AS on Router D. After that, Router D puts the routes received from each AS into a group, selects the route with the lowest MED from each group, and compares routes from different groups. Network 10.0.0.0 learned from Router B is the optimal route. The following output shows the BGP routing table on Router D.

<table>
<thead>
<tr>
<th>Network</th>
<th>NextHop</th>
<th>MED</th>
<th>LocPrf</th>
<th>PrefVal</th>
<th>Path/Ogn</th>
</tr>
</thead>
<tbody>
<tr>
<td>*e 10.0.0.0</td>
<td>2.2.2.2</td>
<td>50</td>
<td>0</td>
<td>300</td>
<td>400e</td>
</tr>
</tbody>
</table>
To enable MED comparison for routes on a per-AS basis:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
| 2.   | Enter BGP instance view or BGP-VPN instance view. | • Enter BGP instance view: `bgp as-number [ instance instance-name ]`
                           • Enter BGP-VPN instance view:
                             a. `bgp as-number [ instance instance-name ]`
                             b. `ip vpn-instance vpn-instance-name`
                           N/A |
| 3.   | Enable MED comparison for routes on a per-AS basis. | `bestroute compare-med` | By default, MED comparison for routes on a per-AS basis is disabled. |

Enabling MED comparison for routes from confederation peers

This task enables BGP to compare the MEDs of routes received from confederation peers. However, if a route received from a confederation peer has an AS number that does not belong to the confederation, BGP does not compare the route with other routes. For example, a confederation has three AS numbers 65006, 65007, and 65009. BGP receives three routes from different confederation peers. The AS_PATH attributes of these routes are 65006 65009, 65007 65009, and 65008 65009, and the MED values of them are 2, 3, and 1. Because the third route’s AS_PATH attribute contains AS number 65008 that does not belong to the confederation, BGP does not compare it with other routes. As a result, the first route becomes the optimal route.

To enable MED comparison for routes from confederation peers:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
| 2.   | Enter BGP instance view or BGP-VPN instance view. | • Enter BGP instance view: `bgp as-number [ instance instance-name ]`
                           • Enter BGP-VPN instance view:
                             a. `bgp as-number [ instance instance-name ]`
                             b. `ip vpn-instance vpn-instance-name`
                           N/A |
| 3.   | Enable MED comparison for routes from confederation peers. | `bestroute med-confederation` | By default, MED comparison for routes from confederation peers is disabled. |

Configuring the NEXT_HOP attribute

By default, a BGP router does not set itself as the next hop for routes advertised to an IBGP peer or peer group. In some cases, however, you must configure the advertising router as the next hop to ensure that the BGP peer can find the correct next hop.
For example, as shown in Figure 62, Router A and Router B establish an EBGP neighbor relationship, and Router B and Router C establish an IBGP neighbor relationship. If Router C has no route destined for IP address 1.1.1.1/24, you must configure Router B to set itself 3.1.1.1/24 as the next hop for the network 2.1.1.1/24 advertised to Router C.

Figure 62 NEXT_HOP attribute configuration

If a BGP router has two peers on a broadcast network, it does not set itself as the next hop for routes sent to an EBGP peer by default. As shown in Figure 63, Router A and Router B establish an EBGP neighbor relationship, and Router B and Router C establish an IBGP neighbor relationship. They are on the same broadcast network 1.1.1.0/24. When Router B sends EBGP routes to Router A, it does not set itself as the next hop by default. However, you can configure Router B to set it (1.1.1.2/24) as the next hop for routes sent to Router A by using the `peer next-hop-local` command as needed.

Figure 63 NEXT_HOP attribute configuration

**IMPORTANT:**

If you have configured BGP load balancing, the router sets itself as the next hop for routes sent to an IBGP peer or peer group regardless of whether the `peer next-hop-local` command is configured.

To configure the NEXT_HOP attribute (IPv4 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP IPv4 unicast address family view, BGP-VPN IPv4 unicast address family view, or BGP IPv4 multicast address family view.</td>
<td>By default, the router sets itself as the next hop for routes sent to an EBGP peer or peer group. However, it does not set itself as the next hop for routes sent to an IBGP peer or peer group.</td>
</tr>
<tr>
<td>3.</td>
<td>Specify the router as the next hop for routes sent to a peer or peer group.</td>
<td></td>
</tr>
</tbody>
</table>

To configure the NEXT_HOP attribute (IPv6 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP IPv6 unicast address family view, or BGP IPv6 multicast address family view.</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>Specify the router as the next hop for routes sent to a peer or peer group.</td>
<td>By default, the router sets itself as the next hop for routes sent to an EBGP peer or peer group. However, it does not set itself as the next hop for routes sent to an IBGP peer or peer group.</td>
</tr>
</tbody>
</table>
Configuring the AS_PATH attribute

Permitting local AS number to appear in routes from a peer or peer group

In general, BGP checks whether the AS_PATH attribute of a route from a peer contains the local AS number. If yes, it discards the route to avoid routing loops.

In certain network environments (for example, a Hub&Spoke network in MPLS L3VPN), however, the AS_PATH attribute of a route from a peer must be allowed to contain the local AS number. Otherwise, the route cannot be advertised correctly.

To permit the local AS number to appear in routes from a peer or peer group and specify the appearance times (IPv4 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
| 2.   | Enter BGP IPv4 unicast address family view, BGP-VPN IPv4 unicast address family view, or BGP IPv4 multicast address family view. | • Enter BGP IPv4 unicast address family view:  
  a. bgp as-number [instance instance-name]  
  b. address-family ipv4 [unicast]  
  • Enter BGP-VPN IPv4 unicast address family view:  
  c. bgp as-number [instance instance-name]  
  d. ip vpn-instance vpn-instance-name  
  e. address-family ipv4 [unicast]  
  • Enter BGP IPv4 multicast address family view:  
  f. bgp as-number [instance instance-name]  
  g. address-family ipv4 multicast | N/A |
| 3.   | Permit the local AS number to appear in routes from a peer or peer group and set the appearance times. | peer {group-name | ipv4-address [mask-length]} allow-as-loop [number] | By default, the local AS number is not allowed in routes from a peer or peer group. |

To permit the local AS number to appear in routes from a peer or peer group and specify the appearance times (IPv6 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>

262
### Ignoring the AS_PATH attribute during optimal route selection

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP instance view or BGP-VPN instance view.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter BGP instance view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- bgp as-number [ instance instance-name ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter BGP-VPN instance view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- bgp as-number [ instance instance-name ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- ip vpn-instance vpn-instance-name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter BGP IPv6 multicast address family view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- bgp as-number [ instance instance-name ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- address-family ipv6 multicast</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter system view.</td>
<td>bestroute as-path-neglect</td>
</tr>
</tbody>
</table>

### Advertising a fake AS number to a peer or peer group

After you move a BGP router from an AS to another AS (from AS 2 to AS 3 for example), you have to modify the AS number of the router on all its EBGP peers. To avoid such modifications, you can configure the router to advertise a fake AS number 2 to its EBGP peers so that the EBGP peers still think that Router A is in AS 2.

To advertise a fake AS number to a peer or peer group (IPv4 unicast/multicast address family):
### Configuring AS number substitution

**IMPORTANT:**
Do not configure AS number substitution in normal circumstances. Otherwise, routing loops might occur.

To use EBGP between PE and CE in MPLS L3VPN, VPN sites in different geographical areas should have different AS numbers. Otherwise, BGP discards route updates containing the local AS number. If two CEs connected to different PEs use the same AS number, you must configure AS number substitution on each PE. This substitution can replace the AS number in route updates originated by the remote CE as its own AS number before advertising them to the connected CE.
As shown in Figure 64, CE 1 and CE 2 use the same AS number 800. To ensure bidirectional communication between the two sites, configure AS number substitution on PE 2. PE 2 replaces AS 800 with AS 100 for the BGP route update originated from CE 1 before advertising it to CE 2. Perform the same configuration on PE 1.

To configure AS number substitution for a peer or peer group (IPv4 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td></td>
<td></td>
<td>N/A</td>
</tr>
</tbody>
</table>
| 2.   | Enter BGP instance view or BGP-VPN instance view. | • Enter BGP instance view: `bgp as-number [ instance instance-name ]`
|      |          | • Enter BGP-VPN instance view:
|      |          | a. `bgp as-number [ instance instance-name ]`
|      |          | b. `ip vpn-instance vpn-instance-name`
|      |          | N/A     |
| 3.   | Configure AS number substitution for a peer or peer group. | `peer { group-name | ipv4-address [ mask-length ] } substitute-as` |
|      |          | By default, AS number substitution is not configured. |

To configure AS number substitution for a peer or peer group (IPv6 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td></td>
<td></td>
<td>N/A</td>
</tr>
</tbody>
</table>
| 2.   | Enter BGP instance view or BGP-VPN instance view. | • Enter BGP instance view: `bgp as-number [ instance instance-name ]`
|      |          | • Enter BGP-VPN instance view:
|      |          | a. `bgp as-number [ instance instance-name ]`
|      |          | b. `ip vpn-instance vpn-instance-name`
|      |          | N/A     |
| 3.   | Configure AS number substitution for a peer or peer group. | `peer { group-name | ipv6-address [ prefix-length ] } substitute-as` |
|      |          | By default, AS number substitution is not configured. |
Removing private AS numbers from updates sent to an EBGP peer or peer group

Private AS numbers are typically used in test networks, and should not be transmitted in public networks. The range of private AS numbers is from 64512 to 65535.

To remove private AS numbers from updates sent to an EBGP peer or peer group (IPv4 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP IPv4 unicast address family view, BGP-VPN IPv4 unicast address family view, or BGP IPv4 multicast address family view.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter BGP IPv4 unicast address family view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>a. bgp as-number [ instance instance-name ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. address-family ipv4 [ unicast ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter BGP-VPN IPv4 unicast address family view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>c. bgp as-number [ instance instance-name ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>d. ip vpn-instance vpn-instance-name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>e. address-family ipv4 [ unicast ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter BGP IPv4 multicast address family view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>f. bgp as-number [ instance instance-name ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>g. address-family ipv4 multicast</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Configure BGP to remove private AS numbers from the AS_PATH attribute of updates sent to an EBGP peer or peer group.</td>
<td>peer { group-name</td>
</tr>
</tbody>
</table>

To remove private AS numbers from updates sent to an EBGP peer or peer group (IPv6 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| 2.   | Enter BGP IPv6 unicast address family view, BGP-VPN IPv6 unicast address family view, or BGP IPv6 multicast address family view. | • Enter BGP IPv6 unicast address family view:  
  a. `bgp as-number`  
     [ `instance name` ]  
  b. `address-family ipv6`  
     [ `unicast` ]  
  • Enter BGP-VPN IPv6 unicast address family view:  
  c. `bgp as-number`  
     [ `instance name` ]  
  d. `ip vpn-instance`  
     `vpn-instance-name`  
  e. `address-family ipv6`  
     [ `unicast` ]  
  • Enter BGP IPv6 multicast address family view:  
  f. `bgp as-number`  
     [ `instance name` ]  
  g. `address-family ipv6 multicast` | N/A |
| 3.   | Configure BGP to remove private AS numbers from the AS_PATH attribute of updates sent to an EBGP peer or peer group. | `peer { group-name | ipv6-address [ prefix-length ] } public-as-only`  
By default, BGP updates sent to an EBGP peer or peer group can carry both public and private AS numbers.  
This command is applicable only to EBGP peers or peer groups. |

**Ignoring the first AS number of EBGP route updates**

By default, BGP checks the first AS number of a received EBGP route update. If the first AS number is neither the AS number of the BGP peer nor a private AS number, the BGP router disconnects the BGP session to the peer.

To ignore the first AS number of EBGP route updates:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP instance view.</td>
<td><code>bgp as-number</code> [ <code>instance name</code> ]</td>
</tr>
<tr>
<td>3.</td>
<td>Configure BGP to ignore the first AS number of EBGP route updates.</td>
<td><code>ignore-first-as</code></td>
</tr>
</tbody>
</table>

**Ignoring IGP metrics during optimal route selection**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
</tbody>
</table>
Step | Command | Remarks
--- | --- | ---
2. | Enter BGP instance view or BGP-VPN instance view.  • Enter BGP instance view: `bgp as-number [ instance instance-name ]`  • Enter BGP-VPN instance view:  a. `bgp as-number [ instance instance-name ]`  b. `ip vpn-instance vpn-instance-name` | N/A
3. | **bestroute igp-metric-ignore** | By default, BGP considers IGP metrics during optimal route selection. If multiple routes to the same destination are available, BGP selects the route with the smallest IGP metric as the optimal route.

### Configuring the SoO attribute

After you configure the SoO attribute for a BGP peer or peer group, BGP adds the SoO attribute into the route updates received from the BGP peer or peer group. In addition, before advertising route updates to the peer or peer group, BGP checks the SoO attribute of the route update against the configured SoO attribute. If they are the same, BGP does not advertise the route updates to the BGP peer or peer group.

To configure the SoO attribute (IPv4 unicast/multicast address family):

Step | Command | Remarks
--- | --- | ---
1. | Enter system view. `system-view` | N/A
2. | Enter BGP IPv4 unicast address family view, BGP-VPN IPv4 unicast address family view, or BGP IPv4 multicast address family view.  • Enter BGP IPv4 unicast address family view:  a. `bgp as-number [ instance instance-name ]`  b. `address-family ipv4 [ unicast ]`  • Enter BGP-VPN IPv4 unicast address family view:  c. `bgp as-number [ instance instance-name ]`  d. `ip vpn-instance vpn-instance-name`  e. `address-family ipv4 [ unicast ]`  • Enter BGP IPv4 multicast address family view:  f. `bgp as-number [ instance instance-name ]`  g. `address-family ipv4 multicast` | N/A
### Step 3. Configure the SoO attribute for a peer or peer group.

```
peer { group-name | ipv4-address [ mask-length ] } soo site-of-origin
```

By default, no SoO attribute is configured for a peer or peer group.

---

**To configure the SoO attribute (IPv6 unicast/multicast address family):**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
</tbody>
</table>
| 2.   | • Enter BGP IPv6 unicast address family view:  
\a. bgp as-number [ instance instance-name ]  
\b. address-family ipv6 [ unicast ]  
• Enter BGP-VPN IPv6 unicast address family view:  
\c. bgp as-number [ instance instance-name ]  
\d. ip vpn-instance vpn-instance-name  
\e. address-family ipv6 [ unicast ]  
• Enter BGP IPv6 multicast address family view:  
\f. bgp as-number [ instance instance-name ]  
\g. address-family ipv6 multicast | N/A |
| 3.   | peer { group-name | ipv6-address [ prefix-length ] } soo site-of-origin | By default, no SoO attribute is configured for a peer or peer group. |

---

**Tuning and optimizing BGP networks**

This section describes how to tune and optimize BGP networks.

**Configuring the keepalive interval and hold time**

BGP sends keepalive messages regularly to keep the BGP session between two routers.

If a router receives no keepalive or update message from a peer within the hold time, it tears down the session.

You can configure the keepalive interval and hold time globally or for a peer or peer group. The individual settings take precedence over the global settings.

The actual keepalive interval and hold time are determined as follows:

- If the hold time settings on the local and peer routers are different, the smaller setting is used. If the hold time is 0, BGP does not send keepalive messages to its peers and never tears down the session.
- If the keepalive interval is not 0, the actual keepalive interval is the smaller one between 1/3 of the hold time and the keepalive interval.

To configure the keepalive interval and hold time (IPv4 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
</tbody>
</table>
| 2. Enter BGP instance view or BGP-VPN instance view. | • Enter BGP instance view: `bgp as-number [ instance instance-name ]`  
  • Enter BGP-VPN instance view: 
    a. `bgp as-number [ instance instance-name ]`  
    b. `ip vpn-instance vpn-instance-name` | N/A |
| 3. Configure the keepalive interval and hold time. | • Configure the global keepalive interval and hold time: `timer keepalive keepalive hold holdtime`  
  • Configure the keepalive interval and hold time for a peer or peer group: 
    peer { group-name | ipv4-address [ mask-length ] } `timer keepalive keepalive hold holdtime` | Use at least one method.  
By default, the keepalive interval is 60 seconds, and hold time is 180 seconds.  
The `timer` command takes effect for new BGP sessions and does not affect existing sessions.  
The timers configured with the `timer` and `peer timer` commands do not take effect until a session is re-established (for example, a session is reset).  
The hold time must be at least three times the keepalive interval. |

To configure the keepalive interval and hold time (IPv6 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
</tbody>
</table>
| 2. Enter BGP instance view or BGP-VPN instance view. | • Enter BGP instance view: `bgp as-number [ instance instance-name ]`  
  • Enter BGP-VPN instance view: 
    a. `bgp as-number [ instance instance-name ]`  
    b. `ip vpn-instance vpn-instance-name` | N/A |
### Configuring the interval for sending updates for the same route

A BGP router sends an update message to its peers when a route is changed. If the route changes frequently, the BGP router keeps sending updates for the same route, resulting in route flapping. To prevent this situation, perform this task to configure the interval for sending updates for the same route to a peer or peer group.

To configure the interval for sending the same update to a peer or peer group (IPv4 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP instance view or BGP-VPN instance view.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter BGP instance view:</td>
<td>bgp as-number</td>
</tr>
<tr>
<td></td>
<td>[ instance instance-name ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter BGP-VPN instance view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>a. bgp as-number</td>
<td></td>
</tr>
<tr>
<td></td>
<td>[ instance instance-name ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. ip vpn-instance</td>
<td></td>
</tr>
<tr>
<td></td>
<td>vpn-instance-name</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Configure the interval for sending updates for the same route to a peer or peer group.</td>
<td>peer { group-name</td>
</tr>
<tr>
<td></td>
<td>[ mask-length ] }</td>
<td>route-update-interval interval</td>
</tr>
</tbody>
</table>

To configure the interval for sending the same update to a peer or peer group (IPv6 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP instance view or BGP-VPN instance view.</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• Enter BGP instance view: bgp as-number [ instance instance-name ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter BGP-VPN instance view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>a. bgp as-number [ instance instance-name ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. ip vpn-instance vpn-instance-name</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Configure the interval for sending updates for the same route to a peer or peer group.</td>
<td>By default, the interval is 15 seconds for an IBGP peer and 30 seconds for an EBGP peer.</td>
</tr>
<tr>
<td></td>
<td>peer { group-name</td>
<td>ipv6-address [ prefix-length ] } route-update-interval interval</td>
</tr>
</tbody>
</table>

### Enabling BGP to establish an EBGP session over multiple hops

To establish an EBGP session, two routers must have a direct physical link and use directly connected interfaces. If no direct link is available, you must use the `peer ebgp-max-hop` command to enable BGP to establish an EBGP session over multiple hops and specify the maximum hops.

When the BGP GTSM feature is enabled, two peers can establish an EBGP session after passing GTSM check, regardless of whether the maximum number of hops is reached.

To enable BGP to establish an indirect EBGP session (IPv4 unicast/multicast address family):  

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP instance view or BGP-VPN instance view.</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• Enter BGP instance view: bgp as-number [ instance instance-name ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter BGP-VPN instance view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>a. bgp as-number [ instance instance-name ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. ip vpn-instance vpn-instance-name</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Enable BGP to establish an EBGP session to an indirectly connected peer or peer group and specify the maximum hop count.</td>
<td>By default, BGP cannot establish an EBGP session to an indirectly connected peer or peer group.</td>
</tr>
<tr>
<td></td>
<td>peer { group-name</td>
<td>ipv4-address [ mask-length ] } ebgp-max-hop [ hop-count ]</td>
</tr>
</tbody>
</table>

To enable BGP to establish an indirect EBGP session (IPv6 unicast/multicast address family):  

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
Enabling immediate re-establishment of direct EBGP connections upon link failure

When the link to a directly connected EBGP peer goes down, the router does not re-establish a session to the peer until the hold time timer expires. This feature enables BGP to immediately recreate the session in that situation. When this feature is disabled, route flapping does not affect EBGP session state.

To enable immediate re-establishment of direct EBGP connections:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>bgp as-number [ instance instance-name ]</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>ebgp-interface-sensitive</td>
<td>By default, immediate re-establishment of direct EBGP connections is enabled.</td>
</tr>
</tbody>
</table>

Enabling 4-byte AS number suppression

BGP supports 4-byte AS numbers. The 4-byte AS number occupies four bytes, in the range of 1 to 4294967295. By default, a device sends an Open message to the peer device for session establishment. The Open message indicates that the device supports 4-byte AS numbers. If the peer device supports 2-byte AS numbers instead of 4-byte AS numbers, the session cannot be established. To resolve this issue, enable the 4-byte AS number suppression feature. The device then sends an Open message to inform the peer that it does not support 4-byte AS numbers, so the BGP session can be established.

If the peer device supports 4-byte AS numbers, do not enable the 4-byte AS number suppression feature. Otherwise, the BGP session cannot be established.

To enable 4-byte AS number suppression (IPv4 unicast/multicast address family):

---

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>Enter BGP instance view or BGP-VPN instance view.</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>Enable BGP to establish an EBGP session to an indirectly connected peer or peer group and specify the maximum hop count.</td>
<td>By default, BGP cannot establish an EBGP session to an indirectly connected peer or peer group.</td>
</tr>
</tbody>
</table>

- Enter BGP instance view: `bgp as-number` [ `instance instance-name` ]
- Enter BGP-VPN instance view:
  - a. `bgp as-number` [ `instance instance-name` ]
  - b. `ip vpn-instance vpn-instance-name`
Step | Command | Remarks
--- | --- | ---
1. | Enter system view. | system-view | N/A
2. Enter BGP instance view or BGP-VPN instance view. | • Enter BGP instance view: `bgp as-number [ instance instance-name ]`  
• Enter BGP-VPN instance view:  
  a. `bgp as-number [ instance instance-name ]`  
  b. `ip vpn-instance vpn-instance-name` | N/A
3. Enable 4-byte AS number suppression. | `peer { group-name | ipv4-address [ mask-length ] }`  
`capability-advertise suppress-4-byte-as` | By default, 4-byte AS number suppression is disabled.

To enable 4-byte AS number suppression (IPv6 unicast/multicast address family):

Step | Command | Remarks
--- | --- | ---
1. | Enter system view. | system-view | N/A
2. Enter BGP instance view or BGP-VPN instance view. | • Enter BGP instance view: `bgp as-number [ instance instance-name ]`  
• Enter BGP-VPN instance view:  
  a. `bgp as-number [ instance instance-name ]`  
  b. `ip vpn-instance vpn-instance-name` | N/A
3. Enable 4-byte AS number suppression. | `peer { group-name | ipv6-address [ prefix-length ] }`  
`capability-advertise suppress-4-byte-as` | By default, 4-byte AS number suppression is disabled.

**Enabling MD5 authentication for BGP peers**

MD5 authentication provides the following benefits:
- Peer authentication ensures that only BGP peers that have the same password can establish TCP connections.
- Integrity check ensures that BGP packets exchanged between peers are intact.

To enable MD5 authentication for BGP peers (IPv4 unicast/multicast address family):

Step | Command | Remarks
--- | --- | ---
1. | Enter system view. | system-view | N/A
**Step** | **Command** | **Remarks**
---|---|---
2. Enter BGP instance view or BGP-VPN instance view. | • Enter BGP instance view: `bgp as-number [ instance instance-name ]`  
• Enter BGP-VPN instance view:  
  a. `bgp as-number [ instance instance-name ]`  
  b. `ip vpn-instance vpn-instance-name` | N/A
3. Enable MD5 authentication for a BGP peer group or peer. | `peer { group-name | ipv4-address [ mask-length ] } password { cipher | simple } password`  
By default, MD5 authentication is disabled. | 

To enable MD5 authentication for BGP peers (IPv6 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
</tbody>
</table>
| 2. Enter BGP instance view or BGP-VPN instance view. | • Enter BGP instance view: `bgp as-number [ instance instance-name ]`  
• Enter BGP-VPN instance view:  
  a. `bgp as-number [ instance instance-name ]`  
  b. `ip vpn-instance vpn-instance-name` | N/A |
| 3. Enable MD5 authentication for a BGP peer group or peer. | `peer { group-name | ipv6-address [ prefix-length ] } password { cipher | simple } password`  
By default, MD5 authentication is disabled. | |

**Configuring BGP load balancing**

Perform this task to specify the maximum number of BGP ECMP routes for load balancing.

To specify the maximum number of BGP ECMP routes for load balancing (IPv4 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
</tbody>
</table>
### Step 2
Enter BGP IPv4 unicast address family view, BGP-VPN IPv4 unicast address family view, or BGP IPv4 multicast address family view.

- **Enter BGP IPv4 unicast address family view:**
  - a. `bgp as-number [ instance instance-name ]`
  - b. `address-family ipv4 [ unicast ]`
- **Enter BGP-VPN IPv4 unicast address family view:**
  - c. `bgp as-number [ instance instance-name ]`
  - d. `ip vpn-instance vpn-instance-name`
  - e. `address-family ipv4 [ unicast ]`
- **Enter BGP IPv4 multicast address family view:**
  - f. `bgp as-number [ instance instance-name ]`
  - g. `address-family ipv4 multicast`

### Step 3
Specify the maximum number of BGP ECMP routes for load balancing.

- `balance [ ebgp | eibgp | ibgp ] number`

By default, load balancing is disabled.

### Step 4
(Optional.) Enable BGP to ignore the AS_PATH attribute when it implements load balancing.

- `balance as-path-neglect`

By default, BGP does not ignore the AS_PATH attribute when it implements load balancing.

To specify the maximum number of BGP ECMP routes for load balancing (IPv6 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td><code>bgp as-number [ instance instance-name ]</code></td>
<td>Enter BGP IPv4 unicast address family view.</td>
</tr>
<tr>
<td>3.</td>
<td><code>address-family ipv4 [ unicast ]</code></td>
<td>Enter BGP-VPN IPv4 unicast address family view.</td>
</tr>
<tr>
<td>4.</td>
<td><code>ip vpn-instance vpn-instance-name</code></td>
<td>Enter BGP IPv4 multicast address family view.</td>
</tr>
</tbody>
</table>

- **N/A**
### Configuring IPsec for IPv6 BGP

Perform this task to configure IPsec for IPv6 BGP. IPsec can provide privacy, integrity, and authentication for IPv6 BGP packets exchanged between BGP peers.

When two IPv6 BGP peers are configured with IPsec (for example, Device A and Device B), Device A encapsulates an IPv6 BGP packet with IPsec before sending it to Device B. If Device B successfully receives and de-encapsulates the packet, it establishes an IPv6 BGP peer relationship with Device A and learns IPv6 BGP routes from Device A. If Device B receives but fails to de-encapsulate the packet, or receives a packet not protected by IPsec, it discards the packet.

To configure IPsec for IPv6 BGP packets (IPv6 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
### Step 3. Enter BGP instance view or BGP-VPN instance view.

- **Enter BGP instance view:**
  ```
  bgp as-number [ instance instance-name ]
  ```
- **Enter BGP-VPN instance view:**
  a. ```
  bgp as-number [ instance instance-name ]
  ```
  b. ```
  ip vpn-instance vpn-instance-name
  ```

### Step 4. Apply the IPsec profile to an IPv6 BGP peer or peer group.

- **Command:**
  ```
  peer { group-name | ipv6-address [ prefix-length ] } ipsec-profile profile-name
  ```

By default, no IPsec profile is configured for any IPv6 BGP peer or peer group.

This command supports only IPsec profiles in manual mode.

---

### Disabling BGP to establish a session to a peer or peer group

This task enables you to temporarily tear down the BGP session to a peer or peer group. Then you can perform network upgrade and maintenance without needing to delete and reconfigure the peer or peer group. To recover the session, execute the `undo peer ignore` command.

To disable BGP to establish a session to a peer or peer group (IPv4 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><code>Enter system view.</code></td>
<td><code>system-view</code></td>
</tr>
</tbody>
</table>
| 2.     | Enter BGP instance view or BGP-VPN instance view. | ```
  bgp as-number [ instance instance-name ]
  ```
  ```
  ip vpn-instance vpn-instance-name
  ```
  | N/A | By default, BGP can establish a session to a peer or peer group. |
| 3.     | Disable BGP to establish a session to a peer or peer group. | ```
  peer { group-name | ipv6-address [ prefix-length ] } ignore
  ```

To disable BGP to establish a session to a peer or peer group (IPv6 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><code>Enter system view.</code></td>
<td><code>system-view</code></td>
</tr>
</tbody>
</table>

---
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>Enter BGP instance view or BGP-VPN instance view. &lt;br&gt;• Enter BGP instance view: <code>bgp as-number [ instance instance-name ]</code>&lt;br&gt;• Enter BGP-VPN instance view:&lt;br&gt;  a. <code>bgp as-number [ instance instance-name ]</code>&lt;br&gt;  b. <code>ip vpn-instance vpn-instance-name</code></td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>Configure GTSM for the specified BGP peer or peer group. &lt;br&gt;peer `{ group-name</td>
<td>ipv6-address [ prefix-length ] } ignore`</td>
</tr>
</tbody>
</table>

### Configuring GTSM for BGP

The Generalized TTL Security Mechanism (GTSM) protects a BGP session by comparing the TTL value in the IP header of incoming BGP packets against a valid TTL range. If the TTL value is within the valid TTL range, the packet is accepted. If not, the packet is discarded.

The valid TTL range is from 255 – the configured hop count + 1 to 255.

When GTSM is configured, the BGP packets sent by the device have a TTL of 255.

GTSM provides best protection for directly connected EBGP sessions, but not for multihop EBGP or IBGP sessions because the TTL of packets might be modified by intermediate devices.

**IMPORTANT:**

- When GTSM is configured, the local device can establish an EBGP session to the peer after both devices pass GTSM check, regardless of whether the maximum number of hops is reached.
- To use GTSM, you must configure GTSM on both the local and peer devices. You can specify different hop-count values for them.

To configure GTSM for BGP (IPv4 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view. <code>system-view</code></td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP instance view or BGP-VPN instance view. &lt;br&gt;• Enter BGP instance view: <code>bgp as-number [ instance instance-name ]</code>&lt;br&gt;• Enter BGP-VPN instance view:&lt;br&gt;  a. <code>bgp as-number [ instance instance-name ]</code>&lt;br&gt;  b. <code>ip vpn-instance vpn-instance-name</code></td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>Configure GTSM for the specified BGP peer or peer group. <code>peer </code>{ group-name</td>
<td>ipv4-address [ mask-length ] } ttl-security hops hop-count`</td>
</tr>
</tbody>
</table>

To configure GTSM for BGP (IPv6 unicast/multicast address family):
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
| 2.   | Enter BGP instance view or BGP-VPN instance view. | • Enter BGP instance view: `bgp as-number [ instance instance-name ]`  
• Enter BGP-VPN instance view:  
  a. `bgp as-number [ instance instance-name ]`  
  b. `ip vpn-instance vpn-instance-name` | N/A |
| 3.   | Configure GTSM for the specified BGP peer or peer group. | `peer { group-name | ipv6-address [ prefix-length ] } ttl-security hops hop-count` | By default, GTSM is disabled. |

### Configuring BGP soft-reset

After you modify the route selection policy, for example, modify the preferred value, you must reset BGP sessions to apply the new policy. The reset operation tears down and re-establishes BGP sessions.

To avoid tearing down BGP sessions, you can use one of the following soft-reset methods to apply the new policy:

- **Enabling route-refresh**—The BGP router advertises a route-refresh message to the specified peer, and the peer resends its routing information to the router. After receiving the routing information, the router filters the routing information by using the new policy.
  
  This method requires that both the local router and the peer support route refresh.

- **Saving updates**—Use the `peer keep-all-routes` command to save all route updates from the specified peer. After modifying the route selection policy, filter routing information by using the new policy.
  
  This method does not require that the local router and the peer support route refresh but it uses more memory resources to save routes.

- **Manual soft-reset**—Use the `refresh bgp` command to enable BGP to send local routing information or advertise a route-refresh message to the specified peer. The peer then resends its routing information. After receiving the routing information, the router filters the routing information by using the new policy.
  
  This method requires that both the local router and the peer support route refresh.

#### Enabling route-refresh

To enable BGP route refresh for a peer or peer group (IPv4 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP instance view or BGP-VPN instance view.</td>
<td>• Enter BGP instance view: <code>bgp as-number [ instance instance-name ]</code>&lt;br&gt;• Enter BGP-VPN instance view:&lt;br&gt;a. <code>bgp as-number [ instance instance-name ]</code>&lt;br&gt;b. <code>ip vpn-instance vpn-instance-name</code></td>
</tr>
<tr>
<td>3.</td>
<td>Enable BGP route refresh for a peer or peer group.</td>
<td>• Enable BGP route refresh for the specified peer or peer group:&lt;br&gt;peer { group-name</td>
</tr>
</tbody>
</table>

To enable BGP route refresh for a peer or peer group (IPv6 unicast/multicast address family): |

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP instance view or BGP-VPN instance view.</td>
<td>• Enter BGP instance view: <code>bgp as-number [ instance instance-name ]</code>&lt;br&gt;• Enter BGP-VPN instance view:&lt;br&gt;a. <code>bgp as-number [ instance instance-name ]</code>&lt;br&gt;b. <code>ip vpn-instance vpn-instance-name</code></td>
</tr>
</tbody>
</table>
### Step 3. Enable BGP route refresh for a peer or peer group.

- Enable BGP route refresh for the specified peer or peer group:
  ```
  peer { group-name | ipv6-address [ prefix-length ] } capability-advertise route-refresh
  ```

- Enable the BGP route refresh, multi-protocol extension, and 4-byte AS number features for the specified peer or peer group:
  ```
  undo peer { group-name | ipv6-address [ prefix-length ] } capability-advertise conventional
  ```

By default, the BGP route refresh, multi-protocol extension, and 4-byte AS number features are enabled.

---

### Saving updates

To save all route updates from the specified peer or peer group (IPv4 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><strong>Enter system view.</strong></td>
<td><strong>system-view</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Enter BGP IPv4 unicast address family view:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>a. <strong>bgp as-number</strong> [ instance instance-name ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. <strong>address-family ipv4 [ unicast ]</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Enter BGP-VPN IPv4 unicast address family view:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>c. <strong>bgp as-number</strong> [ instance instance-name ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>d. <strong>ip vpn-instance vpn-instance-name</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>e. <strong>address-family ipv4 [ unicast ]</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Enter BGP IPv4 multicast address family view:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>f. <strong>bgp as-number</strong> [ instance instance-name ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>g. <strong>address-family ipv4 multicast</strong></td>
<td></td>
</tr>
</tbody>
</table>

2. Enter BGP IPv4 unicast address family view, BGP-VPN IPv4 unicast address family view, or BGP IPv4 multicast address family view.

3. Save all route updates from the peer or peer group.

- `peer { group-name | ipv4-address [ mask-length ] } keep-all-routes`

By default, the routes are not saved. This command takes effect only for the routes received after this command is executed.
To save all route updates from the specified peer or peer group (IPv6 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP IPv6 unicast address family view, or BGP IPv6 multicast address family view.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Enter BGP IPv6 unicast address family view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>a. bgp as-number [ instance instance-name ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. address-family ipv6 [ unicast ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Enter BGP IPv6 multicast address family view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>c. bgp as-number [ instance instance-name ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>d. address-family ipv6 multicast</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Save all route updates from the peer or peer group.</td>
<td>peer { group-name</td>
</tr>
</tbody>
</table>

Configuring manual soft-reset

To configure manual soft-reset (IPv4 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP instance view or BGP-VPN instance view.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Enter BGP instance view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>bgp as-number [ instance instance-name ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Enter BGP-VPN instance view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>a. bgp as-number [ instance instance-name ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. ip vpn-instance vpn-instance-name</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| 3.   | Enable BGP route refresh for a peer or peer group. | • Enable BGP route refresh for the specified peer or peer group:  
  peer { group-name | ipv4-address  
  [ mask-length ] }  
  capability-advertise  
  route-refresh  
  • Enable the BGP route refresh, multi-protocol extension, and 4-byte AS number features for the specified peer or peer group:  
  undo peer { group-name | ipv4-address  
  [ mask-length ] }  
  capability-advertise  
  conventional  
   By default, the BGP route refresh, multi-protocol extension, and 4-byte AS number features are enabled. |

| 4.   | Return to user view. | return |

| 5.   | Perform manual soft-reset. | refresh bgp [ instance  
  instance-name ] { ipv4-address  
  [ mask-length ] | all | external  
  group group-name | internal }  
  { export | import } ipv4  
  { multicast | [ unicast ]  
  [ vpn-instance  
  vpn-instance-name ] } |

To configure manual soft-reset (IPv6 unicast/multicast address family): |

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>

| 2.   | Enter BGP instance view or BGP-VPN instance view. | Enter BGP instance view:  
  bgp as-number [ instance  
  instance-name ]  
  Enter BGP-VPN instance view:  
  a. bgp as-number  
  [ instance  
  instance-name ]  
  b. ip vpn-instance  
  vpn-instance-name |

N/A
Protecting an EBGP peer when memory usage reaches level 2 threshold

Memory usage includes the following threshold levels: normal, level 1, level 2, and level 3. When the level 2 threshold is reached, BGP periodically tears down an EBGP session to release memory resources until the memory usage falls below the level 2 threshold. You can configure this feature to avoid tearing down the EBGP session to an EBGP peer when the memory usage reaches the level 2 threshold.

For more information about memory usage thresholds, see Fundamentals Configuration Guide.

To configure BGP to protect an EBGP peer or peer group when the memory usage reaches level 2 threshold (IPv4 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter BGP instance view or BGP-VPN instance view.</td>
<td></td>
<td>N/A</td>
</tr>
</tbody>
</table>
To configure BGP to protect an EBGP peer or peer group when the memory usage reaches level 2 threshold (IPv6 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
| 2.   | Enter BGP instance view or BGP-VPN instance view. | • Enter BGP instance view: 
bgp as-number [instance instance-name ]
• Enter BGP-VPN instance view:
  a. bgp as-number [instance instance-name ]
  b. ip vpn-instance vpn-instance-name | N/A |
| 3.   | Configure BGP to protect an EBGP peer or peer group when the memory usage reaches level 2 threshold. | peer { group-name | ipv4-address [mask-length ] | ipv6-address [prefix-length ] } low-memory-exempt | By default, BGP tears down an EBGP session to release memory resources periodically when level 2 threshold is reached. |

### Configuring an update delay for local MPLS labels

BGP includes local MPLS labels in advertised VPNv4 routes, VPNv6 routes, labeled IPv4 unicast routes, and labeled IPv6 unicast routes.

When a local label is changed, BGP removes the old label and advertises the new label. Traffic interruption occurs if BGP peers use the old label to forward packets before they learn the new label. To resolve this issue, configure an update delay for local MPLS labels. BGP does not remove the old label before the update delay timer expires.

To configure an update delay for local MPLS labels:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP instance view.</td>
<td>bgp as-number [instance instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Configure an update delay for local MPLS labels.</td>
<td>retain local-label retain-time</td>
</tr>
</tbody>
</table>

### Flushing the suboptimal BGP route to the RIB

This feature flushes the suboptimal BGP route to the RIB when the following conditions are met:

- The optimal route is generated by the `network` command or is redistributed by the `import-route` command.
- The suboptimal route is received from a BGP peer.
After the suboptimal route is flushed to the RIB on a network, BGP immediately switches traffic to the suboptimal route when the optimal route fails.

For example, the device has a static route to the subnet 1.1.1.0/24 that has a higher priority than a BGP route. BGP redistributes the static route and receives a route to 1.1.1.0/24 from a peer. After the flush suboptimal-route command is executed, BGP flushes the received BGP route to the RIB as the suboptimal route. When the static route fails, BGP immediately switches traffic to the suboptimal route if inter-protocol FRR is enabled. For more information about inter-protocol FRR, see "Configuring basic IP routing."

To flush the suboptimal BGP route to the RIB:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP view.</td>
<td>bgp as-number [ instance instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Flush the suboptimal BGP route to the RIB.</td>
<td>flush suboptimal-route</td>
</tr>
</tbody>
</table>

Configuring a large-scale BGP network

In a large network, the number of BGP connections is huge and BGP configuration and maintenance are complicated. To simply BGP configuration, you can use the peer group, community, route reflector, and confederation features as needed. For more information about configuring peer groups, see "Configuring a BGP peer group."

Configuring BGP community

By default, a router does not advertise the COMMUNITY or extended community attribute to its peers or peer groups. When the router receives a route carrying the COMMUNITY or extended community attribute, it removes the attribute before advertising the route to other peers or peer groups.

Perform this task to enable a router to advertise the COMMUNITY or extended community attribute to its peers for route filtering and control. You can also use a routing policy to add or modify the COMMUNITY or extended community attribute for specific routes. For more information about routing policy, see "Configuring routing policies."

To configure BGP community (IPv4 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| **2.** Enter BGP IPv4 unicast address family view, BGP-VPN IPv4 unicast address family view, or BGP IPv4 multicast address family view. | • Enter BGP IPv4 unicast address family view:  
  a. `bgp as-number`  
     `{ instance instance-name }`  
  b. `address-family ipv4`  
     `{ unicast }`  
  • Enter BGP-VPN IPv4 unicast address family view:  
  c. `bgp as-number`  
     `{ instance instance-name }`  
  d. `ip vpn-instance`  
     `{ vpn-instance-name }`  
  e. `address-family ipv4`  
     `{ unicast }`  
  • Enter BGP IPv4 multicast address family view:  
  f. `bgp as-number`  
     `{ instance instance-name }`  
  g. `address-family ipv4`  
     `{ multicast }` | N/A |
| **3.** Advertise the COMMUNITY or extended community attribute to a peer or peer group. | • Advertise the COMMUNITY attribute to a peer or peer group:  
  `peer` `{ group-name | ipv4-address`  
  `{ mask-length }`  
  `advertise-community`  
  • Advertise the extended community attribute to a peer or peer group:  
  `peer` `{ group-name | ipv4-address`  
  `{ mask-length }`  
  `advertise-ext-community` | By default, the COMMUNITY or extended community attribute is not advertised. |
| **4.** (Optional.) Apply a routing policy to routes advertised to a peer or peer group. | `peer` `{ group-name | ipv4-address`  
  `{ mask-length }`  
  `route-policy`  
  `route-policy-name`  
  `export` | By default, no routing policy is applied. |

To configure BGP community (IPv6 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1.</strong> Enter system view.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
</tbody>
</table>
| 2. | Enter BGP IPv6 unicast address family view, BGP-VPN IPv6 unicast address family view, or BGP IPv6 multicast address family view. | • Enter BGP IPv6 unicast address family view:  
  a. `bgp as-number [ instance instance-name ]`  
  b. `address-family ipv6 [ unicast ]`  
  • Enter BGP-VPN IPv6 unicast address family view:  
  c. `bgp as-number [ instance instance-name ]`  
  d. `ip vpn-instance vpn-instance-name`  
  e. `address-family ipv6 [ unicast ]`  
  • Enter BGP IPv6 multicast address family view:  
  f. `bgp as-number [ instance instance-name ]`  
  g. `address-family ipv6 multicast` |
| 3. | Advertise the COMMUNITY or extended community attribute to a peer or peer group. | • Advertise the COMMUNITY attribute to a peer or peer group:  
  `peer { group-name | ipv6-address [ prefix-length ] } advertise-community`  
  • Advertise the extended community attribute to a peer or peer group:  
  `peer { group-name | ipv6-address [ prefix-length ] } advertise-ext-community` |
| 4. | (Optional.) Apply a routing policy to routes advertised to a peer or peer group. | `peer { group-name | ipv6-address [ prefix-length ] } route-policy route-policy-name export` |

### Configuring BGP route reflection

#### Configuring a BGP route reflector

Perform this task to configure a BGP route reflector and its clients. The route reflector and its clients automatically form a cluster identified by the router ID of the route reflector. The route reflector forwards route updates among its clients.

To improve availability, you can specify multiple route reflectors for a cluster. The route reflectors in the cluster must have the same cluster ID to avoid routing loops.

To configure a BGP route reflector (IPv4 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| 2.   | Enter BGP IPv4 unicast address family view, BGP-VPN IPv4 unicast address family view, or BGP IPv4 multicast address family view. | • Enter BGP IPv4 unicast address family view:  
  a. `bgp as-number [instance instance-name]`  
  b. `address-family ipv4 [unicast]`  
  • Enter BGP-VPN IPv4 unicast address family view:  
  c. `bgp as-number [instance instance-name]`  
  d. `ip vpn-instance vpn-instance-name`  
  e. `address-family ipv4 [unicast]`  
  • Enter BGP IPv4 multicast address family view:  
  f. `bgp as-number [instance instance-name]`  
  g. `address-family ipv4 multicast` |
| 3.   | Configure the router as a route reflector and specify a peer or peer group as its client. | `peer {group-name | ipv4-address [mask-length]} reflect-client`  
  By default, no route reflector or client is configured. |
| 4.   | Enable route reflection between clients. | `reflect between-clients`  
  By default, route reflection between clients is enabled. |
| 5.   | (Optional.) Configure the cluster ID of the route reflector. | `reflector cluster-id {cluster-id | ipv4-address}`  
  By default, a route reflector uses its own router ID as the cluster ID. |

To configure a BGP route reflector (IPv6 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
</table>
| 1.   | Enter system view. | `system-view`  
  N/A |
| 2.   | Enter BGP IPv6 unicast address family view, or BGP IPv6 multicast address family view. | • Enter BGP IPv6 unicast address family view:  
  a. `bgp as-number [instance instance-name]`  
  b. `address-family ipv6 [unicast]`  
  • Enter BGP IPv6 multicast address family view:  
  c. `bgp as-number [instance instance-name]`  
  d. `address-family ipv6 multicast` |
<p>|      |         | N/A     |</p>
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td>Configure the router as a route reflector and specify a peer or peer group as its client.</td>
<td>peer { group-name</td>
</tr>
<tr>
<td>4.</td>
<td>Enable route reflection between clients.</td>
<td>reflect between-clients</td>
</tr>
<tr>
<td>5.</td>
<td>(Optional.) Configure the cluster ID of the route reflector.</td>
<td>reflector cluster-id { cluster-id</td>
</tr>
</tbody>
</table>

**Ignoring the ORIGINATOR_ID attribute**

By default, BGP drops incoming route updates whose ORIGINATOR_ID attribute is the same as the local router ID. Some special networks such as firewall networks require BGP to accept such route updates. To meet the requirement, you must configure BGP to ignore the ORIGINATOR_ID attribute.

To ignore the ORIGINATOR_ID attribute (IPv4 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP instance view or BGP-VPN instance view.</td>
<td>• Enter BGP instance view: bgp as-number [ instance instance-name ]&lt;br&gt;• Enter BGP-VPN instance view:&lt;br&gt;a. bgp as-number [ instance instance-name ]&lt;br&gt;b. ip vpn-instance vpn-instance-name</td>
</tr>
<tr>
<td>3.</td>
<td>Ignore the ORIGINATOR_ID attribute.</td>
<td>peer { group-name</td>
</tr>
</tbody>
</table>

To ignore the ORIGINATOR_ID attribute (IPv6 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP instance view or BGP-VPN instance view.</td>
<td>• Enter BGP instance view: bgp as-number [ instance instance-name ]&lt;br&gt;• Enter BGP-VPN instance view:&lt;br&gt;a. bgp as-number [ instance instance-name ]&lt;br&gt;b. ip vpn-instance vpn-instance-name</td>
</tr>
</tbody>
</table>
### Configuring a BGP confederation

BGP confederation provides another way to reduce IBGP connections in an AS.

A confederation contains sub-ASs. In each sub-AS, IBGP peers are fully meshed. Sub-ASs establish EBGP connections in between.

#### Configuring a BGP confederation

After you split an AS into multiple sub-ASs, configure a router in a sub-AS as follows:

1. Enable BGP and specify the AS number of the router. For more information, see "Enabling BGP."
2. Specify the confederation ID. From an outsider's perspective, the sub-ASs of the confederation is a single AS, which is identified by the confederation ID.
3. If the router needs to establish EBGP connections to other sub-ASs, you must specify the peering sub-ASs in the confederation.

A confederation can contain a maximum of 32 sub-ASs. The AS number of a sub-AS is effective only in the confederation.

To configure a BGP confederation:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP instance view.</td>
<td>bgp as-number [ instance instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Configure a confederation ID.</td>
<td>confederation id as-number</td>
</tr>
<tr>
<td>4.</td>
<td>Specify confederation peer sub-ASs in the confederation.</td>
<td>confederation peer-as as-number-list</td>
</tr>
</tbody>
</table>

### Configuring confederation compatibility

If any routers in the confederation do not comply with RFC 3065, enable confederation compatibility to allow the router to work with those routers.

To configure confederation compatibility:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP instance view.</td>
<td>bgp as-number [ instance instance-name ]</td>
</tr>
</tbody>
</table>
### Configuring BGP GR

Graceful Restart (GR) ensures forwarding continuous when a routing protocol restarts or an active/standby switchover occurs. Two routers are required to complete a GR process. The following are router roles in a GR process:

- **GR restarter**—Performs GR upon a BGP restart or active/standby switchover.
- **GR helper**—Helps the GR restarter to complete the GR process.

A device can act as a GR restarter and GR helper at the same time.

BGP GR works as follows:

1. The BGP GR restarter and helper exchange Open messages for GR capability negotiation. If both parties have the GR capability, they establish a GR-capable session. The GR restarter sends the GR timer set by the `graceful-restart timer restart` command to the GR helper in an Open message.

2. When an active/standby switchover occurs or BGP restarts, the GR restarter does not remove existing BGP routes from Routing Information Base (RIB) and Forwarding Information Base (FIB). It still uses these routes for packet forwarding, and it starts the RIB purge timer (set by the `graceful-restart timer purge-time` command). The GR helper marks all routes learned from the GR restarter as stale instead of deleting them. It continues to use these routes for packet forwarding. During the GR process, packet forwarding is not interrupted.

3. After the active/standby switchover or BGP restart completes, the GR restarter re-establishes a BGP session to the GR helper. If the BGP session fails to be established within the GR timer advertised by the GR restarter, the GR helper removes the stale routes.

4. If the BGP session is established, routing information is exchanged for the GR restarter to retrieve route entries and for the GR helper to recover stale routes.

5. Both the GR restarter and the GR helper start the End-Of-RIB marker waiting timer. The End-Of-RIB marker waiting time is set by the `graceful-restart timer wait-for-rib` command. If routing information exchange is not completed within the time, the GR restarter does not receive new routes. The GR restarter updates the RIB with the BGP routes already learned, and removes the aged routes from the RIB. The GR helper removes the stale routes.

6. The GR restarter quits the GR process if routing information exchange is not completed within the RIB purge timer. It updates the RIB with the BGP routes already learned, and removes the aged routes.

Follow these guidelines when you configure BGP GR:

- The End-Of-RIB indicates the end of route updates.
- The maximum time to wait for the End-of-RIB marker configured on the local end is not advertised to the peer. It controls the time for the local end to receive updates from the peer.

As a best practice, perform the following configuration on the GR restarter and GR helper.

To configure BGP GR:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP instance view.</td>
<td>bgp as-number [ instance instance-name ]</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>3.</td>
<td>Enable GR capability for BGP.</td>
<td>graceful-restart</td>
</tr>
<tr>
<td>4.</td>
<td>Configure the GR timer.</td>
<td>graceful-restart timer restart timer</td>
</tr>
<tr>
<td>5.</td>
<td>Configure the maximum time to wait for the End-of-RIB marker.</td>
<td>graceful-restart timer wait-for-rib timer</td>
</tr>
<tr>
<td>6.</td>
<td>Configure the RIB purge timer.</td>
<td>graceful-restart timer purge-time timer</td>
</tr>
</tbody>
</table>

### Configuring BGP NSR

The following matrix shows the feature and hardware compatibility:

<table>
<thead>
<tr>
<th>Hardware</th>
<th>BGP NSR compatibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSR954(JH296A/JH297A/JH298A/JH299A/JH373A)</td>
<td>No</td>
</tr>
<tr>
<td>MSR958(JH300A/JH301A)</td>
<td>No</td>
</tr>
</tbody>
</table>
| MSR1002-4/1003-8S | • In standalone mode: No  
• In IRF mode: Yes |
| MSR2003 | • In standalone mode: No  
• In IRF mode: Yes |
| MSR2004-24/2004-48 | • In standalone mode: No  
• In IRF mode: Yes |
| MSR3012/3024/3044/3064 | • In standalone mode: No  
• In IRF mode: Yes |
| MSR4060/4080 | Yes |

To use BGP nonstop routing (NSR), the system must have a minimum of two MPUs or two IRF member devices.

NSR ensures nonstop services when BGP has redundant processes on multiple MPUs or IRF member devices. In contrast to GR, NSR does not require a neighbor device to recover routing information.

BGP NSR backs up BGP state and data information from the active BGP process to the standby BGP process. The standby BGP process takes over when any of the following events occurs:

- The active BGP process restarts.
- The MPU that runs the active BGP process fails.
- An ISSU starts on the MPU that runs the active BGP process.

When both GR and NSR are configured for BGP, NSR has a higher priority than GR. The device will not act as the GR restarter. If the device acts as a GR helper, it cannot help the restarter to complete GR.

To use BGP NSR in MPLS L3VPN, you must enable RIB NSR. For information about RIB NSR, see "Configuring basic IP routing."
To configure BGP NSR:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP instance view.</td>
<td>bgp as-number [ instance instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Enable BGP NSR.</td>
<td>non-stop-routing</td>
</tr>
</tbody>
</table>

Enabling SNMP notifications for BGP

This feature enables BGP to generate SNMP notifications. The generated SNMP notifications are sent to the SNMP module.

For more information about SNMP notifications, see *Network Management and Monitoring Configuration Guide*.

To enable SNMP notifications for BGP:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable SNMP notifications for BGP.</td>
<td>snmp-agent trap enable bgp [ instance instance-name ]</td>
</tr>
</tbody>
</table>

Enabling logging for session state changes

Perform this task to enable BGP to log BGP session establishment and disconnection events. To display the log information, use the `display bgp peer ipv4 unicast log-info` command or the `display bgp peer ipv6 unicast log-info` command. The logs are sent to the information center. The output rules of the logs (whether to output the logs and where to output) are determined by the information center configuration.

For more information about information center configuration, see *Network Management and Monitoring Configuration Guide*.

To enable logging for session state changes (IPv4 unicast/IPv4 multicast):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP instance view.</td>
<td>bgp as-number [ instance instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Enable logging for session state changes globally.</td>
<td>log-peer-change</td>
</tr>
<tr>
<td>4.</td>
<td>(Optional.) Enter BGP-VPN instance view.</td>
<td>ip vpn-instance vpn-instance-name</td>
</tr>
<tr>
<td>5.</td>
<td>Enable logging for session state changes for a peer or peer group.</td>
<td>peer { group-name</td>
</tr>
</tbody>
</table>
Step | Command | Remarks
--- | --- | ---
1. | Enter system view. | system-view | N/A
2. | Enter BGP instance view. | bgp as-number [ instance instance-name ] | N/A
3. | Enable logging for session state changes globally. | log-peer-change | By default, logging for session state changes is enabled globally.
4. | (Optional.) Enter BGP-VPN instance view. | ip vpn-instance vpn-instance-name | N/A
5. | Enable logging for session state changes for a peer or peer group. | peer { group-name | ipv6-address [ prefix-length ] } log-change | By default, logging for session state changes is enabled for all peers or peer groups.

## Configuring BFD for BGP

### IMPORTANT:
If you have enabled GR, use BFD with caution because BFD might detect a failure before the system performs GR, which will result in GR failure. If you have enabled both BFD and GR for BGP, do not disable BFD during a GR process to avoid GR failure.

BGP maintains neighbor relationships based on the keepalive timer and hold timer in seconds. It requires that the hold time must be at least three times the keepalive interval. This mechanism slows down link failure detection. Once a failure occurs on a high-speed link, a large quantity of packets will be dropped before routing convergence completes. BFD for BGP can solve this problem by fast detecting link failures to reduce convergence time.

Before you enable BFD for a BGP peer or peer group, you must establish a BGP session between the local router and the peer or peer group.

For more information about BFD, see *High Availability Configuration Guide*.

To enable BFD for a BGP peer (IPv4 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter BGP instance view or BGP-VPN instance view.</td>
<td></td>
</tr>
<tr>
<td>a.</td>
<td>Enter BGP instance view:</td>
<td>bgp as-number [ instance instance-name ]</td>
</tr>
<tr>
<td>b.</td>
<td>Enter BGP-VPN instance view:</td>
<td></td>
</tr>
<tr>
<td>a.</td>
<td>bgp as-number [ instance instance-name ]</td>
<td></td>
</tr>
<tr>
<td>a.</td>
<td>ip vpn-instance</td>
<td>vpn-instance-name</td>
</tr>
<tr>
<td>a.</td>
<td>Enable BFD to detect the link to the specified BGP peer or peer group.</td>
<td>peer { group-name</td>
</tr>
</tbody>
</table>

To enable BFD for a BGP peer (IPv6 unicast/multicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| 2.   | Enter BGP instance view or BGP-VPN instance view. • Enter BGP instance view: 
`bgp as-number [ instance instance-name ]` • Enter BGP-VPN instance view: 
a. `bgp as-number [ instance instance-name ]` b. `ip vpn-instance vpn-instance-name` | N/A |
| 3.   | Enable BFD to detect the link to the specified IPv6 BGP peer or peer group. peer `{ group-name | ipv6-address [ prefix-length ] } bfd [ multi-hop | single-hop ]` | By default, BFD is disabled. |

### Configuring BGP FRR

When a link fails, the packets on the link are discarded, and a routing loop might occur until BGP completes routing convergence based on the new network topology.

You can enable BGP fast reroute (FRR) to resolve this issue.

**Figure 65 Network diagram for BGP FRR**

![Network Diagram](image)

After you configure FRR on Router B as shown in Figure 65, BGP generates a backup next hop Router C for the primary route. BGP uses ARP (for IPv4), echo-mode BFD (for IPv4), or ND (for IPv6) to detect the connectivity to Router D. When the link to Router D fails, BGP directs packets to the backup next hop. At the same time, BGP calculates a new optimal route, and forwards packets over the optimal route.

You can use the following methods to configure BGP FRR:

- **Method 1**—Execute the `pic` command in BGP address family view. BGP calculates a backup next hop for each BGP route in the address family if there are two or more unequal-cost routes that reach the destination.

- **Method 2**—Execute the `fast-reroute route-policy` command to use a routing policy in which a backup next hop is specified by using the command `apply [ ipv6 ] fast-reroute backup-nexthop`. The backup next hop calculated by BGP must be the same as the specified backup next hop. Otherwise, BGP does not generate a backup next hop for the primary route. You can also configure `if-match` clauses in the routing policy to identify the routes protected by FRR.

If both methods are configured, Method 2 takes precedence over Method 1.

BGP supports FRR for IPv4 and IPv6 unicast routes, but not for IPv4 and IPv6 multicast routes.

To configure BGP FRR (IPv4 unicast address family):
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>Configure the source address of echo packets.</td>
<td><code>bfd echo-source-ip ipv4-address</code></td>
</tr>
<tr>
<td>3.</td>
<td>Create a routing policy and enter routing policy view.</td>
<td><code>route-policy route-policy-name permit node node-number</code></td>
</tr>
<tr>
<td>4.</td>
<td>Set the backup next hop for FRR.</td>
<td><code>apply fast-reroute backup-nexthop ipv4-address</code></td>
</tr>
<tr>
<td>5.</td>
<td>Return to system view.</td>
<td><code>quit</code></td>
</tr>
<tr>
<td>6.</td>
<td>Enter BGP instance view.</td>
<td><code>bgp as-number [ instance instance-name ]</code></td>
</tr>
<tr>
<td>7.</td>
<td>(Optional.) Use echo-mode BFD to detect the connectivity to the next hop of the primary route.</td>
<td><code>primary-path-detect bfd echo</code></td>
</tr>
<tr>
<td>8.</td>
<td>(Optional.) Enter BGP-VPN instance view.</td>
<td><code>ip vpn-instance vpn-instance-name</code></td>
</tr>
<tr>
<td>9.</td>
<td>Enter BGP IPv4 unicast address family view or BGP-VPN IPv4 unicast address family view.</td>
<td><code>address-family ipv4 [ unicast ]</code></td>
</tr>
</tbody>
</table>
### Step 10. Enable BGP FRR.

<table>
<thead>
<tr>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Method 1) Enable BGP FRR for the address family: <strong>pic</strong></td>
<td>By default, BGP FRR is disabled. Method 1 might result in routing loops. Use it with caution. By default, no routing policy is applied. The <strong>apply fast-reroute backup-nexthop</strong> and <strong>apply ipv6 fast-reroute backup-nexthop</strong> commands can take effect in the applied routing policy. Other <strong>apply</strong> commands do not take effect.</td>
</tr>
<tr>
<td>(Method 2) Apply a routing policy to FRR for the address family: <strong>fast-reroute route-policy route-policy-name</strong></td>
<td></td>
</tr>
</tbody>
</table>

### To configure BGP FRR (IPv6 unicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><strong>system-view</strong></td>
</tr>
<tr>
<td>2.</td>
<td>Create a routing policy and enter routing policy view.</td>
<td><strong>route-policy route-policy-name permit node node-number</strong></td>
</tr>
<tr>
<td>3.</td>
<td>Set the backup next hop for FRR.</td>
<td><strong>apply ipv6 fast-reroute backup-nexthop ipv6-address</strong></td>
</tr>
<tr>
<td>4.</td>
<td>Return to system view.</td>
<td><strong>quit</strong></td>
</tr>
<tr>
<td>5.</td>
<td>Enter BGP instance view or BGP-VPN instance view.</td>
<td><strong>bgp as-number [ instance instance-name ]</strong></td>
</tr>
<tr>
<td></td>
<td>Enter BGP-VPN instance view:</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>a. <strong>bgp as-number [ instance instance-name ]</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. <strong>ip vpn-instance vpn-instance-name</strong></td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>Enter BGP IPv6 unicast address family view or BGP-VPN IPv6 unicast address family view.</td>
<td><strong>address-family ipv6 [ unicast ]</strong></td>
</tr>
</tbody>
</table>
### Configuring BGP policy accounting

BGP policy accounting provides the following functionalities:

- Classifies IP traffic by BGP path attributes such as NEXT HOP, COMMUNITY, and AS_PATH.
- Assigns an index to each class of traffic.
- Collects statistics based on indexes.

Configure BGP policy accounting as follows:

1. Configure a routing policy, and assign an index to the matching BGP routes by using the `apply traffic-index` command. For more information about the `apply traffic-index` command, see [Layer 3—IP Routing Command Reference](#).

2. Configure BGP to use the routing policy. The `network`, `import-route`, `aggregate`, `peer route-policy`, and `peer default-route-advertise` commands can use a routing policy.

3. Enable BGP policy accounting on an interface.

BGP policy accounting supports the following traffic classification policies:

- **Source IP address-based policy**—Used to collect statistics for traffic from a specific source.
  - BGP searches routes to the source address, obtains the traffic index for the routes, and collects statistics for the traffic identified by the index.

- **Destination IP address-based policy**—Used to collect statistics for traffic destined to a specific address.
  - BGP searches routes to the destination address, obtains the traffic index for the routes, and collects statistics for the traffic identified by the index.

This feature is incompatible with fast forwarding as follows:

- When the source IP address-based policy is applied, fast forwarding does not work.
- When the destination IP address-based policy is applied, fast forwarding does not process traffic with a traffic index.

To enable BGP policy accounting (IPv4/IPv6 unicast address family):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td><code>interface interface-type interface-number</code></td>
</tr>
<tr>
<td>3.</td>
<td>Enable BGP policy</td>
<td>`bgp-policy accounting { input</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>3.</td>
<td>accounting on the interface.</td>
<td>output } * [ source ]</td>
</tr>
<tr>
<td>4.</td>
<td>Display BGP policy accounting information.</td>
<td>display bgp-policy { ip</td>
</tr>
</tbody>
</table>

### Configuring 6PE

IPv6 provider edge (6PE) is a transition technology that uses MPLS to connect sparsely populated IPv6 networks through an existing IPv4 backbone network. It is an efficient solution for ISP IPv4/MPLS networks to provide IPv6 traffic switching capability.

![Network diagram for 6PE](image)

6PE mainly performs the following operations:

- **6PE assigns a label to IPv6 routing information received from a CE router, and sends the labeled IPv6 routing information to the peer 6PE device through an MP-BGP session. The peer 6PE device then forwards the IPv6 routing information to the attached customer site.**

- **6PE provides tunnels over the IPv4 backbone so the IPv4 backbone can forward packets for IPv6 networks. The tunnels can be GRE tunnels, MPLS LSPs, or MPLS TE tunnels.**

- **Upon receiving an IPv6 packet, 6PE adds an inner tag (corresponding to the IPv6 packet) and then an outer tag (corresponding to the public network tunnel) to the IPv6 packet. Devices in the IPv4 backbone network forwards the packet based on the outer tag. When the peer 6PE device receives the packet, it removes the outer and inner tags and forwards the original IPv6 packet to the attached customer site.**

To implement exchange of IPv6 routing information, you can configure IPv6 static routing, an IPv6 IGP protocol, or IPv6 BGP between CE and 6PE devices.

For more information about MPLS, MPLS TE, CE, and P, see *MPLS Configuration Guide*. For more information about GRE, see *Layer 3—IP Services Configuration Guide*.

### Configuring basic 6PE

Before you configure 6PE, perform the following tasks:

- **Establish tunnels in the IPv4 backbone network** (see *Layer 3—IP Services Configuration Guide*).

- **Configure basic MPLS on 6PE devices** (see *MPLS Configuration Guide*).

- **Configure BGP on 6PE devices** so that they can advertise tagged IPv6 routing information through BGP sessions. The following describes only BGP configurations on 6PE devices.

To configure basic 6PE:
### Configuring optional 6PE capabilities

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter BGP instance view.</td>
<td>bgp as-number [ instance instance-name ]</td>
<td>N/A</td>
</tr>
<tr>
<td>3. Specify a 6PE peer or peer group and its AS number.</td>
<td>peer { group-name</td>
<td>ipv4-address [ mask-length ] } as-number</td>
</tr>
<tr>
<td>4. Enter BGP IPv6 unicast address family view.</td>
<td>address-family ipv6 [ unicast ]</td>
<td>N/A</td>
</tr>
<tr>
<td>5. Enable BGP to exchange IPv6 unicast routing information with the 6PE peer or peer group.</td>
<td>peer { group-name</td>
<td>ipv4-address [ mask-length ] } enable</td>
</tr>
<tr>
<td>6. Enable BGP to exchange labeled IPv6 routes with the 6PE peer or peer group.</td>
<td>peer { group-name</td>
<td>ipv4-address [ mask-length ] } label-route-capability</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter BGP instance view.</td>
<td>bgp as-number [ instance instance-name ]</td>
<td>N/A</td>
</tr>
<tr>
<td>3. Enter BGP IPv6 unicast address family view.</td>
<td>address-family ipv6 [ unicast ]</td>
<td>N/A</td>
</tr>
<tr>
<td>4. Advertise COMMUNITY attribute to the 6PE peer or peer group.</td>
<td>peer { group-name</td>
<td>ipv4-address [ mask-length ] } advertise-community</td>
</tr>
<tr>
<td>5. Advertise extended community attribute to the 6PE peer or peer group.</td>
<td>peer { group-name</td>
<td>ipv4-address [ mask-length ] } advertise-ext-community</td>
</tr>
<tr>
<td>6. Allow the local AS number to appear in routes from the 6PE peer or peer group and specify the repeat times.</td>
<td>peer { group-name</td>
<td>ipv4-address [ mask-length ] } allow-as-loop [ number ]</td>
</tr>
<tr>
<td>7. Specify an AS path list to filter routes advertised to or received from the 6PE peer or peer group.</td>
<td>peer { group-name</td>
<td>ipv4-address [ mask-length ] } as-path-acl as-path-acl-number { export</td>
</tr>
<tr>
<td>8. Specify an IPv6 ACL to filter routes advertised to or received from the 6PE peer or peer group.</td>
<td>peer { group-name</td>
<td>ipv4-address [ mask-length ] } filter-policy ipv6-acl-number { export</td>
</tr>
<tr>
<td>9. Specify an IPv6 prefix list to filter routes advertised to or received from the 6PE peer or peer group.</td>
<td>peer { group-name</td>
<td>ipv4-address [ mask-length ] } prefix-list ipv6-prefix-name { export</td>
</tr>
<tr>
<td>10. Specify a routing policy to filter routes advertised to or received from the 6PE peer or peer group.</td>
<td>peer { group-name</td>
<td>ipv4-address [ mask-length ] } route-policy route-policy-name { export</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>--------</td>
<td>-------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>11.</td>
<td>Advertise a default route to the 6PE peer or peer group.</td>
<td>By default, no default route is advertised.</td>
</tr>
<tr>
<td></td>
<td>`peer { group-name</td>
<td>ipv4-address [mask-length] } default-route-advertise [route-policy route-policy-name]`</td>
</tr>
<tr>
<td>12.</td>
<td>Save all routes from the 6PE peer or peer group.</td>
<td>By default, routes from a peer or peer group are not saved.</td>
</tr>
<tr>
<td></td>
<td>`peer { group-name</td>
<td>ipv4-address [mask-length] } keep-all-routes`</td>
</tr>
<tr>
<td>13.</td>
<td>Configure BGP updates sent to the 6PE peer or peer group to carry only public AS numbers.</td>
<td>By default, BGP updates sent to a 6PE peer or peer group can carry both public and private AS numbers.</td>
</tr>
<tr>
<td></td>
<td>`peer { group-name</td>
<td>ipv4-address [mask-length] } public-as-only`</td>
</tr>
<tr>
<td>14.</td>
<td>Specify the maximum number of routes that BGP can receive from the 6PE peer or peer group.</td>
<td>By default, the number of routes that a router can receive from the 6PE peer or peer group is not limited.</td>
</tr>
<tr>
<td></td>
<td>`peer { group-name</td>
<td>ipv4-address [mask-length] } route-limit prefix-number {alert-only discard</td>
</tr>
<tr>
<td></td>
<td>[percentage-value] *</td>
<td></td>
</tr>
<tr>
<td>15.</td>
<td>Specify a preferred value for routes received from the 6PE peer or peer group.</td>
<td>By default, the preferred value is 0.</td>
</tr>
<tr>
<td></td>
<td>`peer { group-name</td>
<td>ipv4-address [mask-length] } preferred-value`</td>
</tr>
<tr>
<td>16.</td>
<td>Configure the device as a route reflector and the 6PE peer or peer group as a client.</td>
<td>By default, no route reflector or client is configured.</td>
</tr>
<tr>
<td></td>
<td>`peer { group-name</td>
<td>ipv4-address [mask-length] } reflect-client`</td>
</tr>
<tr>
<td>17.</td>
<td>Configure the SoO attribute for a peer or peer group.</td>
<td>By default, no SoO attribute is configured for a peer or peer group.</td>
</tr>
<tr>
<td></td>
<td>`peer { group-name</td>
<td>ipv4-address [mask-length] } soo site-of-origin`</td>
</tr>
<tr>
<td>18.</td>
<td>Return to user view.</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td><code>return</code></td>
<td></td>
</tr>
<tr>
<td>19.</td>
<td>Display information about the 6PE peer or peer group.</td>
<td>Available in any view.</td>
</tr>
<tr>
<td></td>
<td>`display bgp [instance instance-name] peer ipv6 [unicast] [ipv4-address mask-length] {ipv4-address</td>
<td>group-name group-name } log-info</td>
</tr>
<tr>
<td>20.</td>
<td>Display routing information advertised to or received from the 6PE peer or peer group.</td>
<td>Available in any view.</td>
</tr>
<tr>
<td></td>
<td>`display bgp [instance instance-name] routing-table ipv6 [unicast] peer ipv4-address {advertised-routes</td>
<td>received-routes} [ipv6-address prefix-length] statistics ]`</td>
</tr>
<tr>
<td></td>
<td>`refresh bgp [instance instance-name] ipv4-address [mask-length] {export</td>
<td>import} ipv6 [unicast]`</td>
</tr>
<tr>
<td>22.</td>
<td>Reset a BGP 6PE connection.</td>
<td>Available in user view.</td>
</tr>
<tr>
<td></td>
<td><code>reset bgp [instance instance-name] ipv4-address [mask-length] ipv6 [unicast]</code></td>
<td></td>
</tr>
</tbody>
</table>

**Displaying and maintaining BGP**

**Displaying BGP**

Execute `display` commands in any view (IPv4 unicast address family).
<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display BGP NSR status information.</td>
<td>display bgp [instance instance-name] non-stop-routing status</td>
</tr>
<tr>
<td>Display BGP IPv4 unicast peer group information.</td>
<td>display bgp [instance instance-name] group ipv4 [unicast]</td>
</tr>
<tr>
<td>Display BGP IPv4 unicast or peer group information.</td>
<td>display bgp [instance instance-name] peer ipv4 [unicast]</td>
</tr>
<tr>
<td>Display BGP IPv4 unicast routing information.</td>
<td>display bgp [instance instance-name] routing-table ipv4 [unicast]</td>
</tr>
<tr>
<td>Display BGP IPv6 unicast routing information.</td>
<td>display bgp [instance instance-name] routing-table ipv6 [unicast]</td>
</tr>
<tr>
<td>Display information about routes advertised by the network command and shortcut routes configured by the network short-cut command.</td>
<td>display bgp [instance instance-name] network ipv4 [unicast]</td>
</tr>
<tr>
<td>Display BGP path attribute information.</td>
<td>display bgp [instance instance-name] paths</td>
</tr>
<tr>
<td>Display BGP IPv4 unicast address family update group information.</td>
<td>display bgp [instance instance-name] update-group ipv4 [unicast]</td>
</tr>
<tr>
<td>Display BGP policy accounting information for IPv4 traffic.</td>
<td>display bgp-policy ipv4 statistics [input</td>
</tr>
<tr>
<td>Display information about all BGP instances.</td>
<td>display bgp instance-info</td>
</tr>
</tbody>
</table>

Execute `display` commands in any view (IPv6 unicast address family).
<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display BGP IPv6 unicast routing information.</td>
<td>display bgp [ instance instance-name ] peer ipv6 [ unicast ] [ ipv4-address mask-length</td>
</tr>
<tr>
<td>Display dampened BGP IPv6 unicast routing information.</td>
<td>display bgp [ instance instance-name ] routing-table ipv6 [ unicast ] [ vpn-instance vpn-instance-name ] [ ipv6-address prefix-length</td>
</tr>
<tr>
<td>Display BGP dampening parameter information.</td>
<td>display bgp [ instance instance-name ] dampening parameter ipv6 [ unicast ] [ vpn-instance vpn-instance-name ]</td>
</tr>
<tr>
<td>Display BGP IPv6 unicast routing flap statistics.</td>
<td>display bgp [ instance instance-name ] routing-table flap-info ipv6 [ unicast ] [ vpn-instance vpn-instance-name ] [ ipv6-address prefix-length</td>
</tr>
<tr>
<td>Display incoming labels for BGP IPv6 unicast routes.</td>
<td>display bgp [ instance instance-name ] routing-table ipv6 [ unicast ] inlabel</td>
</tr>
<tr>
<td>Display outgoing labels of BGP IPv6 unicast routes.</td>
<td>display bgp [ instance instance-name ] routing-table ipv6 [ unicast ] outlabel</td>
</tr>
<tr>
<td>Display information about routes advertised by the network command and shortcut routes configured by the network short-cut command.</td>
<td>display bgp [ instance instance-name ] network ipv6 [ unicast ] [ vpn-instance vpn-instance-name ]</td>
</tr>
<tr>
<td>Display BGP path attribute information.</td>
<td>display bgp [ instance instance-name ] paths as-regular-expression</td>
</tr>
</tbody>
</table>
| Display BGP IPv6 unicast address family update group information. | display bgp [ instance instance-name ] update-group ipv6 [ unicast ] [ ipv4-address | ipv6-address ]
display bgp [ instance instance-name ] update-group ipv6 [ unicast ] [ vpn-instance vpn-instance-name | ipv6-address ]
| Display BGP policy accounting information for IPv6 traffic. | display bgp-policy ipv6 statistics { input | output } [ interface interface-type interface-number ] |
| Display information about all BGP instances. | display bgp instance-info |

Display commands in any view (IPv4 multicast address family).

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display BGP NSR status information.</td>
<td>display bgp [ instance instance-name ] non-stop-routing status</td>
</tr>
<tr>
<td>Display BGP IPv4 multicast peer group information.</td>
<td>display bgp [ instance instance-name ] group ipv4 multicast [ group-name ] group-name</td>
</tr>
<tr>
<td>Display BGP IPv4 multicast peer or peer group information.</td>
<td>display bgp [ instance instance-name ] peer ipv4 multicast [ ipv4-address mask-length</td>
</tr>
<tr>
<td>Task</td>
<td>Command</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Display BGP IPv4 multicast routing information.</td>
<td>`display bgp [ instance instance-name ] routing-table ipv4 multicast [ ipv4-address [ { mask</td>
</tr>
<tr>
<td>Display dampened BGP IPv4 multicast routing information.</td>
<td><code>display bgp [ instance instance-name ] routing-table dampened ipv4 multicast</code></td>
</tr>
<tr>
<td>Display BGP dampening parameter information.</td>
<td><code>display bgp [ instance instance-name ] dampening parameter ipv4 multicast</code></td>
</tr>
<tr>
<td>Display BGP IPv4 multicast routing flap statistics.</td>
<td>`display bgp [ instance instance-name ] routing-table flap-info ipv4 multicast [ ipv4-address [ { mask</td>
</tr>
<tr>
<td>Display information about routes advertised by the <code>network</code> command and shortcut routes configured by the <code>network short-cut</code> command.</td>
<td><code>display bgp [ instance instance-name ] network ipv4 multicast</code></td>
</tr>
<tr>
<td>Display BGP path attribute information.</td>
<td><code>display bgp [ instance instance-name ] paths [ as-regular-expression ]</code></td>
</tr>
<tr>
<td>Display BGP IPv4 multicast address family update group information.</td>
<td><code>display bgp [ instance instance-name ] update-group ipv4 multicast [ ipv4-address ]</code></td>
</tr>
<tr>
<td>Display information about all BGP instances.</td>
<td><code>display bgp instance-info</code></td>
</tr>
</tbody>
</table>

**Execute `display` commands in any view (IPv6 multicast address family).**

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display BGP NSR status information.</td>
<td><code>display bgp [ instance instance-name ] non-stop-routing status</code></td>
</tr>
<tr>
<td>Display BGP IPv6 multicast peer group information.</td>
<td><code>display bgp [ instance instance-name ] group ipv6 multicast [ group-name group-name ]</code></td>
</tr>
<tr>
<td>Display BGP IPv6 multicast peer or peer group information.</td>
<td>`display bgp [ instance instance-name ] peer ipv6 multicast [ ipv6-address prefix-length ] { ipv6-address</td>
</tr>
<tr>
<td>Display BGP IPv6 multicast routing information.</td>
<td>`display bgp [ instance instance-name ] routing-table ipv6 multicast [ ipv6-address prefix-length</td>
</tr>
<tr>
<td>Display dampened BGP IPv6 multicast routing information.</td>
<td><code>display bgp [ instance instance-name ] routing-table dampened ipv6 multicast</code></td>
</tr>
<tr>
<td>Display BGP dampening parameter information.</td>
<td><code>display bgp [ instance instance-name ] dampening parameter ipv6 multicast</code></td>
</tr>
<tr>
<td>Display BGP IPv6 multicast routing flap statistics.</td>
<td>`display bgp [ instance instance-name ] routing-table flap-info ipv6 multicast [ ipv6-address prefix-length</td>
</tr>
</tbody>
</table>
### Resetting BGP sessions

Execute `reset` commands in user view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset all BGP sessions.</td>
<td><code>reset bgp [ instance instance-name ] all</code></td>
</tr>
<tr>
<td>Reset BGP sessions for IPv4 unicast address family.</td>
<td>`reset bgp [ instance instance-name ] { as-number</td>
</tr>
<tr>
<td>Reset BGP sessions for IPv6 unicast address family.</td>
<td>`reset bgp [ instance instance-name ] { as-number</td>
</tr>
<tr>
<td>Reset BGP sessions for IPv4 multicast address family.</td>
<td>`reset bgp [ instance instance-name ] { as-number</td>
</tr>
<tr>
<td>Reset BGP sessions for IPv6 multicast address family.</td>
<td>`reset bgp [ instance instance-name ] { as-number</td>
</tr>
</tbody>
</table>

### Clearing BGP information

Execute `reset` commands in user view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear dampening information for BGP IPv4 unicast routes and release suppressed BGP IPv4 unicast routes.</td>
<td>`reset bgp [ instance instance-name ] dampening ipv4 [ unicast</td>
</tr>
<tr>
<td>Clear flap information for BGP IPv4 unicast routes.</td>
<td>`reset bgp [ instance instance-name ] flap-info ipv4 [ unicast</td>
</tr>
<tr>
<td>Clear dampening information for BGP IPv6 unicast routes and release suppressed BGP IPv6 unicast routes.</td>
<td>`reset bgp [ instance instance-name ] dampening ipv6 [ unicast</td>
</tr>
</tbody>
</table>
### IPv4 BGP configuration examples

#### Basic BGP configuration example

**Network requirements**

As shown in Figure 67, all routers run BGP. Run EBGP between Router A and Router B, and run IBGP between Router B and Router C to allow Router C to access network 8.1.1.0/24 connected to Router A.

**Figure 67 Network diagram**

To prevent route flapping caused by port state changes, this example uses loopback interfaces to establish IBGP connections. Because loopback interfaces are virtual interfaces, you need to use the `peer connect-interface` command to specify the loopback interface as the source interface for establishing BGP connections. Enable OSPF in AS 65009 to ensure that Router B can communicate with Router C through loopback interfaces.

The EBGP peers, Router A and Router B (usually in different ISPs), are located in different ASs. Typically, their loopback interfaces are not reachable to each other, so directly connected interfaces are used for establishing EBGP sessions. To enable Router C to access the network 8.1.1.0/24 connected directly to Router A, inject network 8.1.1.0/24 to the BGP routing table of Router A.

**Configuration procedure**

1. Configure IP addresses for interfaces. (Details not shown.)
2. Configure IBGP:

---

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear flap information for BGP IPv6 unicast routes.</td>
<td>`reset bgp [ instance instance-name ] flap-info ipv6 [ unicast ] [ vpn-instance vpn-instance-name ] [ ipv6-address prefix-length</td>
</tr>
<tr>
<td>Clear dampening information for BGP IPv4 multicast routes and release suppressed BGP IPv4 multicast routes.</td>
<td>`reset bgp [ instance instance-name ] dampening ipv4 multicast [ ipv4-address [ mask</td>
</tr>
<tr>
<td>Clear flap information for BGP IPv4 multicast routes.</td>
<td>`reset bgp [ instance instance-name ] flap-info ipv4 multicast [ ipv4-address [ mask</td>
</tr>
<tr>
<td>Clear dampening information for BGP IPv6 multicast routes and release suppressed BGP IPv6 multicast routes.</td>
<td><code>reset bgp [ instance instance-name ] dampening ipv6 multicast [ ipv6-address prefix-length ]</code></td>
</tr>
<tr>
<td>Clear flap information for BGP IPv6 multicast routes.</td>
<td>`reset bgp [ instance instance-name ] flap-info ipv6 multicast [ ipv6-address prefix-length</td>
</tr>
</tbody>
</table>
# Configure Router B.

```
<RouterB> system-view
[RouterB] bgp 65009
[RouterB-bgp-default] router-id 2.2.2.2
[RouterB-bgp-default] peer 3.3.3.3 as-number 65009
[RouterB-bgp-default] peer 3.3.3.3 connect-interface loopback 0
[RouterB-bgp-default] address-family ipv4 unicast
[RouterB-bgp-default-ipv4] peer 3.3.3.3 enable
[RouterB-bgp-default-ipv4] quit
[RouterB-bgp-default] quit
[RouterB] ospf 1
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[RouterB-ospf-1-area-0.0.0.0] network 9.1.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] quit
```

# Configure Router C.

```
<RouterC> system-view
[RouterC] bgp 65009
[RouterC-bgp-default] router-id 3.3.3.3
[RouterC-bgp-default] peer 2.2.2.2 as-number 65009
[RouterC-bgp-default] peer 2.2.2.2 connect-interface loopback 0
[RouterC-bgp-default] address-family ipv4 unicast
[RouterC-bgp-default-ipv4] peer 2.2.2.2 enable
[RouterC-bgp-default-ipv4] quit
[RouterC-bgp-default] quit
[RouterC] ospf 1
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[RouterC-ospf-1-area-0.0.0.0] network 9.1.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] quit
[RouterC-ospf-1] quit
[RouterC] display bgp peer ipv4
```

```
BGP local router ID : 3.3.3.3
Local AS number : 65009
Total number of peers : 1                 Peers in established state : 1

* - Dynamically created peer
Peer                AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

2.2.2.2              65009        7       10    0       0 00:06:09 Established
```

The output shows that Router C has established an IBGP peer relationship with Router B.

3. Configure EBGP:

# Configure Router A.

```
<RouterA> system-view
[RouterA] bgp 65008
[RouterA-bgp-default] router-id 1.1.1.1
```
# Configure Router A.

[RouterA-bgp-default] peer 3.1.1.1 as-number 65009
[RouterA-bgp-default] address-family ipv4 unicast
[RouterA-bgp-default-ipv4] peer 3.1.1.1 enable
[RouterA-bgp-default-ipv4] network 8.1.1.0 24
[RouterA-bgp-default-ipv4] quit
[RouterA-bgp-default] quit

# Configure Router B.

[RouterB] bgp 65009
[RouterB-bgp-default] peer 3.1.1.2 as-number 65008
[RouterB-bgp-default] address-family ipv4 unicast
[RouterB-bgp-default-ipv4] peer 3.1.1.2 enable
[RouterB-bgp-default-ipv4] quit
[RouterB-bgp-default] quit

# Display BGP peer information on Router B.

[RouterB] display bgp peer ipv4

BGP local router ID : 2.2.2.2
Local AS number : 65009
Total number of peers : 2                 Peers in established state : 2

* - Dynamically created peer
Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State
3.3.3.3              65009       12       10    0       3 00:09:16 Established
3.1.1.2              65008        3        3    0       1 00:00:08 Established

The output shows that Router B has established an IBGP peer relationship with Router C and an EBGP peer relationship with Router A.

# Display the BGP routing table on Router A.

[RouterA] display bgp routing-table ipv4

Total number of routes: 1

BGP local router ID is 1.1.1.1
Status codes: * - valid, > - best, d - dampened, h - history,
        s - suppressed, S - stale, i - internal, e - external
        Origin: i - IGP, e - EGP, ? - incomplete

Network            NextHop         MED        LocPrf     PrefVal Path/Ogn
* >  8.1.1.0/24         8.1.1.1         0                     32768   i

# Display the BGP routing table on Router B.

[RouterB] display bgp routing-table ipv4

Total number of routes: 1

BGP local router ID is 2.2.2.2
Status codes: * - valid, > - best, d - dampened, h - history,
        s - suppressed, S - stale, i - internal, e - external
### Display the BGP routing table on Router C.

```bash
[RouterC] display bgp routing-table ipv4
```

Total number of routes: 1

BGP local router ID is 3.3.3.3

Status codes: * - valid, > - best, d - dampened, h - history,
s - suppressed, S - stale, i - internal, e - external

<table>
<thead>
<tr>
<th>Network</th>
<th>NextHop</th>
<th>MED</th>
<th>LocPrf</th>
<th>PrefVal</th>
<th>Path/Ogn</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0/24</td>
<td>3.1.1.2</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>650081</td>
</tr>
</tbody>
</table>

The outputs show that Router A has no route to AS 65009, and Router C has learned network 8.1.1.0, but the next hop 3.1.1.2 is unreachable. As a result, the route is invalid.

#### 4. Redistribute direct routes:

Configure BGP to redistribute direct routes on Router B, so Router A can obtain the route to 9.1.1.0/24, and Router C can obtain the route to 3.1.1.0/24.

**# Configure Router B.**

```bash
[RouterB] bgp 65009
[RouterB-bgp-default] address-family ipv4 unicast
[RouterB-bgp-default-ipv4] import-route direct
[RouterB-bgp-default-ipv4] quit
[RouterB-bgp-default] quit
```

**# Display the BGP routing table on Router A.**

```bash
[RouterA] display bgp routing-table ipv4
```

Total number of routes: 4

BGP local router ID is 1.1.1.1

Status codes: * - valid, > - best, d - dampened, h - history,
s - suppressed, S - stale, i - internal, e - external

<table>
<thead>
<tr>
<th>Network</th>
<th>NextHop</th>
<th>MED</th>
<th>LocPrf</th>
<th>PrefVal</th>
<th>Path/Ogn</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2.2.2/32</td>
<td>3.1.1.1</td>
<td>0</td>
<td>0</td>
<td>65009?</td>
<td></td>
</tr>
<tr>
<td>3.1.1.0/24</td>
<td>3.1.1.1</td>
<td>0</td>
<td>0</td>
<td>65009?</td>
<td></td>
</tr>
<tr>
<td>8.1.1.0/24</td>
<td>8.1.1.1</td>
<td>0</td>
<td>32768</td>
<td>i</td>
<td></td>
</tr>
<tr>
<td>9.1.1.0/24</td>
<td>3.1.1.1</td>
<td>0</td>
<td>0</td>
<td>65009?</td>
<td></td>
</tr>
</tbody>
</table>

Two routes 2.2.2.2/32 and 9.1.1.0/24 have been added in Router A's routing table.

**# Display the BGP routing table on Router C.**

```bash
[RouterC] display bgp routing-table ipv4
```
Total number of routes: 4

BGP local router ID is 3.3.3.3

Status codes: * - valid, > - best, d - dampened, h - history,
s - suppressed, S - stale, i - internal, e - external
Origin: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>NextHop</th>
<th>MED</th>
<th>LocPrf</th>
<th>PrefVal</th>
<th>Path/Ogn</th>
</tr>
</thead>
<tbody>
<tr>
<td>* &gt;i 2.2.2.2/32</td>
<td>2.2.2.2</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>* &gt;i 3.1.1.0/24</td>
<td>2.2.2.2</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>* &gt;i 8.1.1.0/24</td>
<td>3.1.1.2</td>
<td>0</td>
<td>100</td>
<td>650081</td>
<td></td>
</tr>
<tr>
<td>* &gt;i 9.1.1.0/24</td>
<td>2.2.2.2</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
</tbody>
</table>

The output shows that the route 8.1.1.0 has become valid and the next hop is Router A.

Verifying the configuration

```
# Verify that Router C can ping 8.1.1.1.

[RouterC] ping 8.1.1.1

Ping 8.1.1.1 (8.1.1.1): 56 data bytes, press CTRL_C to break
56 bytes from 8.1.1.1: icmp_seq=0 ttl=255 time=2.000 ms
56 bytes from 8.1.1.1: icmp_seq=1 ttl=255 time=0.000 ms
56 bytes from 8.1.1.1: icmp_seq=2 ttl=255 time=0.000 ms
56 bytes from 8.1.1.1: icmp_seq=3 ttl=255 time=0.000 ms
56 bytes from 8.1.1.1: icmp_seq=4 ttl=255 time=1.000 ms

--- Ping statistics for 8.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/0.600/2.000/0.800 ms
```

BGP and IGP route redistribution configuration example

Network requirements

As shown in Figure 68, all devices of company A belong to AS 65008 and all devices of company B belong to AS 65009.

Configure BGP and IGP route redistribution to allow Router A to access network 9.1.2.0/24 in AS 65009, and Router C to access network 8.1.1.0/24 in AS 65008.

Figure 68 Network diagram
Requirements analysis

Configure BGP to redistribute routes from OSPF on Router B, so Router A can obtain the route to 9.1.2.0/24. Configure OSPF to redistribute routes from BGP on Router B, so that Router C can obtain the route to 8.1.1.0/24.

Configuration procedure

1. Configure IP addresses for interfaces. (Details not shown.)
2. Configure OSPF:

   Enable OSPF in AS 65009, so Router B can obtain the route to 9.1.2.0/24.

   # Configure Router B.
   
   <RouterB> system-view
   [RouterB] ospf 1
   [RouterB-ospf-1] area 0
   [RouterB-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
   [RouterB-ospf-1-area-0.0.0.0] network 9.1.1.0 0.0.0.255
   [RouterB-ospf-1-area-0.0.0.0] quit
   [RouterB-ospf-1] quit

   # Configure Router C.
   
   <RouterC> system-view
   [RouterC] ospf 1
   [RouterC-ospf-1] import-route direct
   [RouterC-ospf-1-area-0.0.0.0] network 9.1.1.0 0.0.0.255
   [RouterC-ospf-1-area-0.0.0.0] quit

3. Configure the EBGP connection:

   Configure the EBGP connection and inject network 8.1.1.0/24 to the BGP routing table of Router A, so Router B can obtain the route to 8.1.1.0/24.

   # Configure Router A.
   
   <RouterA> system-view
   [RouterA] bgp 65008
   [RouterA-bgp-default] router-id 1.1.1.1
   [RouterA-bgp-default] peer 3.1.1.1 as-number 65009
   [RouterA-bgp-default] address-family ipv4 unicast
   [RouterA-bgp-default-ipv4] peer 3.1.1.1 enable
   [RouterA-bgp-default-ipv4] network 8.1.1.0 24
   [RouterA-bgp-default-ipv4] quit
   [RouterA-bgp-default] quit

   # Configure Router B.
   
   [RouterB] bgp 65009
   [RouterB-bgp-default] router-id 2.2.2.2
   [RouterB-bgp-default] peer 3.1.1.2 as-number 65008
   [RouterB-bgp-default] address-family ipv4 unicast
   [RouterB-bgp-default-ipv4] peer 3.1.1.2 enable

4. Configure BGP and IGP route redistribution:

   # Configure route redistribution between BGP and OSPF on Router B.
   
   [RouterB-bgp-default-ipv4] import-route ospf 1
   [RouterB-bgp-default-ipv4] quit
[RouterB-bgp-default] quit
[RouterB] ospf 1
[RouterB-ospf-1] import-route bgp
[RouterB-ospf-1] quit

# Display the BGP routing table on Router A.
[RouterA] display bgp routing-table ipv4

Total number of routes: 3

BGP local router ID is 1.1.1.1
Status codes: * - valid, > - best, d - dampened, h - history, s - suppressed, S - stale, i - internal, e - external
Origin: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>NextHop</th>
<th>MED</th>
<th>LocPrf</th>
<th>PrefVal</th>
<th>Path/Ogn</th>
</tr>
</thead>
<tbody>
<tr>
<td>* &gt;e 3.3.3.3/32</td>
<td>3.1.1.1</td>
<td>1</td>
<td></td>
<td>0</td>
<td>65009?</td>
</tr>
<tr>
<td>* &gt; 8.1.1.0/24</td>
<td>8.1.1.1</td>
<td>0</td>
<td></td>
<td>32768</td>
<td>i</td>
</tr>
<tr>
<td>* &gt;e 9.1.2.0/24</td>
<td>3.1.1.1</td>
<td>1</td>
<td></td>
<td>0</td>
<td>65009?</td>
</tr>
</tbody>
</table>

# Display the OSPF routing table on Router C.
[RouterC] display ospf routing

OSPF Process 1 with Router ID 3.3.3.3
Routing Tables

Routing for Network
<table>
<thead>
<tr>
<th>Destination</th>
<th>Cost</th>
<th>Type</th>
<th>NextHop</th>
<th>AdvRouter</th>
<th>Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.1.1.0/24</td>
<td>1</td>
<td>Transit</td>
<td>9.1.1.2</td>
<td>3.3.3.3</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>2.2.2.2/32</td>
<td>1</td>
<td>Stub</td>
<td>9.1.1.1</td>
<td>2.2.2.2</td>
<td>0.0.0.0</td>
</tr>
</tbody>
</table>

Routing for ASEs
<table>
<thead>
<tr>
<th>Destination</th>
<th>Cost</th>
<th>Type</th>
<th>Tag</th>
<th>NextHop</th>
<th>AdvRouter</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0/24</td>
<td>1</td>
<td>Type2</td>
<td>1</td>
<td>9.1.1.1</td>
<td>2.2.2.2</td>
</tr>
</tbody>
</table>

Total Nets: 3
Intra Area: 2  Inter Area: 0  ASE: 1  NSSA: 0

Verifying the configuration

# Use ping to test connectivity.
[RouterA] ping -a 8.1.1.1 9.1.2.1
Ping 9.1.2.1 (9.1.2.1) from 8.1.1.1: 56 data bytes, press CTRL_C to break
56 bytes from 9.1.2.1: icmp_seq=0 ttl=254 time=10.000 ms
56 bytes from 9.1.2.1: icmp_seq=1 ttl=254 time=12.000 ms
56 bytes from 9.1.2.1: icmp_seq=2 ttl=254 time=2.000 ms
56 bytes from 9.1.2.1: icmp_seq=3 ttl=254 time=7.000 ms
56 bytes from 9.1.2.1: icmp_seq=4 ttl=254 time=9.000 ms

--- Ping statistics for 9.1.2.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
BGP route summarization configuration example

Network requirements

As shown in Figure 69, run EBGP between Router C and Router D, so the internal network and external network can communicate with each other.

- In AS 65106, perform the following configurations so the devices in the internal network can communicate:
  - Configure static routing between Router A and Router B.
  - Configure OSPF between Router B and Router C.
  - Configure OSPF to redistribute static routes.

- Configure route summarization on Router C so BGP advertises a summary route instead of advertising routes to the 192.168.64.0/24, 192.168.74.0/24, and 192.168.99.0/24 networks to Router D.

Figure 69 Network diagram

Configuration procedure

1. Configure IP addresses for interfaces. (Details not shown.)
2. Configure static routing between Router A and Router B:

   # Configure a default route with the next hop 192.168.212.1 on Router A.

   <RouterA> system-view
   [RouterA] ip route-static 0.0.0.0 0 192.168.212.1
# Configure static routes to 192.168.64.0/24, 192.168.74.0/24, and 192.168.99.0/24 with the same next hop 192.168.212.161 on Router B.

```
<RouterB> system-view
[RouterB] ip route-static 192.168.64.0 24 192.168.212.161
[RouterB] ip route-static 192.168.74.0 24 192.168.212.161
```

3. Configure OSPF between Router B and Router C and configure OSPF on Router B to redistribute static routes:

```
# Configure OSPF to advertise the local network and enable OSPF to redistribute static routes on Router B.

[RouterB] ospf
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 172.17.100.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] import-route static
[RouterB-ospf-1] quit

# Configure OSPF to advertise local networks on Router C.

[RouterC] ospf
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] network 172.17.100.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] network 10.220.2.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] quit
[RouterC-ospf-1] quit

# Display the IP routing table on Router C.

[RouterC] display ip routing-table protocol ospf

Summary count : 5
OSPF Routing table Status : <Active>
Summary count : 3

<table>
<thead>
<tr>
<th>Destination/Mask</th>
<th>Proto</th>
<th>Pre</th>
<th>Cost</th>
<th>NextHop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.64.0/24</td>
<td>OSPF</td>
<td>150</td>
<td>1</td>
<td>172.17.100.1</td>
<td>GE1/0/1</td>
</tr>
<tr>
<td>192.168.74.0/24</td>
<td>OSPF</td>
<td>150</td>
<td>1</td>
<td>172.17.100.1</td>
<td>GE1/0/1</td>
</tr>
<tr>
<td>192.168.99.0/24</td>
<td>OSPF</td>
<td>150</td>
<td>1</td>
<td>172.17.100.1</td>
<td>GE1/0/1</td>
</tr>
</tbody>
</table>

OSPF Routing table Status : <Inactive>
Summary count : 2

<table>
<thead>
<tr>
<th>Destination/Mask</th>
<th>Proto</th>
<th>Pre</th>
<th>Cost</th>
<th>NextHop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.220.2.0/24</td>
<td>OSPF</td>
<td>10</td>
<td>1</td>
<td>10.220.2.16</td>
<td>GE1/0/2</td>
</tr>
<tr>
<td>172.17.100.0/24</td>
<td>OSPF</td>
<td>10</td>
<td>1</td>
<td>172.17.100.2</td>
<td>GE1/0/1</td>
</tr>
</tbody>
</table>

The output shows that Router C has learned routes to 192.168.64.0/24, 192.168.74.0/24, and 192.168.99.0/24 through OSPF.

4. Configure BGP between Router C and Router D and configure BGP on Router C to redistribute OSPF routes:

```
# On Router C, enable BGP, specify Router D as an EBGP peer, and configure BGP to redistribute OSPF routes.

[RouterC] bgp 65106
```
# Enable BGP, and configure Router C as an EBGP peer on Router D.

```bash
[RouterD] bgp 64631
[RouterD-bgp-default] router-id 4.4.4.4
[RouterD-bgp-default] peer 10.220.2.16 as-number 65106
[RouterD-bgp-default] address-family ipv4 unicast
[RouterD-bgp-default-ipv4] peer 10.220.2.16 enable
[RouterD-bgp-default-ipv4] quit
[RouterD-bgp-default] quit
```

# Display routing table information on Router D.

```bash
[RouterD] display ip routing-table protocol bgp
```

Summary count : 3

BGP Routing table Status : <Active>

Summary count : 3

<table>
<thead>
<tr>
<th>Destination/Mask</th>
<th>Proto</th>
<th>Pre</th>
<th>Cost</th>
<th>NextHop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.64.0/24</td>
<td>BGP</td>
<td>255</td>
<td>1</td>
<td>10.220.2.16</td>
<td>GE1/0/1</td>
</tr>
<tr>
<td>192.168.74.0/24</td>
<td>BGP</td>
<td>255</td>
<td>1</td>
<td>10.220.2.16</td>
<td>GE1/0/1</td>
</tr>
<tr>
<td>192.168.99.0/24</td>
<td>BGP</td>
<td>255</td>
<td>1</td>
<td>10.220.2.16</td>
<td>GE1/0/1</td>
</tr>
</tbody>
</table>

BGP Routing table Status : <Inactive>

Summary count : 0

The output shows that Router D has learned routes to 192.168.64.0/24, 192.168.74.0/24, and 192.168.99.0/24 through BGP.

# Ping the hosts on networks 192.168.64.0/24, 192.168.74.0/24, and 192.168.99.0/24 from Router D. The ping operations succeed.

5. Configure route summarization on Router C to summarize 192.168.64.0/24, 192.168.74.0/24, and 192.168.99.0/24 into a single route 192.168.64.0/18, and disable advertisement of specific routes.

```bash
[RouterC-bgp-default-ipv4] aggregate 192.168.64.0 18 detail-suppressed
[RouterC-bgp-default-ipv4] quit
[RouterC-bgp-default] quit
```

Verifying the configuration

# Display IP routing table information on Router C.

```bash
[RouterC] display ip routing-table | include 192.168
```

<table>
<thead>
<tr>
<th>Destination/Mask</th>
<th>Proto</th>
<th>Pre</th>
<th>Cost</th>
<th>NextHop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.64.0/18</td>
<td>BGP</td>
<td>130</td>
<td>0</td>
<td>127.0.0.1</td>
<td>NULL0</td>
</tr>
<tr>
<td>192.168.64.0/24</td>
<td>OSPF</td>
<td>150</td>
<td>1</td>
<td>172.17.100.1</td>
<td>GE1/0/1</td>
</tr>
<tr>
<td>192.168.74.0/24</td>
<td>OSPF</td>
<td>150</td>
<td>1</td>
<td>172.17.100.1</td>
<td>GE1/0/1</td>
</tr>
<tr>
<td>192.168.99.0/24</td>
<td>OSPF</td>
<td>150</td>
<td>1</td>
<td>172.17.100.1</td>
<td>GE1/0/1</td>
</tr>
</tbody>
</table>

The output shows that Router C has a summary route 192.168.64.0/18 with the egress interface Null 0.

# Display the IP routing table information on Router D.
[RouterD] display ip routing-table protocol bgp

Summary count : 1

BGP Routing table Status : <Active>
Summary count : 1

<table>
<thead>
<tr>
<th>Destination/Mask</th>
<th>Proto</th>
<th>Pre</th>
<th>Cost</th>
<th>NextHop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.64.0/18</td>
<td>BGP</td>
<td>255</td>
<td>0</td>
<td>10.220.2.16</td>
<td>GE1/0/1</td>
</tr>
</tbody>
</table>

BGP Routing table Status : <Inactive>
Summary count : 0

The output shows that Router D has only one route 192.168.64.0/18 to AS 65106.

# Verify that Router D can ping the hosts on subnets 192.168.64.0/24, 192.168.74.0/24, and 192.168.99.0/24. (Details not shown.)

## BGP load balancing configuration example

### Network requirements

As shown in Figure 70, run EBGP between Router A and Router B, and between Router A and Router C. Run IBGP between Router B and Router C.

Configure load balancing over the two EBGP links on Router A.

### Requirements analysis

On Router A, establish EBGP connections with Router B and Router C. Configure BGP to advertise network 8.1.1.0/24 to Router B and Router C. This allows Router B and Router C can access the internal network connected to Router A.

On Router B, establish an EBGP connection with Router A and an IBGP connection with Router C. Configure BGP to advertise network 9.1.1.0/24 to Router A, so that Router A can access the intranet through Router B. Configure a static route to interface loopback 0 on Router C (or use a routing protocol like OSPF) to establish the IBGP connection.

On Router C, establish an EBGP connection with Router A and an IBGP connection with Router B. Configure BGP to advertise network 9.1.1.0/24 to Router A, so that Router A can access the intranet...
through Router C. Configure a static route to interface loopback 0 on Router B (or use another protocol like OSPF) to establish the IBGP connection.

Configure load balancing on Router A.

Configuration procedure

1. Configure IP addresses for interfaces. (Details not shown.)
2. Configure BGP connections:

   # Configure Router A.
   <RouterA> system-view
   [RouterA] bgp 65008
   [RouterA-bgp-default] router-id 1.1.1.1
   [RouterA-bgp-default] peer 3.1.1.1 as-number 65009
   [RouterA-bgp-default] peer 3.1.2.1 as-number 65009
   [RouterA-bgp-default] address-family ipv4 unicast
   [RouterA-bgp-default-ipv4] peer 3.1.1.1 enable
   [RouterA-bgp-default-ipv4] peer 3.1.2.1 enable
   [RouterA-bgp-default-ipv4] network 8.1.1.0 24
   [RouterA-bgp-default-ipv4] quit
   [RouterA-bgp-default] quit

   # Configure Router B.
   <RouterB> system-view
   [RouterB] bgp 65009
   [RouterB-bgp-default] router-id 2.2.2.2
   [RouterB-bgp-default] peer 3.1.1.2 as-number 65008
   [RouterB-bgp-default] peer 3.3.3.3 as-number 65009
   [RouterB-bgp-default] peer 3.3.3.3 connect-interface loopback 0
   [RouterB-bgp-default] address-family ipv4 unicast
   [RouterB-bgp-default-ipv4] peer 3.1.1.2 enable
   [RouterB-bgp-default-ipv4] peer 3.3.3.3 enable
   [RouterB-bgp-default-ipv4] network 9.1.1.0 24
   [RouterB-bgp-default-ipv4] quit
   [RouterB-bgp-default] quit
   [RouterB] ip route-static 3.3.3.3 32 9.1.1.2

   # Configure Router C.
   <RouterC> system-view
   [RouterC] bgp 65009
   [RouterC-bgp-default] router-id 3.3.3.3
   [RouterC-bgp-default] peer 3.1.2.2 as-number 65008
   [RouterC-bgp-default] peer 2.2.2.2 as-number 65009
   [RouterC-bgp-default] peer 2.2.2.2 connect-interface loopback 0
   [RouterC-bgp-default] address-family ipv4 unicast
   [RouterC-bgp-default-ipv4] peer 3.1.2.2 enable
   [RouterC-bgp-default-ipv4] peer 2.2.2.2 enable
   [RouterC-bgp-default-ipv4] network 9.1.1.0 24
   [RouterC-bgp-default-ipv4] quit
   [RouterC-bgp-default] quit
   [RouterC] ip route-static 2.2.2.2 32 9.1.1.1

   # Display the BGP routing table on Router A.

319
[RouterA] display bgp routing-table ipv4

Total number of routes: 3

BGP local router ID is 1.1.1.1

Status codes: * - valid, > - best, d - dampened, h - history,
               s - suppressed, S - stale, i - internal, e - external
               Origin: i - IGP, e - EGP, ? - incomplete

Network            NextHop         MED        LocPrf     PrefVal Path/Ogn
* >  8.1.1.0/24         8.1.1.1         0                     32768       i
* >e 9.1.1.0/24         3.1.1.1         0                     0       65009i
*  e                    3.1.2.1         0                     0       65009i

The output shows two valid routes to destination 9.1.1.0/24. The route with next hop 3.1.1.1 is marked with a greater-than sign (>), indicating that it is the optimal route. The route with next hop 3.1.2.1 is marked with an asterisk (*), indicating that it is a valid route, but not the optimal route.

By using the display ip routing-table command, you can find there is only one route to 9.1.1.0/24 with next hop 3.1.1.1 and egress interface GigabitEthernet 1/0/2.

3. On Router A, configure the maximum number of ECMP routes destined for AS 65009 as 2 to improve link usage.

[RouterA] bgp 65008
[RouterA-bgp-default] address-family ipv4 unicast
[RouterA-bgp-default-ipv4] quit
[RouterA-bgp-default] quit

Verifying the configuration

# Display the BGP routing table on Router A.
[RouterA] display bgp routing-table ipv4

Total number of routes: 3

BGP local router ID is 1.1.1.1

Status codes: * - valid, > - best, d - dampened, h - history,
               s - suppressed, S - stale, i - internal, e - external
               Origin: i - IGP, e - EGP, ? - incomplete

Network            NextHop         MED        LocPrf     PrefVal Path/Ogn
* >  8.1.1.0/24         8.1.1.1         0                     32768       i
* >e 9.1.1.0/24         3.1.1.1         0                     0       65009i
* >e                    3.1.2.1         0                     0       65009i

The output shows that there are two valid routes to the destination 9.1.1.0/24, and both of them are the optimal routes.

By using the display ip routing-table command, you can find there are two routes to 9.1.1.0/24. One has next hop 3.1.1.1 and egress interface GigabitEthernet 1/0/2, and the other has next hop 3.1.2.1 and egress interface GigabitEthernet 1/0/3.
BGP community configuration example

Network requirements

As shown in Figure 71, Router B establishes EBGP connections to Router A and Router C. Configure NO_EXPORT community attribute on Router A so that AS 20 does not advertise routes received from AS 10 to any other AS.

Figure 71 Network diagram

Configuration procedure

1. Configure IP addresses for interfaces. (Details not shown.)
2. Configure EBGP connections:

   # Configure Router A.
   <RouterA> system-view
   [RouterA] bgp 10
   [RouterA-bgp-default] router-id 1.1.1.1
   [RouterA-bgp-default] peer 200.1.2.2 as-number 20
   [RouterA-bgp-default] address-family ipv4 unicast
   [RouterA-bgp-default-ipv4] peer 200.1.2.2 enable
   [RouterA-bgp-default-ipv4] network 9.1.1.0 255.255.255.0
   [RouterA-bgp-default-ipv4] quit
   [RouterA-bgp-default] quit

   # Configure Router B.
   <RouterB> system-view
   [RouterB] bgp 20
   [RouterB-bgp-default] router-id 2.2.2.2
   [RouterB-bgp-default] peer 200.1.2.1 as-number 10
   [RouterB-bgp-default] peer 200.1.3.2 as-number 30
   [RouterB-bgp-default] address-family ipv4 unicast
   [RouterB-bgp-default-ipv4] peer 200.1.2.1 enable
   [RouterB-bgp-default-ipv4] peer 200.1.3.2 enable
   [RouterB-bgp-default-ipv4] quit
   [RouterB-bgp-default] quit

   # Configure Router C.
   <RouterC> system-view
   [RouterC] bgp 30
   [RouterC-bgp-default] router-id 3.3.3.3
[RouterC-bgp-default] peer 200.1.3.1 as-number 20
[RouterC-bgp-default] address-family ipv4 unicast
[RouterC-bgp-default-ipv4] peer 200.1.3.1 enable
[RouterC-bgp-default-ipv4] quit
[RouterC-bgp-default] quit

# Display the BGP route 9.1.1.0 on Router B.
[RouterB] display bgp routing-table ipv4 9.1.1.0

BGP local router ID: 2.2.2.2
Local AS number: 20

Paths: 1 available, 1 best

BGP routing table information of 9.1.1.0/24:
From : 200.1.2.1 (1.1.1.1)
Rely nexthop : 200.1.2.1
Original nexthop: 200.1.2.1
OutLabel : NULL
AS-path : 10
Origin : igp
Attribute value : pref-val 0
State : valid, external, best
IP precedence : N/A
QoS local ID : N/A
Traffic index : N/A

# Display advertisement information for the route 9.1.1.0 on Router B.
[RouterB] display bgp routing-table ipv4 9.1.1.0 advertise-info

BGP local router ID: 2.2.2.2
Local AS number: 20

Paths: 1 best

BGP routing table information of 9.1.1.0/24:
Advertised to peers (1 in total):
  200.1.3.2

The output shows that Router B can advertise the route with the destination 9.1.1.0/24 to other ASs through BGP.

# Display the BGP routing table on Router C.
[RouterC] display bgp routing-table ipv4

Total number of routes: 1

BGP local router ID is 3.3.3.3
Status codes: * = valid, > = best, d = dampened, h = history,
  s = suppressed, S = stale, i = internal, e = external
Origin: i = IGP, e = EGP, ? = incomplete
Router C has learned the route to the destination 9.1.1.0/24 from Router B.

3. Configure BGP COMMUNITY attribute:
   # Configure a routing policy.
   [RouterA] route-policy comm_policy permit node 0
   [RouterA-route-policy-comm_policy-0] apply community no-export
   [RouterA-route-policy-comm_policy-0] quit
   # Apply the routing policy.
   [RouterA] bgp 10
   [RouterA-bgp-default] address-family ipv4 unicast
   [RouterA-bgp-default-ipv4] peer 200.1.2.2 route-policy comm_policy export
   [RouterA-bgp-default-ipv4] peer 200.1.2.2 advertise-community

Verifying the configuration
   # Display the BGP route 9.1.1.0 on Router B.
   [RouterB] display bgp routing-table ipv4 9.1.1.0

   BGP local router ID: 2.2.2.2
   Local AS number: 20

   Paths:  1 available, 1 best

   BGP routing table information of 9.1.1.0/24:
   From : 200.1.2.1 (1.1.1.1)
   Rely nexthop : 200.1.2.1
   Original nexthop: 200.1.2.1
   OutLabel : NULL
   Community : No-Export
   AS-path : 10
   Origin : igp
   Attribute value : pref-val 0
   State : valid, external, best
   IP precedence : N/A
   QoS local ID : N/A
   Traffic index : N/A

   # Display advertisement information for the route 9.1.1.0 on Router B.
   [RouterB] display bgp routing-table ipv4 9.1.1.0 advertise-info

   BGP local router ID: 2.2.2.2
   Local AS number: 20

   Paths:  1 best

   BGP routing table information of 9.1.1.0/24:
   Not advertised to any peers yet

   # Display the BGP routing table on Router C.
[RouterC] display bgp routing-table ipv4

Total number of routes: 0

The output shows that BGP has not learned any route.

BGP route reflector configuration example

Network requirements

As shown in Figure 72, all routers run BGP. Run EBGP between Router A and Router B, run IBGP between Router C and Router B, and between Router C and Router D.

Configure Router C as a route reflector with clients Router B and D to allow Router D to learn route 20.0.0.0/8 from Router C.

Figure 72 Network diagram

Configuration procedure

1. Configure IP addresses for interfaces and configure OSPF in AS 200. (Details not shown.)
2. Configure BGP connections:

# Configure Router A.
<RouterA> system-view
[RouterA] bgp 100
[RouterA-bgp-default] router-id 1.1.1.1
[RouterA-bgp-default] peer 192.1.1.2 as-number 200
[RouterA-bgp-default] address-family ipv4 unicast
[RouterA-bgp-default-ipv4] peer 192.1.1.2 enable
# Inject network 20.0.0.0/8 to the BGP routing table.
[RouterA-bgp-default-ipv4] network 20.0.0.0
[RouterA-bgp-default-ipv4] quit
[RouterA-bgp-default] quit

# Configure Router B.
<RouterB> system-view
[RouterB] bgp 200
[RouterB-bgp-default] router-id 2.2.2.2
[RouterB-bgp-default] peer 192.1.1.1 as-number 100
[RouterB-bgp-default] peer 193.1.1.1 as-number 200
[RouterB-bgp-default] address-family ipv4 unicast
[RouterB-bgp-default-ipv4] peer 192.1.1.1 enable
[RouterB-bgp-default-ipv4] peer 193.1.1.1 enable
[RouterB-bgp-default-ipv4] peer 193.1.1.1 next-hop-local
[RouterB-bgp-default-ipv4] quit
[RouterB-bgp-default] quit

# Configure Router C.
<RouterC> system-view
[RouterC] bgp 200
[RouterC-bgp-default] router-id 3.3.3.3
[RouterC-bgp-default] peer 193.1.1.2 as-number 200
[RouterC-bgp-default] peer 194.1.1.2 as-number 200
[RouterC-bgp-default] address-family ipv4 unicast
[RouterC-bgp-default-ipv4] peer 193.1.1.2 enable
[RouterC-bgp-default-ipv4] peer 194.1.1.2 enable
[RouterC-bgp-default-ipv4] quit
[RouterC-bgp-default] quit

# Configure Router D.
<RouterD> system-view
[RouterD] bgp 200
[RouterD-bgp-default] router-id 4.4.4.4
[RouterD-bgp-default] peer 194.1.1.1 as-number 200
[RouterD-bgp-default] address-family ipv4 unicast
[RouterD-bgp-default-ipv4] peer 194.1.1.1 enable
[RouterD-bgp-default-ipv4] quit
[RouterD-bgp-default] quit

3. Configure Router C as the route reflector.
[RouterC] bgp 200
[RouterC-bgp-default] address-family ipv4 unicast
[RouterC-bgp-default-ipv4] peer 193.1.1.2 reflect-client
[RouterC-bgp-default-ipv4] peer 194.1.1.2 reflect-client
[RouterC-bgp-default-ipv4] quit
[RouterC-bgp-default] quit

Verifying the configuration

# Display the BGP routing table on Router B.
[RouterB] display bgp routing-table ipv4

Total number of routes: 1

BGP local router ID is 2.2.2.2
Status codes: * - valid, > - best, d - dampened, h - history,
               s - suppressed, S - stale, i - internal, e - external
Origin: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>NextHop</th>
<th>MED</th>
<th>LocPrf</th>
<th>PrefVal</th>
<th>Path/Ogn</th>
</tr>
</thead>
<tbody>
<tr>
<td>* &gt;e 20.0.0.0</td>
<td>192.1.1.1</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td>i</td>
</tr>
</tbody>
</table>

# Display the BGP routing table on Router D.
[RouterD] display bgp routing-table ipv4
Total number of routes: 1

BGP local router ID is 4.4.4.4

Status codes: * - valid, > - best, d - dampened, h - history,
s - suppressed, S - stale, i - internal, e - external
Origin: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>NextHop</th>
<th>MED</th>
<th>LocPrf</th>
<th>PrefVal</th>
<th>Path/Ogn</th>
</tr>
</thead>
<tbody>
<tr>
<td>* &gt;1 20.0.0.0</td>
<td>193.1.1.2</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>100i</td>
</tr>
</tbody>
</table>

The output shows that Router D has learned the route 20.0.0.0/8 from Router C.

**BGP confederation configuration example**

**Network requirements**

As shown in Figure 73, split AS 200 into three sub-ASs (AS 65001, AS 65002, and AS 65003) to reduce IBGP connections. Routers in AS 65001 are fully meshed.

**Figure 73 Network diagram**

![Network Diagram]

**Table 15 Interface and IP address assignment**

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router A</td>
<td>GE1/0/1</td>
<td>10.1.2.1/24</td>
<td>Router D</td>
<td>GE1/0/1</td>
<td>10.1.5.1/24</td>
</tr>
<tr>
<td></td>
<td>GE1/0/2</td>
<td>10.1.3.1/24</td>
<td></td>
<td>GE1/0/2</td>
<td>10.1.3.2/24</td>
</tr>
<tr>
<td></td>
<td>GE1/0/3</td>
<td>10.1.4.1/24</td>
<td>Router E</td>
<td>GE1/0/1</td>
<td>10.1.5.2/24</td>
</tr>
<tr>
<td></td>
<td>GE1/0/4</td>
<td>200.1.1.1/24</td>
<td></td>
<td>GE1/0/2</td>
<td>10.1.4.2/24</td>
</tr>
<tr>
<td></td>
<td>GE1/0/5</td>
<td>10.1.1.1/24</td>
<td>Router F</td>
<td>GE1/0/1</td>
<td>9.1.1.1/24</td>
</tr>
<tr>
<td>Router B</td>
<td>GE1/0/1</td>
<td>10.1.1.2/24</td>
<td></td>
<td>GE1/0/2</td>
<td>200.1.1.2/24</td>
</tr>
<tr>
<td>Router C</td>
<td>GE1/0/1</td>
<td>10.1.2.2/24</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Configuration procedure**

1. Configure IP addresses for interfaces. (Details not shown.)
2. Configure the BGP confederation:

# Configure Router A.

<RouterA> system-view
[RouterA] bgp 65001
[RouterA-bgp-default] router-id 1.1.1.1
[RouterA-bgp-default] confederation id 200
[RouterA-bgp-default] confederation peer-as 65002 65003
[RouterA-bgp-default] peer 10.1.1.2 as-number 65002
[RouterA-bgp-default] peer 10.1.2.2 as-number 65003
[RouterA-bgp-default] address-family ipv4 unicast
[RouterA-bgp-default-ipv4] peer 10.1.1.2 enable
[RouterA-bgp-default-ipv4] peer 10.1.2.2 enable
[RouterA-bgp-default-ipv4] peer 10.1.1.2 next-hop-local
[RouterA-bgp-default-ipv4] peer 10.1.2.2 next-hop-local
[RouterA-bgp-default-ipv4] quit
[RouterA-bgp-default] quit

# Configure Router B.

<RouterB> system-view
[RouterB] bgp 65002
[RouterB-bgp-default] router-id 2.2.2.2
[RouterB-bgp-default] confederation id 200
[RouterB-bgp-default] confederation peer-as 65001 65003
[RouterB-bgp-default] peer 10.1.1.1 as-number 65001
[RouterB-bgp-default] address-family ipv4 unicast
[RouterB-bgp-default-ipv4] peer 10.1.1.1 enable
[RouterB-bgp-default-ipv4] quit
[RouterB-bgp-default] quit

# Configure Router C.

<RouterC> system-view
[RouterC] bgp 65003
[RouterC-bgp-default] router-id 3.3.3.3
[RouterC-bgp-default] confederation id 200
[RouterC-bgp-default] confederation peer-as 65001 65002
[RouterC-bgp-default] peer 10.1.2.1 as-number 65001
[RouterC-bgp-default] address-family ipv4 unicast
[RouterC-bgp-default-ipv4] peer 10.1.2.1 enable
[RouterC-bgp-default-ipv4] quit
[RouterC-bgp-default] quit

3. Configure IBGP connections in AS65001:

# Configure Router A.

[RouterA] bgp 65001
[RouterA-bgp-default] peer 10.1.3.2 as-number 65001
[RouterA-bgp-default] peer 10.1.4.2 as-number 65001
[RouterA-bgp-default] address-family ipv4 unicast
[RouterA-bgp-default-ipv4] peer 10.1.3.2 enable
[RouterA-bgp-default-ipv4] peer 10.1.4.2 enable
[RouterA-bgp-default-ipv4] peer 10.1.3.2 next-hop-local
[RouterA-bgp-default-ipv4] peer 10.1.4.2 next-hop-local
# Configure Router D.

<RouterD> system-view
[RouterD] bgp 65001
[RouterD-bgp-default] router-id 4.4.4.4
[RouterD-bgp-default] confederation id 200
[RouterD-bgp-default] peer 10.1.3.1 as-number 65001
[RouterD-bgp-default] peer 10.1.5.2 as-number 65001
[RouterD-bgp-default] address-family ipv4 unicast
[RouterD-bgp-default-ipv4] peer 10.1.3.1 enable
[RouterD-bgp-default-ipv4] peer 10.1.5.2 enable
[RouterD-bgp-default-ipv4] quit
[RouterD-bgp-default] quit

# Configure Router E.

<RouterE> system-view
[RouterE] bgp 65001
[RouterE-bgp-default] router-id 5.5.5.5
[RouterE-bgp-default] confederation id 200
[RouterE-bgp-default] peer 10.1.4.1 as-number 65001
[RouterE-bgp-default] peer 10.1.5.1 as-number 65001
[RouterE-bgp-default] address-family ipv4 unicast
[RouterE-bgp-default-ipv4] peer 10.1.4.1 enable
[RouterE-bgp-default-ipv4] peer 10.1.5.1 enable
[RouterE-bgp-default-ipv4] quit
[RouterE-bgp-default] quit

4. Configure the EBGP connection between AS 100 and AS 200:

# Configure Router A.

[RouterA] bgp 65001
[RouterA-bgp-default] peer 200.1.1.2 as-number 100
[RouterA-bgp-default] address-family ipv4 unicast
[RouterA-bgp-default-ipv4] peer 200.1.1.2 enable
[RouterA-bgp-default-ipv4] quit
[RouterA-bgp-default] quit

# Configure Router F.

<RouterF> system-view
[RouterF] bgp 100
[RouterF-bgp-default] router-id 6.6.6.6
[RouterF-bgp-default] peer 200.1.1.1 as-number 200
[RouterF-bgp-default] address-family ipv4 unicast
[RouterF-bgp-default-ipv4] peer 200.1.1.1 enable
[RouterF-bgp-default-ipv4] network 9.1.1.0 255.255.255.0
[RouterF-bgp-default-ipv4] quit
[RouterF-bgp-default] quit

Verifying the configuration

# Display the BGP routing table on Router B.

[RouterB] display bgp routing-table ipv4
Total number of routes: 1

BGP local router ID is 2.2.2.2

Status codes: * - valid, > - best, d - dampened, h - history,
s - suppressed, S - stale, i - internal, e - external
Origin: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>NextHop</th>
<th>MED</th>
<th>LocPrf</th>
<th>PrefVal</th>
<th>Path/Ogn</th>
</tr>
</thead>
<tbody>
<tr>
<td>* &gt;i 9.1.1.0/24</td>
<td>10.1.1.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>(65001)</td>
</tr>
</tbody>
</table>

[RouterB] display bgp routing-table ipv4 9.1.1.0

BGP local router ID: 2.2.2.2
Local AS number: 65002

Paths: 1 available, 1 best

BGP routing table information of 9.1.1.0/24:
From : 10.1.1.1 (1.1.1.1)
Rely nexthop : 10.1.1.1
Original nexthop: 10.1.1.1
OutLabel : NULL
AS-path : (65001) 100
Origin : igp
Attribute value : MED 0, localpref 100, pref-val 0, pre 255
State : valid, external-confed, best
IP precedence : N/A
QoS local ID : N/A
Traffic index : N/A

# Display the BGP routing table on Router D.

[RouterD] display bgp routing-table ipv4

Total number of routes: 1

BGP local router ID is 4.4.4.4

Status codes: * - valid, > - best, d - dampened, h - history,
s - suppressed, S - stale, i - internal, e - external
Origin: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>NextHop</th>
<th>MED</th>
<th>LocPrf</th>
<th>PrefVal</th>
<th>Path/Ogn</th>
</tr>
</thead>
<tbody>
<tr>
<td>* &gt;i 9.1.1.0/24</td>
<td>10.1.3.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1001</td>
</tr>
</tbody>
</table>

[RouterD] display bgp routing-table ipv4 9.1.1.0

BGP local router ID: 4.4.4.4
Local AS number: 65001
Paths: 1 available, 1 best

BGP routing table information of 9.1.1.0/24:
From: 10.1.3.1 (1.1.1.1)
Rely nexthop: 10.1.3.1
Original nexthop: 10.1.3.1
OutLabel: NULL
AS-path: 100
Origin: igp
Attribute value: MED 0, localpref 100, pref-val 0, pre 255
State: valid, internal-confed, best
IP precedence: N/A
QoS local ID: N/A
Traffic index: N/A

The output shows the following:
- Router F can send route information to Router B and Router C through the confederation by establishing only an EBGP connection with Router A.
- Router B and Router D are in the same confederation, but belong to different sub-ASs. They obtain external route information from Router A and generate identical BGP route entries although they have no direct connection in between.

BGP path selection configuration example

Network requirements

As shown in Figure 74, all routers run BGP.
- EBGP runs between Router A and Router B, and between Router A and Router C.
- IBGP runs between Router B and Router D, and between Router D and Router C. OSPF is the IGP protocol in AS 200.

Configure routing policies to make Router D give priority to the route 1.0.0.0/8 learned from Router C.

Figure 74 Network diagram

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router A</td>
<td>GE1/0/1</td>
<td>1.0.0.1/8</td>
<td>Router D</td>
<td>GE1/0/1</td>
<td>195.1.1.1/24</td>
</tr>
</tbody>
</table>
### Configuration procedure

1. **Configure IP addresses for interfaces.** (Details not shown.)

2. **Configure OSPF on Router B, Router C, and Router D:**

   **# Configure Router B.**
   ```
   <RouterB> system-view
   [RouterB] ospf
   [RouterB-ospf] area 0
   [RouterB-ospf-1-area-0.0.0.0] network 192.1.1.0 0.0.0.255
   [RouterB-ospf-1-area-0.0.0.0] network 194.1.1.0 0.0.0.255
   [RouterB-ospf-1-area-0.0.0.0] quit
   [RouterB-ospf-1] quit
   ```

   **# Configure Router C.**
   ```
   <RouterC> system-view
   [RouterC] ospf
   [RouterC-ospf] area 0
   [RouterC-ospf-1-area-0.0.0.0] network 193.1.1.0 0.0.0.255
   [RouterC-ospf-1-area-0.0.0.0] network 195.1.1.0 0.0.0.255
   [RouterC-ospf-1-area-0.0.0.0] quit
   [RouterC-ospf-1] quit
   ```

   **# Configure Router D.**
   ```
   <RouterD> system-view
   [RouterD] ospf
   [RouterD-ospf] area 0
   [RouterD-ospf-1-area-0.0.0.0] network 194.1.1.0 0.0.0.255
   [RouterD-ospf-1-area-0.0.0.0] network 195.1.1.0 0.0.0.255
   [RouterD-ospf-1-area-0.0.0.0] quit
   [RouterD-ospf-1] quit
   ```

3. **Configure BGP connections:**

   **# Configure Router A.**
   ```
   <RouterA> system-view
   [RouterA] bgp 100
   [RouterA-bgp-default] peer 192.1.1.2 as-number 200
   [RouterA-bgp-default] peer 193.1.1.2 as-number 200
   [RouterA-bgp-default] address-family ipv4 unicast
   [RouterA-bgp-default-ipv4] peer 192.1.1.2 enable
   [RouterA-bgp-default-ipv4] peer 193.1.1.2 enable
   # Inject network 1.0.0.0/8 into the BGP routing table of Router A.
   [RouterA-bgp-default-ipv4] network 1.0.0.0 8
   [RouterA-bgp-default-ipv4] quit
   [RouterA-bgp-default] quit
   ```
# Configure Router B.
[RouterB] bgp 200
[RouterB-bgp-default] peer 192.1.1.1 as-number 100
[RouterB-bgp-default] peer 194.1.1.1 as-number 200
[RouterB-bgp-default] address-family ipv4 unicast
[RouterB-bgp-default-ipv4] peer 192.1.1.1 enable
[RouterB-bgp-default-ipv4] peer 194.1.1.1 enable
[RouterB-bgp-default-ipv4] quit
[RouterB-bgp-default] quit

# Configure Router C.
[RouterC] bgp 200
[RouterC-bgp-default] peer 193.1.1.1 as-number 100
[RouterC-bgp-default] peer 195.1.1.1 as-number 200
[RouterC-bgp-default] address-family ipv4 unicast
[RouterC-bgp-default-ipv4] peer 193.1.1.1 enable
[RouterC-bgp-default-ipv4] peer 195.1.1.1 enable
[RouterC-bgp-default-ipv4] quit
[RouterC-bgp-default] quit

# Configure Router D.
[RouterD] bgp 200
[RouterD-bgp-default] peer 194.1.1.2 as-number 200
[RouterD-bgp-default] peer 195.1.1.2 as-number 200
[RouterD-bgp-default] address-family ipv4 unicast
[RouterD-bgp-default-ipv4] peer 194.1.1.2 enable
[RouterD-bgp-default-ipv4] peer 195.1.1.2 enable
[RouterD-bgp-default-ipv4] quit
[RouterD-bgp-default] quit

4. Configure local preference for the route 1.0.0.0/8 to make Router D give priority to the route learned from Router C:

# Define IPv4 basic ACL 2000 to permit the route 1.0.0.0/8 on Router C.
[RouterC] acl basic 2000
[RouterC-acl-ipv4-basic-2000] rule permit source 1.0.0.0 0.255.255.255
[RouterC-acl-ipv4-basic-2000] quit

# Define routing policy localpref on Router C to set the local preference of route 1.0.0.0/8 to 200 (the default is 100).
[RouterC] route-policy localpref permit node 10
[RouterC-route-policy-localpref-10] if-match ip address acl 2000
[RouterC-route-policy-localpref-10] apply local-preference 200
[RouterC-route-policy-localpref-10] quit

# Apply the routing policy localpref to the route from the peer 193.1.1.1 on Router C.
[RouterC] bgp 200
[RouterC-bgp-default] address-family ipv4 unicast
[RouterC-bgp-default-ipv4] peer 193.1.1.1 route-policy localpref import
[RouterC-bgp-default-ipv4] quit
[RouterC-bgp-default] quit

# Display the BGP routing table on Router D.
[RouterD] display bgp routing-table ipv4
Total number of routes: 2

BGP local router ID is 195.1.1.1

Status codes: * - valid, > - best, d - dampened, h - history, 
  s - suppressed, S - stale, i - internal, e - external 
  Origin: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>NextHop</th>
<th>MED</th>
<th>LocPrf</th>
<th>PrefVal</th>
<th>Path/Ogn</th>
</tr>
</thead>
<tbody>
<tr>
<td>* &gt; i 1.0.0.0</td>
<td>193.1.1.1</td>
<td>200</td>
<td>0</td>
<td>100</td>
<td>100i</td>
</tr>
<tr>
<td>*  i</td>
<td>192.1.1.1</td>
<td>100</td>
<td>0</td>
<td>100</td>
<td>100i</td>
</tr>
</tbody>
</table>

The route 1.0.0.0/8 learned from Router C is the optimal route.

BGP GR configuration example

Network requirements

As shown in Figure 75, run EBGP between Router A and Router B, and run IBGP between Router B and Router C.

Configure BGP GR so that the communication between Router A and Router C is not affected when an active/standby switchover occurs on Router B.

Figure 75 Network diagram

Configuration procedure

1. Configure Router A:
   # Configure IP addresses for interfaces. (Details not shown.)
   # Configure the EBGP connection.
   <RouterA> system-view
   [RouterA] bgp 65008
   [RouterA-bgp-default] router-id 1.1.1.1
   [RouterA-bgp-default] peer 200.1.1.1 as-number 65009
   # Enable GR capability for BGP.
   [RouterA-bgp-default] graceful-restart
   # Inject network 8.0.0.0/8 to the IPv4 BGP routing table.
   [RouterA-bgp-default] address-family ipv4
   [RouterA-bgp-default-ipv4] network 8.0.0.0
   # Enable Router A to exchange IPv4 unicast routing information with Router B.
   [RouterA-bgp-default-ipv4] peer 200.1.1.1 enable

2. Configure Router B:
   # Configure IP addresses for interfaces. (Details not shown.)
# Configure the EBGP connection.
<RouterB> system-view
[RouterB] bgp 65009
[RouterB-bgp-default] router-id 2.2.2.2
[RouterB-bgp-default] peer 200.1.1.2 as-number 65008
# Configure the IBGP connection.
[RouterB-bgp-default] peer 9.1.1.2 as-number 65009
# Enable GR capability for BGP.
[RouterB-bgp-default] graceful-restart
# Inject networks 200.1.1.0/24 and 9.1.1.0/24 to the IPv4 BGP routing table.
[RouterB-bgp-default-ipv4] network 200.1.1.0 24
[RouterB-bgp-default-ipv4] network 9.1.1.0 24
# Enable Router B to exchange IPv4 unicast routing information with Router A and Router C.
[RouterB-bgp-default-ipv4] peer 200.1.1.2 enable
[RouterB-bgp-default-ipv4] peer 9.1.1.2 enable

3. Configure Router C:
   # Configure IP addresses for interfaces. (Details not shown.)
   # Configure the IBGP connection.
<RouterC> system-view
[RouterC] bgp 65009
[RouterC-bgp-default] router-id 3.3.3.3
[RouterC-bgp-default] peer 9.1.1.1 as-number 65009
# Enable GR capability for BGP.
[RouterC-bgp-default] graceful-restart
# Enable Router C to exchange IPv4 unicast routing information with Router B.
[RouterC-bgp-default-ipv4] address-family ipv4
[RouterC-bgp-default-ipv4] peer 9.1.1.1 enable

Verifying the configuration
Ping Router C on Router A. Meanwhile, perform an active/standby switchover on Router B. The ping operation is successful during the whole switchover process. (Details not shown.)

BFD for BGP configuration example

Network requirements
As shown in Figure 76, configure OSPF as the IGP in AS 200.
- Establish two IBGP connections between Router A and Router C. When both paths operate correctly, Router C uses the path Router A<---Router B<---Router C to communicate with network 1.1.1.0/24.
- Configure BFD over the path. When the path fails, BFD can quickly detect the failure and notify it to BGP. Then, the path Router A<---Router D<---Router C takes effect immediately.
Configuration procedure

1. Configure IP addresses for interfaces. (Details not shown.)
2. Configure OSPF so that Router A and Router C can reach each other. (Details not shown.)
3. Configure BGP on Router A:
   
   # Establish two IBGP connections to Router C.
   
   ```
   <RouterA> system-view
   [RouterA] bgp 200
   [RouterA-bgp-default] peer 3.0.2.2 as-number 200
   [RouterA-bgp-default] peer 2.0.2.2 as-number 200
   [RouterA-bgp-default] address-family ipv4 unicast
   [RouterA-bgp-default-ipv4] peer 3.0.2.2 enable
   [RouterA-bgp-default-ipv4] peer 2.0.2.2 enable
   [RouterA-bgp-default-ipv4] quit
   # Create IPv4 basic ACL 2000 to permit 1.1.1.0/24 to pass.
   [RouterA] acl basic 2000
   [RouterA-acl-ipv4-basic-2000] rule permit source 1.1.1.0 0.0.0.255
   [RouterA-acl-ipv4-basic-2000] quit
   # Create two routing policies to set the MED for route 1.1.1.0/24. The policy apply_med_50 sets the MED to 50, and the policy apply_med_100 sets the MED to 100.
   [RouterA] route-policy apply_med_50 permit node 10
   [RouterA-route-policy-apply_med_50-10] if-match ip address acl 2000
   [RouterA-route-policy-apply_med_50-10] apply cost 50
   [RouterA-route-policy-apply_med_50-10] quit
   [RouterA] route-policy apply_med_100 permit node 10
   [RouterA-route-policy-apply_med_100-10] if-match ip address acl 2000
   [RouterA-route-policy-apply_med_100-10] apply cost 100
   [RouterA-route-policy-apply_med_100-10] quit
   # Apply routing policy apply_med_50 to routes outgoing to peer 3.0.2.2, and apply routing policy apply_med_100 to routes outgoing to peer 2.0.2.2.
   [RouterA] bgp 200
   [RouterA-bgp-default] address-family ipv4 unicast
   [RouterA-bgp-default-ipv4] peer 3.0.2.2 route-policy apply_med_50 export
   [RouterA-bgp-default-ipv4] peer 2.0.2.2 route-policy apply_med_100 export
   ```
4. Configure BGP on Router C:

# Establish two IBGP connections to Router A.

<RouterC> system-view
[RouterC] bgp 200
[RouterC-bgp-default] peer 3.0.1.1 as-number 200
[RouterC-bgp-default] peer 2.0.1.1 as-number 200
[RouterC-bgp-default] address-family ipv4 unicast
[RouterC-bgp-default-ipv4] peer 3.0.1.1 enable
[RouterC-bgp-default-ipv4] peer 2.0.1.1 enable
[RouterC-bgp-default-ipv4] quit

# Enable BFD for peer 3.0.1.1.
[RouterC-bgp-default] peer 3.0.1.1 bfd
[RouterC-bgp-default] quit

[RouterC] quit

Verifying the configuration

# Display detailed BFD session information on Router C.

<RouterC> display bfd session verbose
Total Session Num: 1           Up Session Num: 1     Init Mode: Active

IPv4 Session Working Under Ctrl Mode:
  Local Discr: 513               Remote Discr: 513
  Source IP: 3.0.2.2             Destination IP: 3.0.1.1
  Session State: Up              Interface: N/A
  Min Tx Inter: 500ms            Act Tx Inter: 500ms
  Min Rx Inter: 500ms            Detect Inter: 2500ms
  Rx Count: 135                  Tx Count: 135
  Connect Type: Indirect         Running Up for: 00:00:58
  Hold Time: 2457ms              Auth mode: None
  Detect Mode: Async             Slot: 0
  Protocol: BGP
  Version:1
  Diag Info: No Diagnostic

The output shows that a BFD session has been established between Router A and Router C.

# Display BGP peer information on Router C.

<RouterC> display bgp peer ipv4

BGP local router ID: 3.3.3.3
Local AS number: 200
Total number of peers: 2  Peers in established state: 2

* - Dynamically created peer
Peer  AS  MsgRcvd  MsgSent OutQ PrefRcvd Up/Down  State

336
The output shows that Router C has established two BGP connections with Router A, and both connections are in Established state.

# Display route 1.1.1.0/24 on Router C.
<RouterC> display ip routing-table 1.1.1.0 24 verbose

Summary count : 1

Destination: 1.1.1.0/24
  Protocol: BGP            Process ID: 0
  SubProtID: 0x1          Age: 00h03m08s
  Cost: 100            Preference: 255
  IpPre: N/A         QosLocalID: N/A
  Tag: 0              State: Active Adv
  OrigTblID: 0x1         OrigVrf: default-vrf
  TableID: 0x2         OrigAs: 0
  NibID: 0x15000000     LastAs: 0
  AttrID: 0x0           Neighbor: 2.0.1.1
  Flags: 0x10060       OrigNextHop: 2.0.1.1
  Label: NULL         RealNextHop: 2.0.2.1
  BkLabel: NULL       BkNextHop: N/A
  Tunnel ID: Invalid       Interface: GigabitEthernet1/0/2
  BkTunnel ID: Invalid   BkInterface: N/A
  FtnIndex: 0x0      TrafficIndex: N/A
  Connector: N/A

The output shows that Router C communicates with network 1.1.1.0/24 through the path Router C<---Router B<---Router A.

# Break down the link Router C<---Router B<---Router A and then display route 1.1.1.0/24 on Router C.
<RouterC> display ip routing-table 1.1.1.0 24 verbose

Summary count : 1

Destination: 1.1.1.0/24
  Protocol: BGP            Process ID: 0
  SubProtID: 0x1          Age: 00h00m09s
  Cost: 50             Preference: 255
  IpPre: N/A         QosLocalID: N/A
  Tag: 0              State: Active Adv
  OrigTblID: 0x1         OrigVrf: default-vrf
  TableID: 0x2         OrigAs: 0
  NibID: 0x15000001     LastAs: 0
  AttrID: 0x1           Neighbor: 3.0.1.1
  Flags: 0x10060       OrigNextHop: 3.0.1.1
  Label: NULL         RealNextHop: 3.0.2.1
  BkLabel: NULL       BkNextHop: N/A
  Tunnel ID: Invalid       Interface: GigabitEthernet1/0/1
  BkTunnel ID: Invalid   BkInterface: N/A
  FtnIndex: 0x0      TrafficIndex: N/A
  Connector: N/A
BGP FRR configuration example

Network requirements

As shown in Figure 77, configure BGP FRR so that when Link B fails, BGP uses Link A to forward traffic.

Figure 77 Network diagram

Configuration procedure

1. Configure IP addresses for interfaces. (Details not shown.)
2. Configure OSPF in AS 200 to ensure connectivity among Router B, Router C, and Router D. (Details not shown.)
3. Configure BGP connections:
   
   # Configure Router A to establish EBGP sessions to Router B and Router C, and advertise network 1.1.1.1/32.
   <RouterA> system-view
   [RouterA] bgp 100
   [RouterA-bgp-default] router-id 1.1.1.1
   [RouterA-bgp-default] peer 10.1.1.2 as-number 200
   [RouterA-bgp-default] peer 30.1.1.3 as-number 200
   [RouterA-bgp-default] address-family ipv4 unicast
   [RouterA-bgp-default-ipv4] peer 10.1.1.2 enable
   [RouterA-bgp-default-ipv4] peer 30.1.1.3 enable
   [RouterA-bgp-default-ipv4] network 1.1.1.1/32
   
   # Configure Router B to establish an EBGP session to Router A, and an IBGP session to Router D.
   <RouterB> system-view
   [RouterB] bgp 200
# Configure Router B to establish an EBGP session to Router A, and an IBGP session to Router D.

```
[RouterB-bgp-default] router-id 2.2.2.2
[RouterB-bgp-default] peer 10.1.1.1 as-number 100
[RouterB-bgp-default] peer 4.4.4.4 as-number 200
[RouterB-bgp-default] peer 4.4.4.4 connect-interface loopback 0
[RouterB-bgp-default] address-family ipv4 unicast
[RouterB-bgp-default-ipv4] peer 10.1.1.1 enable
[RouterB-bgp-default-ipv4] peer 4.4.4.4 enable
[RouterB-bgp-default-ipv4] peer 4.4.4.4 next-hop-local
[RouterB-bgp-default-ipv4] quit
[RouterB-bgp-default] quit
```

# Configure Router C to establish an EBGP session to Router A, and an IBGP session to Router D.

```
<RouterC> system-view
[RouterC] bgp 200
[RouterC-bgp-default] router-id 3.3.3.3
[RouterC-bgp-default] peer 30.1.1.1 as-number 100
[RouterC-bgp-default] peer 4.4.4.4 as-number 200
[RouterC-bgp-default] peer 4.4.4.4 connect-interface loopback 0
[RouterC-bgp-default] address-family ipv4 unicast
[RouterC-bgp-default-ipv4] peer 30.1.1.1 enable
[RouterC-bgp-default-ipv4] peer 4.4.4.4 enable
[RouterC-bgp-default-ipv4] peer 4.4.4.4 next-hop-local
[RouterC-bgp-default-ipv4] quit
[RouterC-bgp-default] quit
```

# Configure Router D to establish IBGP sessions to Router B and Router C, and advertise network 4.4.4.4/32.

```
<RouterD> system-view
[RouterD] bgp 200
[RouterD-bgp-default] router-id 4.4.4.4
[RouterD-bgp-default] peer 2.2.2.2 as-number 200
[RouterD-bgp-default] peer 2.2.2.2 connect-interface loopback 0
[RouterD-bgp-default] peer 3.3.3.3 as-number 200
[RouterD-bgp-default] peer 3.3.3.3 connect-interface loopback 0
[RouterD-bgp-default] address-family ipv4 unicast
[RouterD-bgp-default-ipv4] peer 2.2.2.2 enable
[RouterD-bgp-default-ipv4] peer 3.3.3.3 enable
[RouterD-bgp-default-ipv4] network 4.4.4.4 32
```

4. Configure preferred values so Link B is used to forward traffic between Router A and Router D:

# Configure Router A to set the preferred value to 100 for routes received from Router B.

```
[RouterA-bgp-default-ipv4] peer 10.1.1.2 preferred-value 100
[RouterA-bgp-default-ipv4] quit
[RouterA-bgp-default] quit
```

# Configure Router D to set the preferred value to 100 for routes received from Router B.

```
[RouterD-bgp-default-ipv4] peer 2.2.2.2 preferred-value 100
[RouterD-bgp-default-ipv4] quit
[RouterD-bgp-default] quit
```

5. Configure BGP FRR:

# On Router A, configure the source address of BFD echo packets as 11.1.1.1.
[RouterA] bfd echo-source-ip 11.1.1.1
# Create routing policy frr to set a backup next hop 30.1.1.3 (Router C) for the route destined for 4.4.4.4/32.
[RouterA] ip prefix-list abc index 10 permit 4.4.4.4 32
[RouterA] route-policy frr permit node 10
[RouterA-route-policy] if-match ip address prefix-list abc
[RouterA-route-policy] apply fast-reroute backup-nexthop 30.1.1.3
[RouterA-route-policy] quit
# Use echo-mode BFD to detect the connectivity to Router D.
[RouterA] bgp 100
[RouterA-bgp-default] primary-path-detect bfd echo
# Apply the routing policy to BGP FRR for BGP IPv4 unicast address family.
[RouterA-bgp-default] address-family ipv4 unicast
[RouterA-bgp-default-ipv4] quit
[RouterA-bgp-default] quit
# On Router D, set the source address of BFD echo packets to 44.1.1.1.
[RouterD] bfd echo-source-ip 44.1.1.1
# Create routing policy frr to set a backup next hop 3.3.3.3 (Router C) for the route destined for 1.1.1.1/32.
[RouterD] ip prefix-list abc index 10 permit 1.1.1.1 32
[RouterD] route-policy frr permit node 10
[RouterD-route-policy] if-match ip address prefix-list abc
[RouterD-route-policy] apply fast-reroute backup-nexthop 3.3.3.3
[RouterD-route-policy] quit
# Use echo-mode BFD to detect the connectivity to Router A.
[RouterD] bgp 200
[RouterD-bgp-default] primary-path-detect bfd echo
# Apply the routing policy to BGP FRR for BGP IPv4 unicast address family.
[RouterD-bgp-default] address-family ipv4 unicast
[RouterD-bgp-default-ipv4] quit
[RouterD-bgp-default] quit

Verifying the configuration
# Display detailed information about the route to 4.4.4.4/32 on Router A. The output shows the backup next hop for the route.
[RouterA] display ip routing-table 4.4.4.4 32 verbose

Summary count : 1

Destination: 4.4.4.4/32
  Protocol: BGP                Process ID: 0
  SubProtID: 0x0               Age: 00h01m52s
  Cost: 0                     Preference: 255
  IpPre: N/A                   QosLocalID: N/A
  Tag: 0                      State: Active Adv
  OrigTblID: 0x0               OrigVrf: default-vrf
  TableID: 0x2                 OrigAs: 200
# Display detailed information about the route to 1.1.1.1/32 on Router D. The output shows the backup next hop for the route.

[RouterD] display ip routing-table 1.1.1.1 32 verbose

Summary count : 1

Destination: 1.1.1.1/32
  Protocol: BGP  Process ID: 0
  SubProtID: 0x1  Age: 00h00m36s
  Cost: 0  Preference: 255
  IpPre: N/A  QosLocalID: N/A
  Tag: 0  State: Active Adv
  OrigTblID: 0x0  OrigVrf: default-vrf
  TableID: 0x2  OrigAs: 100
  NibID: 0x15000003  LastAs: 100
  AttrID: 0x1  Neighbor: 2.2.2.2
  Flags: 0x10060  OrigNextHop: 2.2.2.2
  Label: NULL  RealNextHop: 20.1.1.2
  BkLabel: NULL  BkNextHop: 40.1.1.3
  Tunnel ID: Invalid  Interface: GigabitEthernet1/0/1
  BkTunnel ID: Invalid  BKInterface: GigabitEthernet1/0/2
  FtnIndex: 0x0  TrafficIndex: N/A
  Connector: N/A

Multicast BGP configuration example

Network requirements

As shown in Figure 78, OSPF runs within AS 100 and AS 200 to ensure intra-AS connectivity. MBGP runs between the two ASs to exchange IPv4 unicast routes used for RPF check.

- Configure the Loopback 0 interface of Router A and Router B as the C-BSR and C-RP.
- Configure Router A and Router B to establish a Multicast Source Discovery Protocol (MSDP) peer relationship through MBGP, so that the receiver can receive multicast traffic from the source.
### Table 17 Interface and IP address assignment

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>N/A</td>
<td>10.110.1.100/24</td>
<td>Router C</td>
<td>GE1/0/1</td>
<td>10.110.2.1/24</td>
</tr>
<tr>
<td>Router A</td>
<td>GE1/0/1</td>
<td>10.110.1.1/24</td>
<td>Router A</td>
<td>GE1/0/2</td>
<td>192.168.2.1/24</td>
</tr>
<tr>
<td></td>
<td>GE1/0/2</td>
<td>192.168.1.1/24</td>
<td></td>
<td>GE1/0/3</td>
<td>192.168.4.2/24</td>
</tr>
<tr>
<td></td>
<td>Loop0</td>
<td>1.1.1.1/32</td>
<td></td>
<td>Loop0</td>
<td>3.3.3.3/32</td>
</tr>
<tr>
<td>Router B</td>
<td>GE1/0/1</td>
<td>192.168.1.2/24</td>
<td>Router B</td>
<td>GE1/0/1</td>
<td>192.168.3.2/24</td>
</tr>
<tr>
<td></td>
<td>GE1/0/2</td>
<td>192.168.3.1/24</td>
<td>Router C</td>
<td>GE1/0/2</td>
<td>192.168.4.2/24</td>
</tr>
<tr>
<td></td>
<td>GE1/0/3</td>
<td>192.168.2.1/24</td>
<td></td>
<td>Loop0</td>
<td>4.4.4.4/32</td>
</tr>
<tr>
<td></td>
<td>Loop0</td>
<td>2.2.2.2/32</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Configuration procedure

1. Configure IP addresses for interfaces and configure OSPF (this example uses OSPF process 1) in AS 200 to ensure intra-AS connectivity. (Details not shown.)

2. Enable IP multicast routing, PIM-SM, and IGMP, and configure BSR boundaries:
   
   # On Router A, enable multicast routing globally, and enable PIM-SM on interfaces.
   ```
   <RouterA> system-view
   [RouterA] multicast routing
   [RouterA-mrib] quit
   [RouterA] interface gigabitethernet 1/0/1
   [RouterA-GigabitEthernet1/0/1] pim sm
   [RouterA-GigabitEthernet1/0/1] quit
   [RouterA] interface gigabitethernet 1/0/2
   [RouterA-GigabitEthernet1/0/2] pim sm
   [RouterA-GigabitEthernet1/0/2] quit
   
   # Configure Router B and Router D in the same way that Router A was configured.
   
   # On Router C, enable multicast routing globally.
   ```
3. Configure Loopback 0, C-BSR, and C-RP:
   # Configure the Loopback 0 interface and specify it as the C-BSR and C-RP on Router A.
   [RouterA] interface loopback 0
   [RouterA-LoopBack0] ip address 1.1.1.1 32
   [RouterA-LoopBack0] pim sm
   [RouterA-LoopBack0] quit
   [RouterA] pim
   [RouterA-pim] c-bsr 1.1.1.1
   [RouterA-pim] c-rp 1.1.1.1
   [RouterA-pim] quit
   
   # Configure the Loopback 0 interface and specify it as the C-BSR and C-RP on Router B.
   [RouterB] interface loopback 0
   [RouterB-LoopBack0] ip address 2.2.2.2 32
   [RouterB-LoopBack0] pim sm
   [RouterB-LoopBack0] quit
   [RouterB] pim
   [RouterB-pim] c-bsr 2.2.2.2
   [RouterB-pim] c-rp 2.2.2.2
   [RouterB-pim] quit

4. Configure BGP to establish BGP IPv4 multicast peers and redistribute routes:
   # On Router A, establish an EBGP session to Router B.
   [RouterA] bgp 100
   [RouterA-bgp-default] router-id 1.1.1.1
   [RouterA-bgp-default] peer 192.168.1.2 as-number 200
   
   # Enable exchange of IPv4 unicast routes used for RPF check with Router B.
   [RouterA-bgp-default] address-family ipv4 unicast

# Redistribute direct routes into BGP.
[RouterA-bgp-default] quit

# On Router B, establish an EBGP session to Router A.
[RouterB] bgp 200
[RouterB-bgp-default] router-id 2.2.2.2
[RouterB-bgp-default] peer 192.168.1.1 as-number 100

# Enable exchange of IPv4 unicast routes used for RPF check with Router B.
[RouterB-bgp-default] address-family ipv4 multicast
[RouterB-bgp-default-mul-ipv4] peer 192.168.1.1 enable

# Redistribute OSPF routes into BGP.
[RouterB-bgp-default-mul-ipv4] import-route ospf 1
[RouterB-bgp-default-mul-ipv4] quit
[RouterB-bgp-default] quit

5. Configure MSDP peers:

# Configure an MSDP peer on Router A.
[RouterA] msdp
[RouterA-msdp] peer 192.168.1.2 connect-interface gigabitethernet 1/0/2
[RouterA-msdp] quit

# Configure an MSDP peer on Router B.
[RouterB] msdp
[RouterB-msdp] peer 192.168.1.1 connect-interface gigabitethernet 1/0/1
[RouterB-msdp] quit

Verifying the configuration

# Verify the BGP IPv4 multicast peer information on Router B.
[RouterB] display bgp peer ipv4 multicast

BGP local router ID : 2.2.2.2
Local AS number : 200
Total number of peers : 1    Peers in established state : 1

Peer            AS  MsgRcvd  MsgSent  OutQ PrefRcv Up/Down  State
192.168.1.1    100       56       56     0       0 00:40:54 Established

# Verify the MSDP peer information on Router B.
[RouterB] display msdp brief

Configured  Established  Listen  Connect  Shutdown  Disabled
1            1            0        0        0        0

Peer address  State  Up/Down time  AS  SA count  Reset count
192.168.1.1   Up      00:07:17    100    1         0
Dynamic BGP peer configuration example

Network requirements

As shown in Figure 79, Router A needs to establish IBGP peer relationships with Router B, Router C, and Router D in network 10.1.0.0/16. Configure dynamic BGP peers to simplify the configuration.

Configure Router A as the route reflector, and configure Router B, Router C, and Router D as its clients.

Figure 79 Network diagram

Configuration procedure

1. Configure IP addresses for interfaces. (Details not shown.)
2. Configure IBGP peer relationships:

   # Configure Router A to establish dynamic BGP peer relationships with routers in network 10.1.0.0/16.
   <RouterA> system-view
   [RouterA] bgp 200
   [RouterA-bgp-default] router-id 1.1.1.1
   [RouterA-bgp-default] peer 10.1.0.0 16 as-number 200
   [RouterA-bgp-default] address-family ipv4
   [RouterA-bgp-default-ipv4] peer 10.1.0.0 16 enable

   # Configure Router B to establish an IBGP peer relationship with Router A.
   <RouterB> system-view
   [RouterB] bgp 200
   [RouterB-bgp-default] router-id 2.2.2.2
   [RouterB-bgp-default] peer 10.1.1.1 as-number 200
   [RouterB-bgp-default] address-family ipv4
   [RouterB-bgp-default-ipv4] peer 10.1.0.0 16 enable

   # Configure Router C to establish an IBGP peer relationship with Router A.
   <RouterC> system-view
   [RouterC] bgp 200
   [RouterC-bgp-default] router-id 3.3.3.3
# Configure Router D to establish an IBGP peer relationship with Router A.

<RouterD> system-view
[RouterD] bgp 200
[RouterD-bgp-default] router-id 4.4.4.4
[RouterD-bgp-default] peer 10.1.3.1 as-number 200
[RouterD-bgp-default] address-family ipv4
[RouterD-bgp-default-ipv4] peer 10.1.3.1 enable

# Display BGP peer information on Router A. The output shows that Router A has established IBGP peer relationships with Router B, Router C, and Router D.

[RouterA] display bgp peer ipv4

BGP local router ID : 1.1.1.1
Local AS number : 200

Total number of peers : 3 Peers in established state : 3

* - Dynamically created peer
Peer AS MsgRcvd MsgSent OutQ PrefRcv Up/Down State
*10.1.1.2 200 7 10 0 0 00:06:09 Established
*10.1.2.2 200 7 10 0 0 00:06:09 Established
*10.1.3.2 200 7 10 0 0 00:06:09 Established

3. Configure Router A as the route reflector, and configure peers in network 10.1.0.0/16 as its clients.

[RouterA-bgp-default-ipv4] peer 10.1.0.0 16 reflect-client

4. Configure Router C to advertise network 9.1.1.0/24.

[RouterC-bgp-default-ipv4] network 9.1.1.0 24

Verifying the configuration

# Verify that route 9.1.1.0/24 exists in the BGP routing table on Router A, Router B, Router D. This example uses Router A.

[RouterA-bgp-default] display bgp routing-table ipv4

Total Number of Routes: 1

BGP Local router ID is 1.1.1.1
Status codes: * - valid, > - best, d - dampened, h - history,
 s - suppressed, S - stale, i - internal, e - external
Origin: i - IGP, e - EGP, ? - incomplete

Network NextHop MED LocPrf PrefVal Path/Ogn
* i 9.1.1.0/24 10.1.2.2 0 100 0 ?
IPv6 BGP configuration examples

IPv6 BGP basic configuration example

Network requirements

As shown in Figure 80, all routers run BGP. Run EBGP between Router A and Router B, and run IBGP between Router B and Router C to allow Router C to access network 50::/64 connected to Router A.

Figure 80 Network diagram

Configuration procedure

1. Configure IP addresses for interfaces. (Details not shown.)
2. Configure IBGP:
   
   # Configure Router B.
   <RouterB> system-view
   [RouterB] bgp 65009
   [RouterB-bgp-default] router-id 2.2.2.2
   [RouterB-bgp-default] peer 9::2 as-number 65009
   [RouterB-bgp-default] address-family ipv6
   [RouterB-bgp-default-ipv6] peer 9::2 enable
   [RouterB-bgp-default-ipv6] quit

   # Configure Router C.
   <RouterC> system-view
   [RouterC] bgp 65009
   [RouterC-bgp-default] router-id 3.3.3.3
   [RouterC-bgp-default] peer 9::1 as-number 65009
   [RouterC-bgp-default] address-family ipv6
   [RouterC-bgp-default-ipv6] peer 9::1 enable

3. Configure EBGP:
   
   # Configure Router A.
   <RouterA> system-view
   [RouterA] bgp 65008
   [RouterA-bgp-default] router-id 1.1.1.1
   [RouterA-bgp-default] peer 10::1 as-number 65009
   [RouterA-bgp-default] address-family ipv6
   [RouterA-bgp-default-ipv6] peer 10::1 enable

   # Configure Router B.
   [RouterB-bgp-default] peer 10::2 as-number 65008
   [RouterB-bgp-default] address-family ipv6
4. Inject network routes to the BGP routing table:

   # Configure Router A.
   [RouterA-bgp-default-ipv6] network 10::64
   [RouterA-bgp-default-ipv6] network 50::64
   [RouterA-bgp-default-ipv6] quit
   [RouterA-bgp-default] quit

   # Configure Router B.
   [RouterB-bgp-default-ipv6] network 10::64
   [RouterB-bgp-default-ipv6] network 9::64
   [RouterB-bgp-default-ipv6] quit
   [RouterB-bgp-default] quit

   # Configure Router C.
   [RouterC-bgp-default-ipv6] network 9::64
   [RouterC-bgp-default-ipv6] quit
   [RouterC-bgp-default] quit

Verifying the configuration

   # Display IPv6 BGP peer information on Router B.
   [RouterB] display bgp peer ipv6

   BGP local router ID: 2.2.2.2
   Local AS number: 65009
   Total number of peers: 2                  Peers in established state: 2

   * - Dynamically created peer
   Peer                    AS  MsgRcvd  MsgSent OutQ  PrefRcvd Up/Down  State
   9::2                 65009       41       43    0       1 00:29:00 Established
   10::2                65008       38       38    0       2 00:27:20 Established

   The output shows that Router A and Router B have established an EBGP connection, and Router B and Router C have established an IBGP connection.

   # Display IPv6 BGP routing table information on Router A.
   [RouterA] display bgp routing-table ipv6

   Total number of routes: 4

   BGP local router ID is 1.1.1.1
   Status codes: * - valid, > - best, d - dampened, h - history,
   s - suppressed, S - stale, i - internal, e - external
   Origin: i - IGP, e - EGP, ? - incomplete

   * >e Network : 9::   PrefixLen : 64
     NextHop : 10::1  LocPrf  :
     PrefVal : 0  OutLabel : NULL
     MED     : 0
     Path/Ogn: 65009
<table>
<thead>
<tr>
<th>* &gt; Network</th>
<th>10::</th>
<th>PrefixLen</th>
<th>64</th>
</tr>
</thead>
<tbody>
<tr>
<td>NextHop</td>
<td>::</td>
<td>LocPrf</td>
<td></td>
</tr>
<tr>
<td>PrefVal</td>
<td>32768</td>
<td>OutLabel</td>
<td>NULL</td>
</tr>
<tr>
<td>MED</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Path/Ogn</td>
<td>i</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>* e Network</th>
<th>10::</th>
<th>PrefixLen</th>
<th>64</th>
</tr>
</thead>
<tbody>
<tr>
<td>NextHop</td>
<td>10::1</td>
<td>LocPrf</td>
<td></td>
</tr>
<tr>
<td>PrefVal</td>
<td>0</td>
<td>OutLabel</td>
<td>NULL</td>
</tr>
<tr>
<td>MED</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Path/Ogn</td>
<td>65009i</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>* &gt; Network</th>
<th>50::</th>
<th>PrefixLen</th>
<th>64</th>
</tr>
</thead>
<tbody>
<tr>
<td>NextHop</td>
<td>::</td>
<td>LocPrf</td>
<td></td>
</tr>
<tr>
<td>PrefVal</td>
<td>32768</td>
<td>OutLabel</td>
<td>NULL</td>
</tr>
<tr>
<td>MED</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Path/Ogn</td>
<td>i</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The output shows that Router A has learned routing information of AS 65009.

**# Display IPv6 BGP routing table information on Router C.**

```
[RouterC] display bgp routing-table ipv6
```

Total number of routes: 4

BGP local router ID is 3.3.3.3

Status codes: * - valid, > - best, d - dampened, h - history,
  s - suppressed, S - stale, i - internal, e - external
  Origin: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>* &gt; Network</th>
<th>9::</th>
<th>PrefixLen</th>
<th>64</th>
</tr>
</thead>
<tbody>
<tr>
<td>NextHop</td>
<td>::</td>
<td>LocPrf</td>
<td></td>
</tr>
<tr>
<td>PrefVal</td>
<td>32768</td>
<td>OutLabel</td>
<td>NULL</td>
</tr>
<tr>
<td>MED</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Path/Ogn</td>
<td>i</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>* i Network</th>
<th>9::</th>
<th>PrefixLen</th>
<th>64</th>
</tr>
</thead>
<tbody>
<tr>
<td>NextHop</td>
<td>9::1</td>
<td>LocPrf</td>
<td>100</td>
</tr>
<tr>
<td>PrefVal</td>
<td>0</td>
<td>OutLabel</td>
<td>NULL</td>
</tr>
<tr>
<td>MED</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Path/Ogn</td>
<td>i</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>* &gt;i Network</th>
<th>10::</th>
<th>PrefixLen</th>
<th>64</th>
</tr>
</thead>
<tbody>
<tr>
<td>NextHop</td>
<td>9::1</td>
<td>LocPrf</td>
<td>100</td>
</tr>
<tr>
<td>PrefVal</td>
<td>0</td>
<td>OutLabel</td>
<td>NULL</td>
</tr>
<tr>
<td>MED</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Path/Ogn</td>
<td>i</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>* &gt;i Network</th>
<th>50::</th>
<th>PrefixLen</th>
<th>64</th>
</tr>
</thead>
<tbody>
<tr>
<td>NextHop</td>
<td>10::2</td>
<td>LocPrf</td>
<td>100</td>
</tr>
</tbody>
</table>

349
The output shows that Router C has learned the route 50::/64.

# Verify that Router C can ping hosts on network 50::/64. (Details not shown.)

**IPv6 BGP route reflector configuration example**

**Network requirements**

As shown in Figure 81, run EBGP between Router A and Router B, and run IBGP between Router C and Router B, and between Router C and Router D.

Configure Router C as a route reflector with clients Router B and Router D.

**Figure 81 Network diagram**

**Configuration procedure**

1. Configure IPv6 addresses for interfaces and IPv4 addresses for loopback interfaces. (Details not shown.)
2. Configure IBGP and EBGP connections and advertise network routes through IPv6 BGP:
   # Configure Router A.
   <RouterA> system-view
   [RouterA] bgp 100
   [RouterA-bgp-default] router-id 1.1.1.1
   [RouterA-bgp-default] peer 100::2 as-number 200
   [RouterA-bgp-default] address-family ipv6
   [RouterA-bgp-default-ipv6] peer 100::2 enable
   [RouterA-bgp-default-ipv6] network 1:: 64
   [RouterA-bgp-default-ipv6] network 100:: 96
   [RouterA-bgp-default-ipv6] quit
   [RouterA-bgp-default] quit
   # Configure Router B.
   <RouterB> system-view
   [RouterB] bgp 200
   [RouterB-bgp-default] router-id 2.2.2.2
   [RouterB-bgp-default] peer 100::1 as-number 100
   [RouterB-bgp-default] peer 101::1 as-number 200
   [RouterB-bgp-default] address-family ipv6
# Configure Router B.

[RouterB-bgp-default-ipv6] peer 100::1 enable
[RouterB-bgp-default-ipv6] peer 101::1 enable
[RouterB-bgp-default-ipv6] peer 101::1 next-hop-local
[RouterB-bgp-default-ipv6] network 100:: 96
[RouterB-bgp-default-ipv6] network 101:: 96
[RouterB-bgp-default-ipv6] quit
[RouterB-bgp-default] quit

# Configure Router C.

<RouterC> system-view
[RouterC] bgp 200
[RouterC-bgp-default] router-id 3.3.3.3
[RouterC-bgp-default] peer 101::2 as-number 200
[RouterC-bgp-default] peer 102::2 as-number 200
[RouterC-bgp-default] address-family ipv6
[RouterC-bgp-default-ipv6] peer 101::2 enable
[RouterC-bgp-default-ipv6] peer 102::2 enable
[RouterC-bgp-default-ipv6] network 101:: 96
[RouterC-bgp-default-ipv6] network 102:: 96

# Configure Router D.

<RouterD> system-view
[RouterD] bgp 200
[RouterD-bgp-default] router-id 4.4.4.4
[RouterD-bgp-default] peer 102::1 as-number 200
[RouterD-bgp-default] address-family ipv6
[RouterD-bgp-default-ipv6] peer 102::1 enable
[RouterD-bgp-default-ipv6] network 102:: 96

3. Configure Router C as a route reflector, and configure Router B and Router D as its clients.

[RouterC-bgp-default-ipv6] peer 101::2 reflect-client
[RouterC-bgp-default-ipv6] peer 102::2 reflect-client
[RouterC-bgp-default-ipv6] quit
[RouterC-bgp-default] quit

Verifying the configuration

# Execute the display bgp routing-table ipv6 command on Router D.

[RouterD] display bgp routing-table ipv6

Total number of routes: 5

BGP local router ID is 4.4.4.4
Status codes: * - valid, > - best, d - dampened, h - history,
    s - suppressed, S - stale, i - internal, e - external
    Origin: i - IGP, e - EGP, ? - incomplete

* >i Network : 1:: PrefixLen : 64
  NextHop : 101::2 LocPrf : 100
  PrefVal : 0 OutLabel : NULL
  MED : 0
  Path/Ogn: 100i
The output shows that Router D has learned the network 1::/64 from Router C through route reflection.

6PE configuration example

Network requirements

Use 6PE to connect two isolated IPv6 networks over an IPv4/MPLS network.

- The ISP uses OSPF as the IGP.
- PE 1 and PE 2 are edge devices of the ISP, and establish an IPv4 IBGP connection between them.
- CE 1 and CE 2 are edge devices of the IPv6 networks, and they connect the IPv6 networks to the ISP.
- A CE and a PE exchange IPv6 packets through IPv6 static routing.
Configuration procedure

1. Configure IPv6 addresses and IPv4 addresses for interfaces. (Details not shown.)
2. Configure PE 1:
   - # Enable LDP globally, and configure the LSP generation policy.
     <PE1> system-view
     [PE1] mpls lsr-id 2.2.2.2
     [PE1] mpls ldp
     [PE1-ldp] lsp-trigger all
     [PE1-ldp] quit
   - # Enable MPLS and LDP on GigabitEthernet 1/0/2.
     [PE1] interface gigabitethernet 1/0/2
     [PE1-GigabitEthernet1/0/2] mpls enable
     [PE1-GigabitEthernet1/0/2] mpls ldp enable
     [PE1-GigabitEthernet1/0/2] quit
   - # Configure IBGP, enable the peer’s 6PE capabilities, and redistribute IPv6 direct and static routes.
     [PE1-bgp-default] router-id 2.2.2.2
     [PE1-bgp-default] peer 3.3.3.3 as-number 65100
     [PE1-bgp-default] peer 3.3.3.3 connect-interface loopback 0
     [PE1-bgp-default] address-family ipv6
     [PE1-bgp-default-ipv6] import-route direct
     [PE1-bgp-default-ipv6] import-route static
     [PE1-bgp-default-ipv6] peer 3.3.3.3 enable
     [PE1-bgp-default-ipv6] peer 3.3.3.3 label-route-capability
     [PE1-bgp-default-ipv6] quit
     [PE1-bgp-default] quit
   - # Configure the static route to CE 1.
     [PE1] ipv6 route-static 1::1 128 10::1
   - # Configure OSPF for the ISP.
     [PE1-ospf-1] area 0
     [PE1-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
     [PE1-ospf-1-area-0.0.0.0] network 1.1.0.0 0.0.255.255
3. Configure PE 2:
   # Enable LDP globally, and configure the LSP generation policy.
   <PE2> system-view
   [PE2] mpls lsr-id 3.3.3.3
   [PE2] mpls ldp
   [PE2-mpls-ldp] lsp-trigger all
   [PE2-mpls-ldp] quit
   # Enable MPLS and LDP on GigabitEthernet 1/0/2.
   [PE2] interface gigabitethernet 1/0/2
   [PE2-GigabitEthernet1/0/2] mpls enable
   [PE2-GigabitEthernet1/0/2] mpls ldp enable
   [PE2-GigabitEthernet1/0/2] quit
   # Configure IBGP, enable the peer's 6PE capabilities, and redistribute IPv6 direct and static routes.
   [PE2] bgp 65100
   [PE2-bgp-default] router-id 3.3.3.3
   [PE2-bgp-default] peer 2.2.2.2 as-number 65100
   [PE2-bgp-default] peer 2.2.2.2 connect-interface loopback 0
   [PE2-bgp-default] address-family ipv6
   [PE2-bgp-default-ipv6] import-route direct
   [PE2-bgp-default-ipv6] import-route static
   [PE2-bgp-default-ipv6] peer 2.2.2.2 enable
   [PE2-bgp-default-ipv6] peer 2.2.2.2 label-route-capability
   [PE2-bgp-default-ipv6] quit
   [PE2-bgp-default] quit
   # Configure the static route to CE 2.
   [PE2] ipv6 route-static :: 0 128 20::1
   # Configure OSPF for the ISP.
   [PE2] ospf
   [PE2-ospf-1] area 0
   [PE2-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
   [PE2-ospf-1-area-0.0.0.0] network 1.1.0.0 0.0.255.255
   [PE2-ospf-1-area-0.0.0.0] quit
   [PE2-ospf-1] quit

4. Configure a static route, with PE 1 as the default next hop.
   <CE1> system-view
   [CE1] ipv6 route-static :: 0 10::2

5. Configure a static route on CE 2, with PE 2 as the default next hop.
   <CE2> system-view
   [CE2] ipv6 route-static :: 0 20::2

Verifying the configuration
   # Display the IPv6 BGP routing tables on PE 1 and PE 2. The output shows that each of them has two IPv6 network routes. The following shows the output on PE 1:
   [PE1] display bgp routing-table ipv6
Total number of routes: 5

BGP local router ID is 2.2.2.2

Status codes: * - valid, > - best, d - dampened, h - history,
               s - suppressed, S - stale, i - internal, e - external
               Origin: i - IGP, e - EGP, ? - incomplete

* >  Network : 1::1                         PrefixLen : 128
    NextHop : 10::1                          LocPrf : 
    PrefVal : 32768                          OutLabel : NULL
    MED : 0                                  
    Path/Ogn: ?                              

* >i Network : 4::4                         PrefixLen : 128
    NextHop : ::FFFF:3.3.3.3                LocPrf : 100
    PrefVal : 0                             OutLabel : 1279
    MED : 0                                 
    Path/Ogn: ?                              

* >  Network : 10::                           PrefixLen : 64
    NextHop : ::                             LocPrf : 
    PrefVal : 32768                          OutLabel : NULL
    MED : 0                                  
    Path/Ogn: ?                              

* >  Network : 10::2                        PrefixLen : 128
    NextHop : ::1                            LocPrf : 
    PrefVal : 32768                          OutLabel : NULL
    MED : 0                                  
    Path/Ogn: ?                              

* >i Network : 20::                         PrefixLen : 64
    NextHop : ::FFFF:3.3.3.3                LocPrf : 100
    PrefVal : 0                             OutLabel : 1278
    MED : 0                                 
    Path/Ogn: ?                              

# Verify that CE 1 can ping the IPv6 address 4::4 (loopback interface address) of CE 2. (Details not shown.)

BFD for IPv6 BGP configuration example

Network requirements

As shown in Figure 83, configure OSPFv3 as the IGP in AS 200.

- Establish two IBGP connections between Router A and Router C. When both paths operate correctly, Router C uses the path Router A<---Router B<---Router C to exchange packets with network 1200::0/64.
- Configure BFD over the path. When the path fails, BFD can quickly detect the failure and notify it to IPv6 BGP. Then, the path Router A<---Router D<---Router C takes effect immediately.
Configuration procedure

1. Configure IPv6 addresses for interfaces. (Details not shown.)
2. Configure OSPFv3 so that Router A and Router C can reach each other. (Details not shown.)
3. Configure IPv6 BGP on Router A:
   # Establish two IBGP connections to Router C.
   <RouterA> system-view
   [RouterA] bgp 200
   [RouterA-bgp-default] router-id 1.1.1.1
   [RouterA-bgp-default] peer 2002::2 as-number 200
   [RouterA-bgp-default] peer 3002::2 as-number 200
   [RouterA-bgp-default] address-family ipv6
   [RouterA-bgp-default-ipv6] peer 3002::2 enable
   [RouterA-bgp-default-ipv6] quit
   # Create IPv6 basic ACL 2000 to permit 1200::0/64 to pass.
   [RouterA] acl ipv6 basic 2000
   [RouterA-acl-ipv6-basic-2000] rule permit source 1200:: 64
   [RouterA-acl-ipv6-basic-2000] quit
   # Create two routing policies to set the MED for route 1200::0/64. The policy apply_med_50 sets the MED to 50, and the policy apply_med_100 sets the MED to 100.
   [RouterA] route-policy apply_med_50 permit node 10
   [RouterA-route-policy-apply_med_50-10] if-match ipv6 address acl 2000
   [RouterA-route-policy-apply_med_50-10] apply cost 50
   [RouterA-route-policy-apply_med_50-10] quit
   [RouterA] route-policy apply_med_100 permit node 10
   [RouterA-route-policy-apply_med_100-10] if-match ipv6 address acl 2000
   [RouterA-route-policy-apply_med_100-10] apply cost 100
   [RouterA-route-policy-apply_med_100-10] quit
   # Apply routing policy apply_med_50 to routes outgoing to peer 3002::2, and apply routing policy apply_med_100 to routes outgoing to peer 2002::2.
   [RouterA] bgp 200
   [RouterA-bgp-default] address-family ipv6 unicast
   [RouterA-bgp-default-ipv6] peer 3002::2 route-policy apply_med_50 export
[RouterA-bgp-default-ipv6] peer 2002::2 route-policy apply_med_100 export
[RouterA-bgp-default-ipv6] quit
# Enable BFD for peer 3002::2.
[RouterA-bgp-default] peer 3002::2 bfd
[RouterA-bgp-default] quit

4. Configure IPv6 BGP on Router C:
   # Establish two IBGP connections to Router A.
   <RouterC> system-view
   [RouterC] bgp 200
   [RouterC-bgp-default] router-id 3.3.3.3
   [RouterC-bgp-default] peer 3001::1 as-number 200
   [RouterC-bgp-default] peer 2001::1 as-number 200
   [RouterC-bgp-default] address-family ipv6
   [RouterC-bgp-default-ipv6] peer 3001::1 enable
   [RouterC-bgp-default-ipv6] peer 2001::1 enable
   [RouterC-bgp-default-ipv6] quit
   # Enable BFD for peer 3001::1.
   [RouterC-bgp-default] peer 3001::1 bfd
   [RouterC-bgp-default] quit
   [RouterC] quit

Verifying the configuration

# Display detailed BFD session information on Router C.
  <RouterC> display bfd session verbose
  Total Session Num: 1   Up Session Num: 1   Init Mode: Active

  IPv6 Session Working Under Ctrl Mode:
     Local Discr: 513                  Remote Discr: 513
     Source IP: 3002::2
     Destination IP: 3001::1
     Session State: Up                      Interface: N/A
     Min Tx Inter: 500ms                Act Tx Inter: 500ms
     Min Rx Inter: 500ms                Detect Inter: 2500ms
     Rx Count: 13                        Tx Count: 14
     Connect Type: Indirect           Running Up for: 00:00:05
     Hold Time: 2243ms                  Auth mode: None
     Detect Mode: Async                        Slot: 0
     Protocol: BGP4+                     Diag Info: No Diagnostic
     Version:1

The output shows that a BFD session has been established between Router A and Router C.

# Display BGP peer information on Router C.
  <RouterC> display bgp peer ipv6

  BGP local router ID: 3.3.3.3
  Local AS number: 200
  Total number of peers: 2              Peers in established state: 2
The output shows that Router C has established two BGP connections with Router A, and both connections are in Established state.

# Display route 1200::0/64 on Router C.

```
<RouterC> display ipv6 routing-table 1200::0 64 verbose
```

Summary count : 1

Destination: 1200::/64

```
Protocol: BGP4+   Process ID: 0
SubProtID: 0x1    Age: 00h00m57s
Cost: 100        Preference: 255
IpPre: N/A       QosLocalID: N/A
Tag: 0           State: Active Adv
OrigTblID: 0x1    OrigVrf: default-vrf
TableID: 0xa     OrigAs: 0
NibID: 0x25000000 LastAs: 0
AttrID: 0x0      Neighbor: 2001::1
Flags: 0x10060  OrigNextHop: 2001::1
Label: NULL     RealNextHop: FE80::20C:29FF:FE40:715
BkLabel: NULL   BkNextHop: N/A
Tunnel ID: Invalid Interface: GigabitEthernet1/0/1
BkTunnel ID: Invalid BkInterface: N/A
```

The output shows that Router C communicates with network 1200::0/64 through the path Router C<—>Router B<—>Router A.

# Break down the path Router C<—>Router B<—>Router A and then display route 1200::0/64 on Router C.

```
<RouterC> display ipv6 routing-table 1200::0 64 verbose
```

Summary count : 1

Destination: 1200::/64

```
Protocol: BGP4+   Process ID: 0
SubProtID: 0x1    Age: 00h01m07s
Cost: 50         Preference: 255
IpPre: N/A       QosLocalID: N/A
Tag: 0           State: Active Adv
OrigTblID: 0x1    OrigVrf: default-vrf
TableID: 0xa     OrigAs: 0
NibID: 0x25000001 LastAs: 0
AttrID: 0x1      Neighbor: 3001::1
Flags: 0x10060  OrigNextHop: 3001::1
Label: NULL     RealNextHop: FE80::20C:29FF:FE4A:3873
BkLabel: NULL   BkNextHop: N/A
Tunnel ID: Invalid Interface: GigabitEthernet1/0/1
BkTunnel ID: Invalid BkInterface: N/A
```

The output shows that Router C communicates with network 1200::0/64 through the path Router C<—>Router B<—>Router A.
The output shows that Router C communicates with network 1200::0/64 through the path Router C<—>Router D<—>Router A.

### IPsec for IPv6 BGP packets configuration example

#### Network requirements

As shown in Figure 84, all routers run IPv6 BGP. Establish an IBGP connection between Router A and Router B, and establish an EBGP connection between Router B and Router C.

To enhance security, configure IPsec to protect IPv6 BGP packets.

#### Figure 84 Network diagram

![Network Diagram](image)

#### Configuration procedure

1. Configure IPv6 addresses for interfaces. (Details not shown.)
2. Establish an IBGP connection between Router A and Router B:

   ```
   # Configure Router A.
   <RouterA> system-view
   [RouterA] bgp 65008
   [RouterA-bgp-default] router-id 1.1.1.1
   [RouterA-bgp-default] group ibgp internal
   [RouterA-bgp-default] peer 1::2 group ibgp
   [RouterA-bgp-default] address-family ipv6 unicast
   [RouterA-bgp-default-ipv6] peer ibgp enable
   [RouterA-bgp-default-ipv6] quit
   [RouterA-bgp-default] quit
   
   # Configure Router B.
   <RouterB> system-view
   [RouterB] bgp 65008
   [RouterB-bgp-default] router-id 2.2.2.2
   [RouterB-bgp-default] group ibgp internal
   [RouterB-bgp-default] peer 1::1 group ibgp
   [RouterB-bgp-default] address-family ipv6 unicast
   [RouterB-bgp-default-ipv6] peer ibgp enable
   [RouterB-bgp-default-ipv6] quit
   ```

3. Establish an EBGP connection between Router B and Router C:

   ```
   # Configure Router C.
   <RouterC> system-view
   [RouterC] bgp 65009
   [RouterC-bgp-default] router-id 3.3.3.3
   [RouterC-bgp-default] group ebgp external
   [RouterC-bgp-default] peer 3::1 as-number 65008
   ```
# Configure Router B.
[RouterB-bgp-default] group ebgp external
[RouterB-bgp-default] peer 3::2 as-number 65009
[RouterB-bgp-default] peer 3::2 group ebgp
[RouterB-bgp-default] address-family ipv6 unicast
[RouterB-bgp-default-ipv6] peer ebgp enable
[RouterB-bgp-default-ipv6] quit
[RouterB-bgp-default] quit

4. Configure IPsec transform sets and IPsec profiles:
   # On Router A, create an IPsec transform set named tran1.
   [RouterA] ipsec transform-set tran1
   # Set the encapsulation mode to transport mode.
   [RouterA-ipsec-transform-set-tran1] encapsulation-mode transport
   # Set the security protocol to ESP, the encryption algorithm to DES, and authentication
   algorithm to SHA1.
   [RouterA-ipsec-transform-set-tran1] esp encryption-algorithm des
   [RouterA-ipsec-transform-set-tran1] esp authentication-algorithm shal
   [RouterA-ipsec-transform-set-tran1] quit
   # Create an IPsec profile named policy001, and specify the manual mode for it.
   [RouterA] ipsec profile policy001 manual
   # Use IPsec transform set tran1.
   [RouterA-ipsec-profile-policy001-manual] transform-set tran1
   # Set the SPIs of the inbound and outbound SAs to 12345.
   [RouterA-ipsec-profile-policy001-manual] sa spi outbound esp 12345
   [RouterA-ipsec-profile-policy001-manual] sa spi inbound esp 12345
   # Set the keys for the inbound and outbound SAs using ESP to abcdefg.
   [RouterA-ipsec-profile-policy001-manual] sa string-key outbound esp simple abcdefg
   [RouterA-ipsec-profile-policy001-manual] sa string-key inbound esp simple abcdefg
   [RouterA-ipsec-profile-policy001-manual] quit
   # On Router B, create an IPsec transform set named tran1.
   [RouterB] ipsec transform-set tran1
   # Set the encapsulation mode to transport mode.
   [RouterB-ipsec-transform-set-tran1] encapsulation-mode transport
   # Set the security protocol to ESP, the encryption algorithm to DES, and authentication
   algorithm to SHA1.
   [RouterB-ipsec-transform-set-tran1] esp encryption-algorithm des
   [RouterB-ipsec-transform-set-tran1] esp authentication-algorithm shal
   [RouterB-ipsec-transform-set-tran1] quit
   # Create IPsec profile named policy001, and specify the manual mode for it.
   [RouterB] ipsec profile policy001 manual
   # Use IPsec transform set tran1.
   [RouterB-ipsec-profile-policy001-manual] transform-set tran1
Set the SPIs of the inbound and outbound SAs to 12345.

```
[RouterB-ipsec-profile-policy001-manual] sa spi outbound esp 12345
[RouterB-ipsec-profile-policy001-manual] sa spi inbound esp 12345
```

Set the keys for the inbound and outbound SAs using ESP to abcdefg.

```
[RouterB-ipsec-profile-policy001-manual] sa string-key outbound esp simple abcdefg
[RouterB-ipsec-profile-policy001-manual] sa string-key inbound esp simple abcdefg
```

Create an IPsec transform set named tran2.

```
[RouterB-ipsec-transform-set-tran2] encapsulation-mode transport
[RouterB-ipsec-transform-set-tran2] esp encryption-algorithm des
[RouterB-ipsec-transform-set-tran2] esp authentication-algorithm sha1
```

Create IPsec profile named policy002, and specify the manual mode for it.

```
[RouterB-ipsec-profile-policy002-manual] transform-set tran2
```

Set the SPIs of the inbound and outbound SAs to 54321.

```
[RouterB-ipsec-profile-policy002-manual] sa spi outbound esp 54321
[RouterB-ipsec-profile-policy002-manual] sa spi inbound esp 54321
```

Set the keys for the inbound and outbound SAs using ESP to gfedcba.

```
[RouterB-ipsec-profile-policy002-manual] sa string-key outbound esp simple gfedcba
[RouterB-ipsec-profile-policy002-manual] sa string-key inbound esp simple gfedcba
```

On Router C, create an IPsec transform set named tran2.

```
[RouterC-ipsec-transform-set-tran2] encapsulation-mode transport
[RouterC-ipsec-transform-set-tran2] esp encryption-algorithm des
[RouterC-ipsec-transform-set-tran2] esp authentication-algorithm sha1
```

Create IPsec profile named policy002, and specify the manual mode for it.

```
[RouterC-ipsec-profile-policy002-manual] transform-set tran2
```

Set the SPIs of the inbound and outbound SAs to 54321.

```
[RouterC-ipsec-profile-policy002-manual] sa spi outbound esp 54321
[RouterC-ipsec-profile-policy002-manual] sa spi inbound esp 54321
```

Set the keys for the inbound and outbound SAs using ESP to gfedcba.

```
[RouterC-ipsec-profile-policy002-manual] sa string-key outbound esp simple gfedcba
[RouterC-ipsec-profile-policy002-manual] sa string-key inbound esp simple gfedcba
```
5. Configure IPsec to protect IPv6 BGP packets between Router A and Router B:
   # Configure Router A.
   [RouterA] bgp 65008
   [RouterA-bgp-default] peer 1:2 ipsec-profile policy001
   [RouterA-bgp-default] quit
   # Configure Router B.
   [RouterB] bgp 65008
   [RouterB-bgp-default] peer 1:1 ipsec-profile policy001
   [RouterB-bgp-default] quit

6. Configure IPsec to protect IPv6 BGP packets between Router B and Router C:
   # Configure Router C.
   [RouterC] bgp 65009
   [RouterC-bgp-default] peer ebgp ipsec-profile policy002
   [RouterC-bgp-default] quit
   # Configure Router B.
   [RouterB] bgp 65008
   [RouterB-bgp-default] peer ebgp ipsec-profile policy002
   [RouterB-bgp-default] quit

Verifying the configuration

# Display detailed information about IPv6 BGP peers on Router B.
[RouterB] display bgp peer ipv6 verbose

Peer: 1::1      Local: 2.2.2.2
Type: IBGP link
BGP version 4, remote router ID 1.1.1.1
BGP current state: Established, Up for 00h05m54s
BGP current event: KATimerExpired
BGP last state: OpenConfirm
Port: Local - 24896    Remote - 179
Configured: Active Hold Time: 180 sec   Keepalive Time: 60 sec
Received: Active Hold Time: 180 sec   Keepalive Time: 60 sec
Negotiated: Active Hold Time: 180 sec   Keepalive Time: 60 sec
Peer optional capabilities:
Peer support BGP multi-protocol extended
Peer support BGP route refresh capability
Peer support BGP route AS4 capability
Address family IPv6 Unicast: advertised and received

InQ updates: 0, OutQ updates: 0
NLRI statistics:
   Rcvd: UnReach NLRI 0, Reach NLRI 0
   Sent: UnReach NLRI 0, Reach NLRI 3

Message statistics:
   Msg type     Last rcvd time/ Current rcvd count/ History rcvd count/
   Last sent time/ Current sent count/ History sent count
Open       18:59:15-2013.4.24 1 1
18:59:15-2013.4.24  1  2
Update - 0 0
18:59:16-2013.4.24  1  1
Notification - 0 0
18:59:15-2013.4.24  0  1
Keepalive 18:59:15-2013.4.24  1  1
18:59:15-2013.4.24  1  1
RouteRefresh - 0 0
- 0 0
Total - 2 2
- 3 5

Maximum allowed prefix number: 4294967295
Threshold: 75%
Minimum time between advertisements is 15 seconds
Optional capabilities:
  Multi-protocol extended capability has been enabled
  Route refresh capability has been enabled
Peer preferred value: 0
IPsec profile name: policy001

Routing policy configured:
No routing policy is configured

Peer: 3::2   Local: 2.2.2.2
Type: EBGP link
BGP version 4, remote router ID 3.3.3.3
BGP current state: Established, Up for 00h05m00s
BGP current event: KATimerExpired
BGP last state: OpenConfirm
Port:  Local - 24897   Remote - 179
Configured: Active Hold Time: 180 sec   Keepalive Time: 60 sec
Received : Active Hold Time: 180 sec
Negotiated: Active Hold Time: 180 sec   Keepalive Time: 60 sec
Peer optional capabilities:
  Peer support BGP multi-protocol extended
  Peer support BGP route refresh capability
  Peer support BGP route AS4 capability
  Address family IPv6 Unicast: advertised and received

Received: Total 8 messages, Update messages 1
Sent: Total 8 messages, Update messages 1
Maximum allowed prefix number: 4294967295
Threshold: 75%
Minimum time between advertisements is 30 seconds
Optional capabilities:
  Multi-protocol extended capability has been enabled
  Route refresh capability has been enabled
Peer preferred value: 0
IPsec profile name: policy002

Routing policy configured:
No routing policy is configured

The output shows that IBGP and EBGP peers are established and both sent and received IPv6 BGP packets are encapsulated by IPsec.

IPv6 BGP FRR configuration example

Network requirements

As shown in Figure 85, configure BGP FRR so that when Link B fails, BGP uses Link A to forward traffic.

Figure 85 Network diagram

Configuration procedure

1. Configure IPv6 addresses for interfaces. (Details not shown.)
2. Configure OSPFv3 in AS 200 to ensure connectivity among Router B, Router C, and Router D. (Details not shown.)
3. Configure BGP connections:
   # Configure Router A to establish EBGP sessions to Router B and Router C, and advertise network 1::/64.
   <RouterA> system-view
   [RouterA] bgp 100
   [RouterA] router-id 1.1.1.1
   [RouterA-bgp-default] peer 3001::2 as-number 200
   [RouterA-bgp-default] peer 2001::2 as-number 200
   [RouterA-bgp-default] address-family ipv6 unicast
   [RouterA-bgp-default-ipv6] peer 3001::2 enable
   [RouterA-bgp-default-ipv6] peer 2001::2 enable
   [RouterA-bgp-default-ipv6] network 1::/64
   [RouterA-bgp-default-ipv6] quit
   [RouterA-bgp-default] quit
# Configure Router B to establish an EBGP session to Router A, and an IBGP session to Router D.

```yaml
<RouterB> system-view
[RouterB] bgp 200
[RouterB] router-id 2.2.2.2
[RouterB-bgp-default] peer 3001::1 as-number 100
[RouterB-bgp-default] peer 3002::2 as-number 200
[RouterB-bgp-default] address-family ipv6 unicast
[RouterB-bgp-default-ipv6] peer 3001::1 enable
[RouterB-bgp-default-ipv6] peer 3002::2 enable
[RouterB-bgp-default-ipv6] peer 3002::2 next-hop-local
[RouterB-bgp-default-ipv6] quit
[RouterB-bgp-default] quit
```

# Configure Router C to establish an EBGP session to Router A, and an IBGP session to Router D.

```yaml
<RouterC> system-view
[RouterC] bgp 200
[RouterC] router-id 3.3.3.3
[RouterC-bgp-default] peer 2001::1 as-number 100
[RouterC-bgp-default] peer 2002::2 as-number 200
[RouterC-bgp-default] address-family ipv6 unicast
[RouterC-bgp-default-ipv6] peer 2001::1 enable
[RouterC-bgp-default-ipv6] peer 2002::2 enable
[RouterC-bgp-default-ipv6] peer 2002::2 next-hop-local
[RouterC-bgp-default-ipv6] quit
[RouterC-bgp-default] quit
```

# Configure Router D to establish IBGP sessions to Router B and Router C, and advertise network 4::/64.

```yaml
<RouterD> system-view
[RouterD] bgp 200
[RouterD-bgp-default] peer 3002::1 as-number 200
[RouterD-bgp-default] peer 2002::1 as-number 200
[RouterD-bgp-default] address-family ipv6 unicast
[RouterD-bgp-default-ipv6] peer 3002::1 enable
[RouterD-bgp-default-ipv6] peer 2002::1 enable
[RouterD-bgp-default-ipv6] network 4:: 64
[RouterD-bgp-default-ipv6] quit
[RouterD-bgp-default] quit
```

4. Configure preferred values so Link B is used to forward traffic between Router A and Router D:

   # Configure Router A to set the preferred value to 100 for routes received from Router B.
   ```yaml
   [RouterA-bgp-default-ipv6] peer 3001::2 preferred-value 100
   [RouterA-bgp-default-ipv6] quit
   [RouterA-bgp-default] quit
   ```

   # Configure Router D to set the preferred value to 100 for routes received from Router B.
   ```yaml
   [RouterD-bgp-default-ipv6] peer 3002::1 preferred-value 100
   [RouterD-bgp-default-ipv6] quit
   [RouterD-bgp-default] quit
   ```

5. Configure BGP FRR:
# On Router A, create routing policy frr to set a backup next hop 2001::2 (Router C) for the route destined for 4::/64.

```bash
<RouterA> system-view
[RouterA] ipv6 prefix-list abc index 10 permit 4:: 64
[RouterA] route-policy frr permit node 10
[RouterA-route-policy] if-match ipv6 address prefix-list abc
[RouterA-route-policy] apply ipv6 fast-reroute backup-nexthop 2001::2
[RouterA-route-policy] quit
```

# Apply the routing policy to BGP FRR for BGP IPv6 unicast address family.

```bash
[RouterA] bgp 100
[RouterA-bgp-default] address-family ipv6 unicast
[RouterA-bgp-default-ipv6] quit
[RouterA-bgp-default] quit
```

# On Router D, create routing policy frr to set a backup next hop 2002::1 (Router C) for the route destined for 1::/64.

```bash
<RouterD> system-view
[RouterD] ipv6 prefix-list abc index 10 permit 1:: 64
[RouterD] route-policy frr permit node 10
[RouterD-route-policy] if-match ipv6 address prefix-list abc
[RouterD-route-policy] apply ipv6 fast-reroute backup-nexthop 2002::1
[RouterD-route-policy] quit
```

# Apply the routing policy to BGP FRR for BGP IPv6 unicast address family.

```bash
[RouterD] bgp 200
[RouterD-bgp-default] address-family ipv6 unicast
[RouterD-bgp-default-ipv6] quit
[RouterD-bgp-default] quit
```

**Verifying the configuration**

# Display detailed information about the route to 4::/64 on Router A. The output shows the backup next hop for the route.

```bash
[RouterA] display ipv6 routing-table 4:: 64 verbose
```

Summary count : 1

**Destination:** 4::/64  
**Protocol:** BGP4+  
**Process ID:** 0  
**SubProtID:** 0x2  
**Age:** 00h00m58s  
**Cost:** 0  
**IpPre:** N/A  
**QosLocalID:** N/A  
**Tag:** 0  
**State:** Active Adv  
**OrigVrf:** default-vrf  
**OrigTblID:** 0x0  
**OrigAs:** 200  
**TableID:** 0xa  
**NibID:** 0x25000003  
**LastAs:** 200  
**AttrID:** 0x3  
**Neighbor:** 3001::2  
**Flags:** 0x10060  
**OrigNextHop:** 3001::2  
**Label:** NULL  
**RealNextHop:** 2001::2  
**BkLabel:** NULL  
**BkNextHop:** 2001::2
IPv6 multicast BGP configuration example

Network requirements

As shown in Figure 86, OSPFv3 runs within AS 100 and AS 200 to ensure intra-AS connectivity. IPv6 MBGP runs between the two ASs to exchange IPv6 unicast routes used for RPF check.

Enable Anycast RP on Router A and Router B.
Table 18 Interface and IP address assignment

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>N/A</td>
<td>1002::100/64</td>
<td>Router B</td>
<td>GE1/0/1</td>
<td>1001::2/64</td>
</tr>
<tr>
<td>Router A</td>
<td>GE1/0/1</td>
<td>1002::1/64</td>
<td>GE1/0/2</td>
<td>2002::1/64</td>
<td></td>
</tr>
<tr>
<td></td>
<td>GE1/0/2</td>
<td>1001::1/64</td>
<td>GE1/0/3</td>
<td>2001::1/64</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Loop0</td>
<td>1:1::1/128</td>
<td>Loop0</td>
<td>1:1::1/128</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Loop1</td>
<td>1:1::2/128</td>
<td>Loop1</td>
<td>2:2::2/128</td>
<td></td>
</tr>
<tr>
<td>Router C</td>
<td>GE1/0/1</td>
<td>3002::1/64</td>
<td>Router D</td>
<td>GE1/0/1</td>
<td>2002::2/64</td>
</tr>
<tr>
<td></td>
<td>GE1/0/2</td>
<td>2001::2/64</td>
<td>GE1/0/2</td>
<td>3001::2/64</td>
<td></td>
</tr>
<tr>
<td></td>
<td>GE1/0/3</td>
<td>3001::1/64</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Configuration procedure

1. Configure IPv6 addresses for interfaces and configure OSPFv3 (this example uses OSPFv3 process 1) in AS 200 to ensure intra-AS connectivity. (Details not shown.)
2. Enable IPv6 multicast routing, IPv6 PIM-SM, and MLD, and configure BSR boundaries:
   # On Router A, enable IPv6 multicast routing globally, and enable IPv6 PIM-SM on interfaces.
   <RouterA> system-view
   [RouterA] ipv6 multicast routing
   [RouterA-mrib6] quit
   [RouterA] interface gigabitethernet 1/0/1
   [RouterA-GigabitEthernet1/0/1] ipv6 pim sm
   [RouterA-GigabitEthernet1/0/1] quit
   [RouterA] interface gigabitethernet 1/0/2
   [RouterA-GigabitEthernet1/0/2] ipv6 pim sm
   [RouterA-GigabitEthernet1/0/2] quit
   [RouterA] interface loopback 0
   [RouterA-LoopBack0] ipv6 pim sm
   [RouterA-LoopBack0] quit
   # Configure Router B and Router D in the same way that Router A was configured.
# On Router C, enable IPv6 multicast routing globally.

```
<RouterC> system-view
[RouterC] ipv6 multicast routing
[RouterC-mrib6] quit
```

# Enable IPv6 PIM-SM on interfaces, and enable MLD on GigabitEthernet 1/0/1.

```
[RouterC] interface gigabitethernet 1/0/2
[RouterC-GigabitEthernet1/0/2] ipv6 pim sm
[RouterC-GigabitEthernet1/0/2] quit
```

```
[RouterC] interface gigabitethernet 1/0/3
[RouterC-GigabitEthernet1/0/3] ipv6 pim sm
[RouterC-GigabitEthernet1/0/3] quit
```

```
[RouterC] interface gigabitethernet 1/0/1
[RouterC-GigabitEthernet1/0/1] ipv6 pim sm
[RouterC-GigabitEthernet1/0/1] mld enable
[RouterC-GigabitEthernet1/0/1] quit
```

# Configure the BSR boundary on Router A.

```
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] ipv6 pim bsr-boundary
[RouterA-GigabitEthernet1/0/2] quit
```

# Configure the BSR boundary on Router B.

```
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] ipv6 pim bsr-boundary
[RouterB-GigabitEthernet1/0/1] quit
```

3. Enable Anycast RP, and specify C-BSR and C-RP:

   # Configure Router A.

```
[RouterA] ipv6 pim
[RouterA-pim6] anycast-rp 1:1::1 1:1::2
[RouterA-pim6] anycast-rp 1:1::1 2:2::2
[RouterA-pim6] c-bsr 1:1::1
[RouterA-pim6] c-rp 1:1::1
[RouterA-pim6] quit
```

   # Configure Router B.

```
[RouterB] ipv6 pim
[RouterB-pim6] anycast-rp 1:1::1 1:1::2
[RouterB-pim6] anycast-rp 1:1::1 2:2::2
[RouterB-pim6] c-bsr 1:1::1
[RouterB-pim6] c-rp 1:1::1
[RouterB-pim6] quit
```

4. Configure BGP to establish BGP IPv6 multicast peers and redistribute routes:

   # On Router A, establish an EBGP session to Router B.

```
[RouterA] bgp 100
[RouterA-bgp-default] router-id 1.1.1.1
[RouterA-bgp-default] peer 1001::2 as-number 200
```

   # Enable exchange of IPv6 unicast routes used for RPF check with Router B.

```
[RouterA-bgp-default] address-family ipv6 multicast
[RouterA-bgp-default-mul-ipv6] peer 1001::2 enable
```

   # Redistribute direct routes into BGP.
[RouterA-bgp-default-mul-ipv6] quit

# On Router B, establish an EBGP session to Router A.
[RouterB] bgp 200
[RouterB-bgp-default] router-id 2.2.2.2
[RouterB-bgp-default] peer 1001::1 as-number 100

# Enable exchange of IPv6 unicast routes used for RPF check with Router B.
[RouterB-bgp-default] address-family ipv6 multicast
[RouterB-bgp-default-mul-ipv6] peer 1001::1 enable

# Redistribute OSPFv3 routes into BGP.
[RouterB-bgp-default-mul-ipv6] import-route ospfv3 1
[RouterB-bgp-default-mul-ipv6] quit

5. Establish BGP IPv6 unicast peer relationships between Router A and Router B and redistribute routes:

# On Router A, enable BGP to exchange IPv6 unicast routes with Router B, and redistribute direct routes into BGP.
[RouterA-bgp-default] address-family ipv6 unicast
[RouterA-bgp-default-ipv6] peer 1001::2 enable
[RouterA-bgp-default-ipv6] import-route direct
[RouterA-bgp-default] quit

# On Router B, enable BGP to exchange IPv6 unicast routes with Router A, and redistribute direct routes into BGP.
[RouterB-bgp-default] address-family ipv6 unicast
[RouterB-bgp-default-ipv6] peer 1001::1 enable
[RouterB-bgp-default-ipv6] import-route direct
[RouterB-bgp-default] quit

Verifying the configuration

# Verify the BGP IPv6 multicast peer information on Router B.
[RouterB] display bgp peer ipv6 multicast

BGP local router ID : 2.2.2.2
Local AS number : 200
Total number of peers : 3  Peers in established state : 3

Peer AS MsgRcvd MsgSent OutQ PrefRcv Up/Down State
1001::1 100 56 56 0 00:40:54 Established

# Verify the RPF information for the multicast source on Router B.
[RouterB] display ipv6 multicast rpf-info 1002::1

RPF information about source 1002::1:
RPF interface: GE1/0/1, RPF neighbor: 1001::1
Referenced prefix/prefix length: 1002::/64
Referenced route type: mbgp
Route selection rule: preference-preferred
Load splitting rule: disable

370
Troubleshooting BGP

Symptom

The `display bgp peer ipv4 unicast` or `display bgp peer ipv6 unicast` command output shows that the state of the connection to a peer cannot become established.

Analysis

To become BGP peers, any two routers must establish a TCP connection using port 179 and exchange Open messages successfully.

Solution

1. To resolve the problem:
   a. Use the `display current-configuration` command to verify the current configuration, and verify that the peer’s AS number is correct.
   b. Use the `display bgp peer ipv4 unicast` or `display bgp peer ipv6 unicast` command to verify that the peer’s IP/IPv6 address is correct.
   c. If a loopback interface is used, verify that the loopback interface is specified with the `peer connect-interface` command.
   d. If the peer is a non-direct EBGP peer, verify that the `peer ebgp-max-hop` command is configured.
   e. If the `peer ttl-security hops` command is configured, verify that the command is configured on the peer. Verify that the hop-count values configured on them are greater than the number of hops between them.
   f. Verify that a valid route to the peer is available.
   g. Use the `ping` command to verify the connectivity to the peer.
   h. Use the `display tcp verbose` or `display ipv6 tcp verbose` command to verify the TCP connection.
   i. Verify that no ACL rule is applied to disable TCP port 179.

2. If the problem persists, contact Hewlett Packard Enterprise Support.
Configuring PBR

Overview

Policy-based routing (PBR) uses user-defined policies to route packets. A policy can specify parameters for packets that match specific criteria such as ACLs or that have specific lengths. The parameters include the next hop, output interface, default next hop, and default output interface.

A device forwards received packets using the following process:
1. The device uses PBR to forward matching packets.
2. If the packets do not match the PBR policy or the PBR-based forwarding fails, the device uses the routing table, excluding the default route, to forward the packets.
3. If the routing table-based forwarding fails, the device uses the default next hop or default output interface defined in PBR to forward packets.
4. If the default next hop or default output interface-based forwarding fails, the device uses the default route to forward packets.

PBR includes local PBR and interface PBR.
- Local PBR guides the forwarding of locally generated packets, such as the ICMP packets generated by using the ping command.
- Interface PBR guides the forwarding of packets received on an interface only.

Policy

A policy includes match criteria and actions to be taken on the matching packets. A policy can have one or multiple nodes as follows:
- Each node is identified by a node number. A smaller node number has a higher priority.
- A node contains if-match and apply clauses. An if-match clause specifies a match criterion, and an apply clause specifies an action.
- A node has a match mode of permit or deny.

A policy compares packets with nodes in priority order. If a packet matches the criteria on a node, it is processed by the action on the node. Otherwise, it goes to the next node for a match. If the packet does not match the criteria on any node, it is forwarded according to the routing table.

if-match clause

PBR supports the following types of if-match clauses:
- if-match acl—Sets an ACL match criterion.
- if-match packet-length—Sets a packet length match criterion to match the total length of data packets.

You can specify multiple types of if-match clauses for a node but only one if-match clause of each type. To match a node, a packet must match all types of the if-match clauses for the node.

apply clause

PBR supports the types of apply clauses shown in Table 19. You can specify multiple apply clauses for a node, but some of them might not be executed. The following apply clauses determine the packet forwarding paths in a descending order:
- apply access-vpn vpn-instance
- apply next-hop
• apply output-interface
• apply default-next-hop
• apply default-output-interface

Table 19 Priorities and meanings of apply clauses

<table>
<thead>
<tr>
<th>Clause</th>
<th>Meaning</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>apply precedence</td>
<td>Sets an IP precedence.</td>
<td>This clause is always executed.</td>
</tr>
<tr>
<td>apply ip-df df-value</td>
<td>Sets the Don't Fragment (DF) bit in the IP header.</td>
<td>This clause is always executed.</td>
</tr>
</tbody>
</table>
| apply loadshare { next-hop | output-interface | default-next-hop | default-output-interface } | Enables load sharing among multiple next hops, output interfaces, default next hops, and default output interfaces. | Multiple next hops, output interfaces, default next hops, or default output interfaces operate in either primary/backup or load sharing mode. For example:
  • Primary/backup mode—The first configured output interface is used. When the primary output interface fails, the first configured backup output interface takes over.
  • Load sharing mode—Multiple output interfaces load share traffic on a per-packet basis in turn, according to the configuration order. Multiple next hops load share traffic according to their weights.
By default, the primary/backup mode applies. |
| apply access-vpn vpn-instance | Sets VPN instances. | If a packet matches a forwarding entry of a specified VPN instance, it is forwarded in the VPN instance. |
| apply next-hop and apply output-interface | Sets next hops and sets output interfaces. | Only the apply next-hop clause is executed when both are configured. |
| apply default-next-hop and apply default-output-interface | Sets default next hops and sets default output interfaces. | Only the apply default-next-hop clause is executed when both are configured. They take effect only when no next hop or output interface is set or the next hop and output interface are invalid, and the packet does not match any route in the routing table. |
| apply continue | Compares packets with the next node upon failure on the current node. | The apply continue clause applies when the apply access-vpn vpn-instance, apply next-hop, apply output-interface, apply default-next-hop, and apply default-output-interface clauses are not configured or become invalid. For example, the specified next hop is unreachable, the specified output interface is down, or the packets cannot be forwarded in the specified VPN instance. |

Relationship between the match mode and clauses on the node

<table>
<thead>
<tr>
<th>Does a packet match all the if-match clauses on the node?</th>
<th>Match mode</th>
<th>Deny</th>
</tr>
</thead>
</table>
| Yes. | Permit | If the node is configured with apply clauses, PBR executes the apply clauses on the node.  
  o If the PBR-based forwarding | The packet is forwarded according to the routing table. |

373
### Does a packet match all the if-match clauses on the node?

<table>
<thead>
<tr>
<th>Match mode</th>
<th>Permit</th>
<th>Deny</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>succeeds, PBR does not compare the packet with the next node.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>o If the PBR-based forwarding fails and the <code>apply continue</code> clause is not configured, PBR does not compare the packet with the next node.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>o If the PBR-based forwarding fails and the <code>apply continue</code> clause is configured, PBR compares the packet with the next node.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If the node is configured with no <code>apply</code> clauses, the packet is forwarded according to the routing table.</td>
<td></td>
</tr>
</tbody>
</table>

- No. PBR compares the packet with the next node.
- PBR compares the packet with the next node.

A node that has no **if-match** clauses matches any packet.

### PBR and Track

PBR can work with the Track feature to dynamically adapt the availability status of an `apply` clause to the link status of a tracked object. The tracked object can be a next hop, output interface, default next hop, or default output interface.

- When the track entry associated with an object changes to **Negative**, the `apply` clause is invalid.
- When the track entry changes to **Positive** or **NotReady**, the `apply` clause is valid.

For more information about Track-PBR collaboration, see *High Availability Configuration Guide*.

### Command and hardware compatibility

Commands and descriptions for centralized devices apply to the following routers:

- MSR1002-4/1003-8S.
- MSR2003.
- MSR3012/3024/3044/3064.
- MSR958(JH300A/JH301A).

Commands and descriptions for distributed devices apply to MSR4060 and MSR4080 routers.
**PBR configuration task list**

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Required.) Configuring a policy:</td>
</tr>
<tr>
<td>• Creating a node</td>
</tr>
<tr>
<td>• Setting match criteria for a node</td>
</tr>
<tr>
<td>• Configuring actions for a node</td>
</tr>
<tr>
<td>(Required.) Configuring PBR:</td>
</tr>
<tr>
<td>• Configuring local PBR</td>
</tr>
<tr>
<td>• Configuring interface PBR</td>
</tr>
</tbody>
</table>

### Configuring a policy

#### Creating a node

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create a node for a policy, and enter its view.</td>
<td>policy-based-route policy-name [ deny</td>
</tr>
</tbody>
</table>

#### Setting match criteria for a node

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter policy node view.</td>
<td>policy-based-route policy-name [ deny</td>
</tr>
<tr>
<td>3.</td>
<td>Set an ACL match criterion.</td>
<td>if-match acl acl-number { acl-number</td>
</tr>
<tr>
<td>4.</td>
<td>Set a packet length match criterion.</td>
<td>if-match packet-length min-len max-len</td>
</tr>
</tbody>
</table>

**NOTE:**
An ACL match criterion uses the specified ACL to match packets if the action in the ACL rule is `permit`. If the specified ACL does not exist or the action in the ACL rule is `deny`, no packet is matched.

#### Configuring actions for a node

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>2.</td>
<td>Enter policy node view.</td>
<td>policy-based-route policy-name [ deny</td>
</tr>
<tr>
<td>3.</td>
<td>Set an IP precedence.</td>
<td>apply precedence { type</td>
</tr>
<tr>
<td>4.</td>
<td>Set the DF bit in the IP header.</td>
<td>apply ip-df df-value</td>
</tr>
<tr>
<td>5.</td>
<td>Set VPN instances.</td>
<td>apply access-vpn vpn-instance-name &amp;&lt;1-n&gt;</td>
</tr>
<tr>
<td>6.</td>
<td>Set next hops.</td>
<td>apply next-hop [ vpn-instance-name</td>
</tr>
<tr>
<td>7.</td>
<td>Enable load sharing among multiple next hops.</td>
<td>apply loadshare next-hop</td>
</tr>
<tr>
<td>8.</td>
<td>Set output interfaces.</td>
<td>apply output-interface { interface-type interface-number [ track track-entry-number ] } &amp;&lt;1-n&gt;</td>
</tr>
<tr>
<td>9.</td>
<td>Enable load sharing among multiple output interfaces.</td>
<td>apply loadshare output-interface</td>
</tr>
<tr>
<td>10.</td>
<td>Set default next hops.</td>
<td>apply default-next-hop [ vpn-instance-name</td>
</tr>
<tr>
<td>11.</td>
<td>Enable load sharing among multiple</td>
<td>apply loadshare default-next-hop</td>
</tr>
</tbody>
</table>
### Configuring PBR

#### Configuring local PBR

Configure PBR by applying a policy locally. PBR uses the policy to guide the forwarding of locally generated packets. The specified policy must already exist. Otherwise, the local PBR configuration fails.

You can apply only one policy locally. Before you apply a new policy, you must first remove the current policy.

Local PBR might affect local services, such as ping and Telnet. Do not configure local PBR unless doing so is required.

To configure local PBR:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>ip local policy-based-route policy-name</td>
<td>By default, no policy is locally applied.</td>
</tr>
</tbody>
</table>

#### Configuring interface PBR

Configure PBR by applying a policy to an interface. PBR uses the policy to guide the forwarding of packets received on the interface. The specified policy must already exist. Otherwise, the interface PBR configuration fails.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.</td>
<td>apply default-output-interface { interface-type interface-number [ track track-entry-number ] }&amp;&lt;1-n&gt;</td>
<td>By default, no default output interface is specified. You can specify multiple default output interfaces for backup or load sharing in one command line or by executing this command multiple times. You can specify a maximum of n default output interfaces for a node. The value of n is 4.</td>
</tr>
<tr>
<td>13.</td>
<td>apply loadshare default-output-interface</td>
<td>By default, the default output interfaces operate in primary/backup mode.</td>
</tr>
<tr>
<td>14.</td>
<td>apply continue</td>
<td>By default, PBR does not compare packets with the next node upon match failure on the current node. This command takes effect only when the match mode of the node is permit.</td>
</tr>
</tbody>
</table>
You can apply only one policy to an interface. Before you apply a new policy, you must first remove the current policy from the interface.

You can apply a policy to multiple interfaces.

To configure interface PBR:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Apply a policy to the interface.</td>
<td>ip policy-based-route policy-name</td>
</tr>
</tbody>
</table>

Displaying and maintaining PBR

Execute **display** commands in any view and **reset** commands in user view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display PBR policy information.</td>
<td>display ip policy-based-route [ policy policy-name ]</td>
</tr>
<tr>
<td>Display PBR configuration.</td>
<td>display ip policy-based-route setup</td>
</tr>
<tr>
<td>Display local PBR configuration and statistics (centralized devices in standalone mode).</td>
<td>display ip policy-based-route local</td>
</tr>
<tr>
<td>Display local PBR configuration and statistics (distributed devices in standalone mode/centralized devices in IRF mode).</td>
<td>display ip policy-based-route local [ slot slot-number ]</td>
</tr>
<tr>
<td>Display local PBR configuration and statistics (distributed devices in IRF mode).</td>
<td>display ip policy-based-route local [ chassis chassis-number slot slot-number ]</td>
</tr>
<tr>
<td>Display interface PBR configuration and statistics (centralized devices in standalone mode).</td>
<td>display ip policy-based-route interface interface-type interface-number</td>
</tr>
<tr>
<td>Display interface PBR configuration and statistics (distributed devices in standalone mode/centralized devices in IRF mode).</td>
<td>display ip policy-based-route interface interface-type interface-number [ slot slot-number ]</td>
</tr>
<tr>
<td>Display interface PBR configuration and statistics (distributed devices in IRF mode).</td>
<td>display ip policy-based-route interface interface-type interface-number [ chassis chassis-number slot slot-number ]</td>
</tr>
<tr>
<td>Clear PBR statistics.</td>
<td>reset ip policy-based-route statistics [ policy policy-name ]</td>
</tr>
</tbody>
</table>

PBR configuration examples

Packet type-based local PBR configuration example

**Network requirements**

As shown in Figure 87, Router B and Router C cannot reach each other.

Configure PBR on Router A to forward all TCP packets to the next hop 1.1.2.2.
Configuration procedure

1. Configure Router A:
   
   # Configure the IP addresses of GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.
   
   <RouterA> system-view
   [RouterA] interface gigabitethernet 1/0/1
   [RouterA-GigabitEthernet1/0/1] ip address 1.1.2.1 24
   [RouterA-GigabitEthernet1/0/1] quit
   [RouterA] interface gigabitethernet 1/0/2
   [RouterA-GigabitEthernet1/0/2] ip address 1.1.3.1 24
   [RouterA-GigabitEthernet1/0/2] quit
   
   # Configure ACL 3101 to match TCP packets.
   [RouterA] acl advanced 3101
   [RouterA-acl-ipv4-adv-3101] rule permit tcp
   [RouterA-acl-ipv4-adv-3101] quit
   
   # Configure Node 5 for the policy aaa to forward TCP packets to next hop 1.1.2.2.
   [RouterA] policy-based-route aaa permit node 5
   [RouterA-pbr-aaa-5] if-match acl 3101
   [RouterA-pbr-aaa-5] apply next-hop 1.1.2.2
   [RouterA-pbr-aaa-5] quit
   
   # Configure local PBR by applying the policy aaa to Router A.
   [RouterA] ip local policy-based-route aaa

2. On Router B, configure the IP address of GigabitEthernet 1/0/1.
   
   <RouterB> system-view
   [RouterB] interface gigabitethernet 1/0/1
   [RouterB-GigabitEthernet1/0/1] ip address 1.1.2.2 24

3. On Router C, configure the IP address of GigabitEthernet 1/0/2.
   
   <RouterC> system-view
   [RouterC] interface gigabitethernet 1/0/2
   [RouterC-GigabitEthernet1/0/2] ip address 1.1.3.2 24

Verifying the configuration

# Telnet to Router B on Router A. The operation succeeds. (Details not shown.)
# Telnet to Router C on Router A. The operation fails. (Details not shown.)
# Ping Router C from Router A. The operation succeeds. (Details not shown.)

Telnet uses TCP, and ping uses ICMP. The results show the following:

- All TCP packets sent from Router A are forwarded to the next hop 1.1.2.2.
- Other packets are forwarded through GigabitEthernet 1/0/2.
- The local PBR configuration is effective.
Packet type-based interface PBR configuration example

Network requirements

As shown in Figure 88, Router B and Router C cannot reach each other.

Configure PBR on Router A to forward all TCP packets received on GigabitEthernet 1/0/1 to the next hop 1.1.2.2.

Figure 88 Network diagram

<table>
<thead>
<tr>
<th>Router B</th>
<th>Router C</th>
</tr>
</thead>
<tbody>
<tr>
<td>GE1/0/2</td>
<td>GE1/0/3</td>
</tr>
<tr>
<td>1.1.2.2/24</td>
<td>1.1.3.2/24</td>
</tr>
<tr>
<td>GE1/0/2</td>
<td>GE1/0/3</td>
</tr>
<tr>
<td>1.1.2.1/24</td>
<td>1.1.3.1/24</td>
</tr>
<tr>
<td>Router A</td>
<td></td>
</tr>
<tr>
<td>GE1/0/1</td>
<td></td>
</tr>
<tr>
<td>10.110.0.10/24</td>
<td></td>
</tr>
</tbody>
</table>

Host A

10.110.0.20/24
Gateway: 10.110.0.10

Configuration procedure

1. Make sure Router B and Router C can reach Host A. (Details not shown.)
2. Configure Router A:
   # Configure the IP addresses of GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3.
   <RouterA> system-view
   [RouterA] interface gigabitethernet 1/0/2
   [RouterA-GigabitEthernet1/0/2] ip address 1.1.2.1 24
   [RouterA-GigabitEthernet1/0/2] quit
   [RouterA] interface gigabitethernet 1/0/3
   [RouterA-GigabitEthernet1/0/3] ip address 1.1.3.1 24
   [RouterA-GigabitEthernet1/0/3] quit
   # Configure ACL 3101 to match TCP packets.
   [RouterA] acl advanced 3101
   [RouterA-acl-ipv4-adv-3101] rule permit tcp
   [RouterA-acl-ipv4-adv-3101] quit
   # Configure Node 5 for the policy aaa to forward TCP packets to next hop 1.1.2.2.
   [RouterA] policy-based-route aaa permit node 5
   [RouterA-pbr-aaa-5] if-match acl 3101
   [RouterA-pbr-aaa-5] apply next-hop 1.1.2.2
   [RouterA-pbr-aaa-5] quit
# Configure interface PBR by applying the policy aaa to GigabitEthernet 1/0/1.

[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] ip address 10.110.0.10 24
[RouterA-GigabitEthernet1/0/1] ip policy-based-route aaa
[RouterA-GigabitEthernet1/0/1] quit

Verifying the configuration

# On Host A, Telnet to Router B that is directly connected to Router A. The operation succeeds. (Details not shown.)
# On Host A, Telnet to Router C that is directly connected to Router A. The operation fails. (Details not shown.)
# Ping Router C from Host A. The operation succeeds. (Details not shown.)

Telnet uses TCP, and ping uses ICMP. The results show the following:

- All TCP packets arriving on GigabitEthernet 1/0/1 of Router A are forwarded to the next hop 1.1.2.2.
- Other packets are forwarded through GigabitEthernet 1/0/3.
- The interface PBR configuration is effective.

Packet length-based interface PBR configuration example

Network requirements

As shown in Figure 89, configure interface PBR to guide the forwarding of packets received on GigabitEthernet 1/0/1 of Router A as follows:

- Set the next hop of packets with a length of 64 to 300 bytes to 150.1.1.2/24.
- Set the next hop of packets with a length of 301 to 1000 bytes to 151.1.1.2/24.

Router A forwards other packets according to the routing table.

Figure 89 Network diagram

Configuration procedure

1. Configure Router A:

# Configure the IP addresses of GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3.

    <RouterA> system-view
    [RouterA] interface gigabitethernet 1/0/2
    [RouterA-GigabitEthernet1/0/2] ip address 150.1.1.1 24
    [RouterA-GigabitEthernet1/0/2] quit
    [RouterA] interface gigabitethernet 1/0/3
    [RouterA-GigabitEthernet1/0/3] ip address 151.1.1.1 24
# Configure RIP.
[RouterA] rip
[RouterA-rip-1] network 192.1.1.0
[RouterA-rip-1] network 150.1.0.0
[RouterA-rip-1] network 151.1.0.0
[RouterA-rip-1] quit

# Configure Node 10 for the policy lab1 to forward packets with a length of 64 to 300 bytes to the next hop 150.1.1.2.
[RouterA] policy-based-route lab1 permit node 10
[RouterA-pbr-lab1-10] if-match packet-length 64 300
[RouterA-pbr-lab1-10] apply next-hop 150.1.1.2
[RouterA-pbr-lab1-10] quit

# Configure Node 20 for the policy lab1 to forward packets with a length of 301 to 1000 bytes to the next hop 151.1.1.2.
[RouterA] policy-based-route lab1 permit node 20
[RouterA-pbr-lab1-20] if-match packet-length 301 1000
[RouterA-pbr-lab1-20] apply next-hop 151.1.1.2
[RouterA-pbr-lab1-20] quit

# Configure interface PBR by applying the policy lab1 to GigabitEthernet 1/0/1.
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] ip address 192.1.1.1 24
[RouterA-GigabitEthernet1/0/1] ip policy-based-route lab1
[RouterA-GigabitEthernet1/0/1] quit

2. Configure Router B:

# Configure the IP addresses of GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3.
<RouterB> system-view
[RouterB] interface gigabitethernet 1/0/2
[RouterB-GigabitEthernet1/0/2] ip address 150.1.1.2 24
[RouterB-GigabitEthernet1/0/2] quit
[RouterB] interface gigabitethernet 1/0/3
[RouterB-GigabitEthernet1/0/3] ip address 151.1.1.2 24
[RouterB-GigabitEthernet1/0/3] quit

# Configure the loopback interface address.
[RouterB] interface loopback 0
[RouterB-LoopBack0] ip address 10.1.1.1 32
[RouterB-LoopBack0] quit

# Configure RIP.
[RouterB] rip
[RouterB-rip-1] network 10.0.0.0
[RouterB-rip-1] network 150.1.0.0
[RouterB-rip-1] network 151.1.0.0
[RouterB-rip-1] quit

Verifying the configuration

# Execute the debugging ip policy-based-route command on Router A.
<RouterA> debugging ip policy-based-route
<RouterA> terminal logging level 7
<RouterA> terminal monitor

# Ping Loopback 0 of Router B from Host A, and set the data length to 64 bytes. In this way, the total length of the data packet is in the range of 64 to 300 bytes.
C:\> ping -n 1 -l 64 10.1.1.1

Pinging 10.1.1.1 with 64 bytes of data:

Reply from 10.1.1.1: bytes=64 time=1ms TTL=64

Ping statistics for 10.1.1.1:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

The debugging information about PBR displayed on Router A is as follows:
<RouterA>

The output shows that Router A sets the next hop for the received packets to 150.1.1.2 according to PBR. The packets are forwarded through GigabitEthernet 1/0/2.

# Ping Loopback 0 of Router B from Host A, and set the data length to 300 bytes. In this way, the total length of the data packet is in the range of 301 to 1000 bytes.
C:\> ping -n 1 -l 300 10.1.1.1

Pinging 10.1.1.1 with 300 bytes of data:

Reply from 10.1.1.1: bytes=300 time=1ms TTL=64

Ping statistics for 10.1.1.1:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

The debugging information about PBR displayed on Router A is as follows:
<RouterA>

The output shows that Router A sets the next hop for the received packets to 150.1.1.2 according to PBR. The packets are forwarded through GigabitEthernet 1/0/2.

Packet source-IP-based interface PBR configuration example

Network requirements

As shown in Figure 90, Router B and Router C cannot reach each other.
Configure interface PBR to guide the forwarding of packets received on GigabitEthernet 1/0/1 of Router A as follows:

- Set the next hop of packets sourced from 192.168.10.2 to 4.1.1.2/24.
- Set the next hop of other packets to 5.1.1.2/24.

**Figure 90 Network diagram**

Configuration procedure

1. Make sure Router B can reach Host A and Host B, and Router C can reach Host A and Host B. (Details not shown.)
2. Configure Router A:

   # Configure the IP addresses of GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3.
   ```
   <RouterA> system-view
   [RouterA] interface gigabitethernet 1/0/2
   [RouterA-GigabitEthernet1/0/2] ip address 4.1.1.1 24
   [RouterA-GigabitEthernet1/0/2] quit
   [RouterA] interface gigabitethernet 1/0/3
   [RouterA-GigabitEthernet1/0/3] ip address 5.1.1.1 24
   [RouterA-GigabitEthernet1/0/3] quit
   ```

   # Configure ACL 2000 to match packets sourced from 192.168.10.2.
   ```
   [RouterA] acl basic 2000
   [RouterA-acl-ipv4-basic-2000] rule 10 permit source 192.168.10.2 0
   [RouterA-acl-ipv4-basic-2000] quit
   ```

   # Configure Node 0 for the policy aaa to forward packets sourced from 192.168.10.2 to next hop 4.1.1.2. Configure Node 1 for the policy aaa to forward other packets to next hop 5.1.1.2.
   ```
   [RouterA] policy-based-route aaa permit node 0
   [RouterA-pbr-aaa-0] if-match acl 2000
   [RouterA-pbr-aaa-0] apply next-hop 4.1.1.2
   [RouterA-pbr-aaa-0] quit
   [RouterA] policy-based-route aaa permit node 1
   ```
[RouterA-pbr-aaa-1] apply next-hop 5.1.1.2
[RouterA-pbr-aaa-1] quit

# Configure interface PBR by applying the policy aaa to GigabitEthernet 1/0/1.
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] ip address 192.168.10.1 24
[RouterA-GigabitEthernet1/0/1] ip policy-based-route aaa
[RouterA-GigabitEthernet1/0/1] quit

Verifying the configuration

# Configure IP address 192.168.10.3/24 for Host B, and specify its gateway address as 192.168.10.1. (Details not shown.)
# Ping Router B from Host A. The operation succeeds. (Details not shown.)
# Ping Router B from Host B. The operation fails. (Details not shown.)
# Ping Router C from Host A. The operation fails. (Details not shown.)
# Ping Router C from Host B. The operation succeeds. (Details not shown.)

The results show the following:

- All packets sourced from 192.168.10.2 are forwarded to the next hop 4.1.1.2.
- Packets sourced from 192.168.10.3 are forwarded to the next hop 5.1.1.2.
- The interface PBR configuration is effective.
# Configuring IPv6 static routing

Static routes are manually configured and cannot adapt to network topology changes. If a fault or a topological change occurs in the network, the network administrator must modify the static routes manually. IPv6 static routing works well in a simple IPv6 network.

## Configuring an IPv6 static route

Before you configure an IPv6 static route, complete the following tasks:

- Configure parameters for the related interfaces.
- Configure link layer attributes for the related interfaces.
- Make sure the neighboring nodes can reach each other.

To configure an IPv6 static route:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure an IPv6 static route.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Method 1:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>`ipv6 route-static ipv6-address prefix-length { interface-type interface-number</td>
<td>next-hop-address }</td>
</tr>
<tr>
<td></td>
<td>Method 2:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>`ipv6 route-static vpn-instance s-vpn-instance-name ipv6-address prefix-length { interface-type interface-number</td>
<td>next-hop-address }</td>
</tr>
<tr>
<td>3.</td>
<td>(Optional.) Set the default preference for IPv6 static routes.</td>
<td><code>ipv6 route-static default-preference default-preference</code></td>
</tr>
<tr>
<td>4.</td>
<td>(Optional.) Delete all IPv6 static routes, including the default route.</td>
<td><code>delete ipv6 [ vpn-instance vpn-instance-name ] static-routes all</code></td>
</tr>
</tbody>
</table>

## Configuring BFD for IPv6 static routes

BFD provides a general purpose, standard, and medium- and protocol-independent fast failure detection mechanism. It can uniformly and quickly detect the failures of the bidirectional forwarding paths between two routers for protocols, such as routing protocols and MPLS. For more information about BFD, see *High Availability Configuration Guide*.

**IMPORTANT:**

Enabling BFD for a flapping route could worsen the situation.
Bidirectional control mode

To use BFD bidirectional control detection between two devices, enable BFD control mode for each device’s static route destined to the peer.

To configure a static route and enable BFD control mode, use one of the following methods:
- Specify an output interface and a direct next hop.
- Specify an indirect next hop and a BFD packet source address for the static route.

To configure BFD control mode for an IPv6 static route (direct next hop):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure BFD control mode for an IPv6 static route.</td>
<td>ipv6 route-static [ vpn-instance s-vpn-instance-name ] ipv6-address prefix-length interface-type interface-number next-hop-address bfd control-packet bfd-source ipv6-address [ preference preference ] [ tag tag-value ] [ description text ]</td>
</tr>
</tbody>
</table>

To configure BFD control mode for an IPv6 static route (indirect next hop):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure BFD control mode for an IPv6 static route.</td>
<td>ipv6 route-static [ vpn-instance s-vpn-instance-name ] ipv6-address prefix-length [ vpn-instance d-vpn-instance-name ] [ next-hop-address bfd control-packet bfd-source ipv6-address ] [ preference preference ] [ tag tag-value ] [ description text ]</td>
</tr>
</tbody>
</table>

Single-hop echo mode

With BFD echo mode enabled for a static route, the output interface sends BFD echo packets to the destination device, which loops the packets back to test the link reachability.

⚠️ IMPORTANT: Do not use BFD for a static route with the output interface in spoofing state.

To configure BFD echo mode for an IPv6 static route:
### Step Command Remarks

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
<tr>
<td>2. Configure the source address of echo packets.</td>
<td><code>bfd echo-source-ipv6 ipv6-address</code></td>
<td>By default, the source address of echo packets is not configured. The source address of echo packets must be a global unicast address. For more information about this command, see High Availability Command Reference.</td>
</tr>
<tr>
<td>3. Configure BFD echo mode for an IPv6 static route.</td>
<td><code>ipv6 route-static [ vpn-instance s-vpn-instance-name ] ipv6-address prefix-length interface-type interface-number next-hop-address bfd echo-packet [ bfd-source ipv6-address ] [ preference preference ] [ tag tag-value ] [ description text ]</code></td>
<td>By default, BFD echo mode for an IPv6 static route is not configured. The next hop IPv6 address must be a global unicast address.</td>
</tr>
</tbody>
</table>

### Displaying and maintaining IPv6 static routes

Execute `display` commands in any view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display IPv6 static route information.</td>
<td>`display ipv6 routing-table protocol static [ inactive</td>
</tr>
<tr>
<td>Display IPv6 static route next hop information.</td>
<td><code>display ipv6 route-static nib [ nib-id ] [ verbose ]</code></td>
</tr>
<tr>
<td>Display IPv6 static routing table information.</td>
<td><code>display ipv6 route-static routing-table [ vpn-instance vpn-instance-name ] [ ipv6-address prefix-length ]</code></td>
</tr>
</tbody>
</table>

### IPv6 static routing configuration examples

**Basic IPv6 static route configuration example**

**Network requirements**

As shown in Figure 91, configure IPv6 static routes so that hosts can reach each other.
Configuration procedure

1. Configure IPv6 addresses for interfaces. (Details not shown.)
2. Configure IPv6 static routes:
   # Configure the default IPv6 route on Router A.
   <RouterA> system-view
   [RouterA] ipv6 route-static :: 0 4::2
   # Configure two IPv6 static routes on Router B.
   <RouterB> system-view
   [RouterB] ipv6 route-static 1:: 64 4::1
   [RouterB] ipv6 route-static 3:: 64 5::1
   # Configure the default IPv6 route on Router C.
   <RouterC> system-view
   [RouterC] ipv6 route-static :: 0 5::2
3. Configure the IPv6 addresses for all hosts and configure the default gateway of Host A, Host B, and Host C as 1::1, 2::1, and 3::1.

Verifying the configuration

# Display the IPv6 static route information on Router A.
 [RouterA] display ipv6 routing-table protocol static
Summary Count : 1
Static Routing table Status : <Active>
Summary Count : 1

Destination: :: Protocol : Static
NextHop : 4::2 Preference: 60
Interface : GE1/0/2 Cost : 0

Static Routing table Status : <Inactive>
Summary Count : 0
# Display the IPv6 static route information on Router B.
 [RouterB] display ipv6 routing-table protocol static
Summary Count : 2

Static Routing table Status : <Active>
Summary Count : 2

Destination: 1::/64                                      Protocol  : Static
NextHop    : 4::1                                        Preference: 60
Interface  : GE1/0/1                                     Cost      : 0

Destination: 3::/64                                      Protocol  : Static
NextHop    : 5::1                                        Preference: 60
Interface  : GE1/0/2                                     Cost      : 0

Static Routing table Status : <Inactive>
Summary Count : 0

# Use the ping command to test reachability.

[RouterA] ping ipv6 3::1
Ping6(56 data bytes) 4::1 --> 3::1, press CTRL_C to break
56 bytes from 3::1, icmp_seq=0 hlim=62 time=0.700 ms
56 bytes from 3::1, icmp_seq=1 hlim=62 time=0.351 ms
56 bytes from 3::1, icmp_seq=2 hlim=62 time=0.338 ms
56 bytes from 3::1, icmp_seq=3 hlim=62 time=0.373 ms
56 bytes from 3::1, icmp_seq=4 hlim=62 time=0.316 ms

--- Ping6 statistics for 3::1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.316/0.416/0.700/0.143 ms

BFD for IPv6 static routes configuration example (direct next hop)

Network requirements

As shown in Figure 92:

- Configure an IPv6 static route to subnet 120::/64 on Router A.
- Configure an IPv6 static route to subnet 121::/64 on Router B.
- Enable BFD for both routes.
- Configure an IPv6 static route to subnet 120::/64 and an IPv6 static route to subnet 121::/64 on Router C.

When the link between Router A and Router B through the Layer 2 switch fails, BFD can detect the failure immediately and inform Router A and Router B to communicate through Router C.
Table 20 Interface and IP address assignment

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IPv6 address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router A</td>
<td>GE1/0/1</td>
<td>12::1/64</td>
</tr>
<tr>
<td>Router A</td>
<td>GE1/0/2</td>
<td>10::102/64</td>
</tr>
<tr>
<td>Router B</td>
<td>GE1/0/1</td>
<td>12::2/64</td>
</tr>
<tr>
<td>Router B</td>
<td>GE1/0/2</td>
<td>13::1/64</td>
</tr>
<tr>
<td>Router C</td>
<td>GE1/0/1</td>
<td>10::100/64</td>
</tr>
<tr>
<td>Router C</td>
<td>GE1/0/2</td>
<td>13::2/64</td>
</tr>
</tbody>
</table>

Configuration procedure

1. Configure IPv6 addresses for interfaces. (Details not shown.)
2. Configure IPv6 static routes and BFD:

   # Configure IPv6 static routes on Router A, and enable BFD control mode for the IPv6 static route that traverses GigabitEthernet 1/0/1.
   <RouterA> system-view
   [RouterA] interface gigabitethernet 1/0/1
   [RouterA-GigabitEthernet1/0/1] bfd min-transmit-interval 500
   [RouterA-GigabitEthernet1/0/1] bfd min-receive-interval 500
   [RouterA-GigabitEthernet1/0/1] bfd detect-multiplier 9
   [RouterA-GigabitEthernet1/0/1] quit
   [RouterA] ipv6 route-static 120:: 64 gigabitethernet 1/0/1 12::2 bfd control-packet
   [RouterA] ipv6 route-static 120:: 64 10::100 preference 65
   [RouterA] quit

   # Configure IPv6 static routes on Router B, and enable BFD control mode for the IPv6 static route that traverses the Layer 2 switch.
   <RouterB> system-view
   [RouterB] interface gigabitethernet 1/0/1
   [RouterB-GigabitEthernet1/0/1] bfd min-transmit-interval 500
   [RouterB-GigabitEthernet1/0/1] bfd min-receive-interval 500
   [RouterB-GigabitEthernet1/0/1] bfd detect-multiplier 9
   [RouterB-GigabitEthernet1/0/1] quit
   [RouterB] ipv6 route-static 121:: 64 gigabitethernet 1/0/1 12::1 bfd control-packet
   [RouterB] ipv6 route-static 121:: 64 13::2 preference 65
   [RouterB] quit

   # Configure IPv6 static routes on Router C.
Verifying the configuration

# Display BFD sessions on Router A.
<RouterA> display bfd session

Total Session Num: 1    Up Session Num: 1    Init Mode: Active

IPv6 Session Working Under Ctrl Mode:

<table>
<thead>
<tr>
<th>Local Discr: 513</th>
<th>Remote Discr: 33</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP: 12::1</td>
<td></td>
</tr>
<tr>
<td>Destination IP: 12::2</td>
<td></td>
</tr>
<tr>
<td>Session State: Up</td>
<td>Interface: GE1/0/1</td>
</tr>
<tr>
<td>Hold Time: 2012ms</td>
<td></td>
</tr>
</tbody>
</table>

The output shows that the BFD session has been created.

# Display IPv6 static routes on Router A.
<RouterA> display ipv6 routing-table protocol static

Summary Count : 1

Static Routing table Status : <Active>
Summary Count : 1

<table>
<thead>
<tr>
<th>Destination: 120::/64</th>
<th>Protocol : Static</th>
</tr>
</thead>
<tbody>
<tr>
<td>NextHop : 12::2</td>
<td>Preference: 60</td>
</tr>
<tr>
<td>Interface : GE1/0/1</td>
<td>Cost : 0</td>
</tr>
</tbody>
</table>

Static Routing table Status : <Inactive>
Summary Count : 0

The output shows that Router A communicates with Router B through GigabitEthernet 1/0/1. The link over GigabitEthernet 1/0/1 fails.

# Display IPv6 static routes on Router A.
<RouterA> display ipv6 routing-table protocol static

Summary Count : 1

Static Routing table Status : <Active>
Summary Count : 1

<table>
<thead>
<tr>
<th>Destination: 120::/64</th>
<th>Protocol : Static</th>
</tr>
</thead>
<tbody>
<tr>
<td>NextHop : 10::100</td>
<td>Preference: 65</td>
</tr>
<tr>
<td>Interface : GE1/0/2</td>
<td>Cost : 0</td>
</tr>
</tbody>
</table>

Static Routing table Status : <Inactive>
Summary Count : 0
The output shows that Router A communicates with Router B through GigabitEthernet 1/0/2.

BFD for IPv6 static routes configuration example (indirect next hop)

Network requirements

As shown in Figure 93:
- Router A has a route to interface Loopback 1 (2::9/128) on Router B, and the output interface is GigabitEthernet 1/0/1.
- Router B has a route to interface Loopback 1 (1::9/128) on Router A, and the output interface is GigabitEthernet 1/0/1.
- Router D has a route to 1::9/128, and the output interface is GigabitEthernet 1/0/1. It also has a route to 2::9/128, and the output interface is GigabitEthernet 1/0/2.

Configure the following:
- Configure an IPv6 static route to subnet 120::/64 on Router A.
- Configure an IPv6 static route to subnet 121::/64 on Router B.
- Enable BFD for both routes.
- Configure an IPv6 static route to subnet 120::/64 and an IPv6 static route to subnet 121::/64 on both Router C and Router D.

When the link between Router A and Router B through Router D fails, BFD can detect the failure immediately and Router A and Router B can communicate through Router C.

Figure 93 Network diagram

Table 21 Interface and IP address assignment

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IPv6 address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router A</td>
<td>GE1/0/1</td>
<td>12::1/64</td>
</tr>
<tr>
<td>Router A</td>
<td>GE1/0/2</td>
<td>10::102/64</td>
</tr>
<tr>
<td>Router A</td>
<td>Loop1</td>
<td>1::9/128</td>
</tr>
<tr>
<td>Router B</td>
<td>GE1/0/1</td>
<td>11::2/64</td>
</tr>
<tr>
<td>Router B</td>
<td>GE1/0/2</td>
<td>13::1/64</td>
</tr>
<tr>
<td>Router B</td>
<td>Loop1</td>
<td>2::9/128</td>
</tr>
<tr>
<td>Router C</td>
<td>GE1/0/1</td>
<td>10::100/64</td>
</tr>
<tr>
<td>Router C</td>
<td>GE1/0/2</td>
<td>13::2/64</td>
</tr>
</tbody>
</table>
Device Interface IPv6 address
---
Router D GE1/0/1 12::2/64
Router D GE1/0/2 11::1/64

Configuration procedure

1. Configure IPv6 addresses for interfaces. (Details not shown.)
2. Configure IPv6 static routes and BFD:

   # Configure IPv6 static routes on Router A and enable BFD control packet mode for the IPv6 static route that traverses Router D.
   <RouterA> system-view
   [RouterA] bfd multi-hop min-transmit-interval 500
   [RouterA] bfd multi-hop min-receive-interval 500
   [RouterA] bfd multi-hop detect-multiplier 9
   [RouterA] ipv6 route-static 120:: 64 2::9 bfd control-packet bfd-source 1::9
   [RouterA] ipv6 route-static 120:: 64 10::100 preference 65
   [RouterA] ipv6 route-static 2::9 128 12::2
   [RouterA] quit

   # Configure IPv6 static routes on Router B and enable BFD control mode for the IPv6 static route that traverses Router D.
   <RouterB> system-view
   [RouterB] bfd multi-hop min-transmit-interval 500
   [RouterB] bfd multi-hop min-receive-interval 500
   [RouterB] bfd multi-hop detect-multiplier 9
   [RouterB] ipv6 route-static 121:: 64 1::9 bfd control-packet bfd-source 2::9
   [RouterB] ipv6 route-static 121:: 64 13::2 preference 65
   [RouterB] ipv6 route-static 1::9 128 11::1
   [RouterB] quit

   # Configure IPv6 static routes on Router C.
   <RouterC> system-view
   [RouterC] ipv6 route-static 120:: 64 13::1
   [RouterC] ipv6 route-static 121:: 64 10::102

   # Configure IPv6 static routes on Router D.
   <RouterD> system-view
   [RouterD] ipv6 route-static 120:: 64 11::2
   [RouterD] ipv6 route-static 121:: 64 12::1
   [RouterD] ipv6 route-static 2::9 128 11::2
   [RouterD] ipv6 route-static 1::9 128 12::1

Verifying the configuration

# Display BFD sessions on Router A.
<RouterA> display bfd session

Total Session Num: 1 Up Session Num: 1 Init Mode: Active

IPv6 Session Working Under Ctrl Mode:

<table>
<thead>
<tr>
<th>Local Discr: 513</th>
<th>Remote Discr: 33</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP: 1:9</td>
<td></td>
</tr>
</tbody>
</table>
The output shows that the BFD session has been created.

# Display IPv6 static routes on Router A.

```bash
<RouterA> display ipv6 routing-table protocol static
```

Summary Count : 1

Static Routing table Status : <Active>
Summary Count : 1

<table>
<thead>
<tr>
<th>Destination: 120::/64</th>
<th>Protocol : Static</th>
</tr>
</thead>
<tbody>
<tr>
<td>NextHop : 2::9</td>
<td>Preference: 60</td>
</tr>
<tr>
<td>Interface : GE1/0/1</td>
<td>Cost : 0</td>
</tr>
</tbody>
</table>

Static Routing table Status : <Inactive>
Summary Count : 0

The output shows that Router A communicates with Router B through GigabitEthernet 1/0/1. The link over GigabitEthernet 1/0/1 fails.

# Display IPv6 static routes on Router A.

```bash
<RouterA> display ipv6 routing-table protocol static
```

Summary Count : 1

Static Routing table Status : <Active>
Summary Count : 1

<table>
<thead>
<tr>
<th>Destination: 120::/64</th>
<th>Protocol : Static</th>
</tr>
</thead>
<tbody>
<tr>
<td>NextHop : 10::100</td>
<td>Preference: 65</td>
</tr>
<tr>
<td>Interface : GE1/0/2</td>
<td>Cost : 0</td>
</tr>
</tbody>
</table>

Static Routing table Status : <Inactive>
Summary Count : 0

The output shows that Router A communicates with Router B through GigabitEthernet 1/0/2.
Configuring an IPv6 default route

A default IPv6 route is used to forward packets that match no entry in the routing table.

A default IPv6 route can be configured in either of the following ways:

- The network administrator can configure a default route with a destination prefix of ::/0. For more information, see "Configuring an IPv6 static route."

- Some dynamic routing protocols, such as OSPFv3, IPv6 IS-IS, and RIPng, can generate a default IPv6 route. For example, an upstream router running OSPFv3 can generate a default IPv6 route and advertise it to other routers. These routers install the default IPv6 route with the next hop being the upstream router. For more information, see the respective chapters on those routing protocols in this configuration guide.
Configuring RIPng

Overview

RIP next generation (RIPng) is an extension of RIP-2 for support of IPv6. Most RIP concepts are applicable to RIPng.

RIPng is a distance vector routing protocol. It employs UDP to exchange route information through port 521. RIPng uses a hop count to measure the distance to a destination. The hop count is the metric or cost. The hop count from a router to a directly connected network is 0. The hop count between two directly connected routers is 1. When the hop count is greater than or equal to 16, the destination network or host is unreachable.

By default, the routing update is sent every 30 seconds. If the router receives no routing updates from a neighbor within 180 seconds, the routes learned from the neighbor are considered unreachable. If no routing update is received within another 240 seconds, the router removes these routes from the routing table.

RIPng for IPv6 has the following differences from RIP:
- **UDP port number**—RIPng uses UDP port 521 to send and receive routing information.
- **Multicast address**—RIPng uses FF02::9 as the link-local-router multicast address.
- **Destination Prefix**—128-bit destination address prefix.
- **Next hop**—128-bit IPv6 address.
- **Source address**—RIPng uses FE80::/10 as the link-local source address.

RIPng route entries

RIPng stores route entries in a database. Each route entry contains the following elements:
- **Destination address**—IPv6 address of a destination host or a network.
- **Next hop address**—IPv6 address of the next hop.
- **Egress interface**—Egress interface of the route.
- **Metric**—Cost from the local router to the destination.
- **Route time**—Time elapsed since the most recent update. The time is reset to 0 every time the route entry is updated.
- **Route tag**—Used for route control. For more information, see "Configuring routing policies."

RIPng packets

RIPng uses request and response packets to exchange routing information as follows:

1. When RIPng starts or needs to update some route entries, it sends a multicast request packet to neighbors.
2. When a RIPng neighbor receives the request packet, it sends back a response packet that contains the local routing table. RIPng can also advertise route updates in response packets periodically or advertise a triggered update caused by a route change.
3. After RIPng receives the response, it checks the validity of the response before adding routes to its routing table, including the following details:
   - Whether the source IPv6 address is the link-local address.
   - Whether the port number is correct.
4. A response packet that fails the check is discarded.

Protocols and standards

- RFC 2080, RIPvng for IPv6
- RFC 2081, RIPvng Protocol Applicability Statement

### RIPvng configuration task list

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Required.) Configuring basic RIPvng</td>
</tr>
<tr>
<td>(Optional.) Configuring RIPvng route control:</td>
</tr>
<tr>
<td>Configuring an additional routing metric</td>
</tr>
<tr>
<td>Configuring RIPvng route summarization</td>
</tr>
<tr>
<td>Advertising a default route</td>
</tr>
<tr>
<td>Configuring received/redistributed route filtering</td>
</tr>
<tr>
<td>Setting a preference for RIPvng</td>
</tr>
<tr>
<td>Configuring RIPvng route redistribution</td>
</tr>
<tr>
<td>(Optional.) Tuning and optimizing the RIPvng network:</td>
</tr>
<tr>
<td>Setting RIPvng timers</td>
</tr>
<tr>
<td>Configuring split horizon and poison reverse</td>
</tr>
<tr>
<td>Configuring zero field check on RIPvng packets</td>
</tr>
<tr>
<td>Setting the maximum number of ECMP routes</td>
</tr>
<tr>
<td>Configuring the RIPvng packet sending rate</td>
</tr>
<tr>
<td>Setting the interval for sending triggered updates</td>
</tr>
<tr>
<td>(Optional.) Configuring RIPvng GR</td>
</tr>
<tr>
<td>(Optional.) Configuring RIPvng NSR</td>
</tr>
<tr>
<td>(Optional.) Configuring RIPvng FRR</td>
</tr>
<tr>
<td>(Optional.) Applying an IPsec profile</td>
</tr>
</tbody>
</table>

### Configuring basic RIPvng

Before you configure basic RIPvng, configure IPv6 addresses for interfaces to ensure IPv6 connectivity between neighboring nodes.

To configure basic RIPvng:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable RIPvng and enter its view.</td>
<td>ripng [ process-id ] [ vpn-instance vpn-instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Return to system view.</td>
<td>quit</td>
</tr>
<tr>
<td>4.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
</tbody>
</table>
### Configuring RIPv6 route control

Before you configure RIPv6, complete the following tasks:
- Configure IPv6 addresses for interfaces to ensure IPv6 connectivity between neighboring nodes.
- Configure basic RIPv6.

### Configuring an additional routing metric

An additional routing metric (hop count) can be added to the metric of an inbound or outbound RIPv6 route.

An outbound additional metric is added to the metric of a sent route, and it does not change the route's metric in the routing table.

An inbound additional metric is added to the metric of a received route before the route is added into the routing table, and the route's metric is changed.

To configure an inbound or outbound additional routing metric:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>ripng metricin value</td>
<td>The default setting is 0.</td>
</tr>
<tr>
<td>4.</td>
<td>ripng metricout value</td>
<td>The default setting is 1.</td>
</tr>
</tbody>
</table>

### Configuring RIPv6 route summarization

Configure route summarization on an interface, so RIPv6 advertises a summary route based on the longest match.

RIPv6 route summarization improves network scalability, reduces routing table size, and increases routing table lookup efficiency.

RIPv6 advertises a summary route with the smallest metric of all the specific routes.

For example, RIPv6 has two specific routes to be advertised through an interface: 1:11:11::24 with a metric of 2 and 1:11:12::34 with a metric of 3. Configure route summarization on the interface, so RIPv6 advertises a single route 11::0/16 with a metric of 2.

To configure RIPv6 route summarization:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.</td>
<td>Enable RIPv6 on the interface.</td>
<td>ripng process-id enable</td>
</tr>
</tbody>
</table>
### Advertising a default route

You can configure RIPng to advertise a default route with the specified cost to its neighbors.

To configure RIPng to advertise a default route:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>ripng default-route { only</td>
<td>originate } [ cost cost-value</td>
</tr>
</tbody>
</table>

### Configuring received/redistributed route filtering

Perform this task to filter received or redistributed routes by using an IPv6 ACL or IPv6 prefix list. You can also configure RIPng to filter routes redistributed from other routing protocols and routes from a specified neighbor.

To configure a RIPng route filtering policy:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>ripng [ process-id ] [ vpn-instance vpn-instance-name ]</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>filter-policy { ipv6-acl-number</td>
<td>prefix-list prefix-list-name } import</td>
</tr>
<tr>
<td>4.</td>
<td>filter-policy { ipv6-acl-number</td>
<td>prefix-list prefix-list-name } export [ protocol [ process-id ] ]</td>
</tr>
</tbody>
</table>

### Setting a preference for RIPng

Routing protocols each have a preference. When they find routes to the same destination, the route found by the routing protocol with the highest preference is selected as the optimal route. You can manually set a preference for RIPng. The smaller the value, the higher the preference.

To set a preference for RIPng:
### Configuring RIPng route redistribution

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter RIPng view.</td>
<td>ripng [ process-id ] [ vpn-instance vpn-instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Set a preference for RIPng.</td>
<td>preference { preference</td>
</tr>
<tr>
<td>4.</td>
<td>(Optional.) Set a default routing metric for redistributed routes.</td>
<td>default cost cost-value</td>
</tr>
</tbody>
</table>

### Tuning and optimizing the RIPng network

This section describes how to tune and optimize the performance of the RIPng network as well as applications under special network environments.

Before you tune and optimize the RIPng network, complete the following tasks:

- Configure IPv6 addresses for interfaces to ensure IPv6 connectivity between neighboring nodes.
- Configure basic RIPng.

### Setting RIPng timers

You can adjust RIPng timers to optimize the performance of the RIPng network.

When you adjust RIPng timers, consider the network performance, and perform unified configurations on routers running RIPng to avoid unnecessary network traffic or route oscillation.

To set RIPng timers:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter RIPng view.</td>
<td>ripng [ process-id ] [ vpn-instance vpn-instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Set RIPng timers.</td>
<td>timers { garbage-collect }</td>
</tr>
</tbody>
</table>
Configuring split horizon and poison reverse

If both split horizon and poison reverse are configured, only the poison reverse function takes effect.

**Configuring split horizon**

Split horizon disables RIPng from sending routes through the interface where the routes were learned to prevent routing loops between neighbors.

As a best practice, enable split horizon to prevent routing loops in normal cases.

To configure split horizon:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface interface-type</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface-number</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ripng split-horizon</td>
<td>By default, split horizon is enabled.</td>
</tr>
</tbody>
</table>

**Configuring poison reverse**

Poison reverse enables a route learned from an interface to be advertised through the interface. However, the metric of the route is set to 16, which means the route is unreachable.

To configure poison reverse:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface interface-type</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface-number</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ripng poison-reverse</td>
<td>By default, poison reverse is disabled.</td>
</tr>
</tbody>
</table>

**Configuring zero field check on RIPng packets**

Some fields in the RIPng packet header must be zero. These fields are called zero fields. You can enable zero field check on incoming RIPng packets. If a zero field of a packet contains a non-zero value, RIPng does not process the packets. If you are certain that all packets are trustworthy, disable the zero field check to save CPU resources.

To configure RIPng zero field check:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>N/A</td>
</tr>
</tbody>
</table>
### Setting the maximum number of ECMP routes

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter RIPng view.</td>
<td>ripng [ process-id ] [ vpn-instance vpn-instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Set the maximum number of ECMP routes.</td>
<td>maximum load-balancing number</td>
</tr>
</tbody>
</table>

### Configuring the RIPng packet sending rate

Perform this task to specify the interval for sending RIPng packets and the maximum number of RIPng packets that can be sent at each interval. This feature can avoid excessive RIPng packets from affecting system performance and consuming too much bandwidth.

To configure the RIPng packet sending rate:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter RIPng view.</td>
<td>ripng [ process-id ] [ vpn-instance vpn-instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Set the interval for sending RIPng packets and the maximum number of RIPng packets that can be sent at each interval.</td>
<td>output-delay time count</td>
</tr>
<tr>
<td>4.</td>
<td>Return to system view.</td>
<td>quit</td>
</tr>
<tr>
<td>5.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>6.</td>
<td>Set the interval for sending RIPng packets and the maximum number of RIPng packets that can be sent at each interval.</td>
<td>ripng output-delay time count</td>
</tr>
</tbody>
</table>

### Setting the interval for sending triggered updates

Perform this task to avoid network overhead and reduce system resource consumption caused by frequent RIPng triggered updates.
You can use the `timer triggered` command to set the maximum interval, minimum interval, and incremental interval for sending RIPng triggered updates.

For a stable network, the minimum interval is used. If network changes become frequent, the triggered update sending interval is incremented by the incremental interval × $2^{n-2}$ for each triggered update until the maximum interval is reached. The value $n$ is the number of triggered update times.

To set the interval for sending triggered updates:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter RIPng view.</td>
<td>ripng [ process-id ] [ vpn-instance vpn-instance-name ]</td>
</tr>
</tbody>
</table>
| 3.   | Set the interval for sending triggered updates. | timer triggered maximum-interval [ minimum-interval [ incremental-interval ] ] | By default:  
• The maximum interval is 5 seconds.  
• The minimum interval is 50 milliseconds.  
• The incremental interval is 200 milliseconds. |

## Configuring RIPng GR

GR ensures forwarding continuity when a routing protocol restarts or an active/standby switchover occurs.

Two routers are required to complete a GR process. The following are router roles in a GR process:

- **GR restarter**—Graceful restarting router. It must have GR capability.
- **GR helper**—A neighbor of the GR restarter. It helps the GR restarter to complete the GR process.

After RIPng restarts on a router, the router must learn RIPng routes again and updates its FIB table, which causes network disconnections and route reconvergence.

With the GR feature, the restarting router (known as the GR restarter) can notify the event to its GR capable neighbors. GR capable neighbors (known as GR helpers) maintain their adjacencies with the router within a configurable GR interval. During this process, the FIB table of the router does not change. After the restart, the router contacts its neighbors to retrieve its FIB.

By default, a RIPng-enabled device acts as the GR helper. Perform this task on the GR restarter.

---

**IMPORTANT:**

You cannot enable RIPng NSR on a device that acts as GR restarter.

To configure GR on the GR restarter:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable RIPng and enter RIPng view.</td>
<td>ripng [ process-id ] [ vpn-instance vpn-instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Enable the GR capability for RIPng.</td>
<td>graceful-restart</td>
</tr>
<tr>
<td>4.</td>
<td>(Optional.) Set the GR</td>
<td>graceful-restart interval interval</td>
</tr>
</tbody>
</table>
Configuring RIPng NSR

The following matrix shows the feature and hardware compatibility:

<table>
<thead>
<tr>
<th>Hardware</th>
<th>BootWare image preload compatibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSR954(JH296A/JH297A/JH298A/JH299A/JH373A)</td>
<td>No</td>
</tr>
<tr>
<td>MSR958(JH300A/JH301A)</td>
<td>No</td>
</tr>
<tr>
<td>MSR1002-4/1003-8S</td>
<td>In standalone mode: No</td>
</tr>
<tr>
<td></td>
<td>In IRF mode: Yes</td>
</tr>
<tr>
<td>MSR2003</td>
<td>In standalone mode: No</td>
</tr>
<tr>
<td></td>
<td>In IRF mode: Yes</td>
</tr>
<tr>
<td>MSR2004-24/2004-48</td>
<td>In standalone mode: No</td>
</tr>
<tr>
<td></td>
<td>In IRF mode: Yes</td>
</tr>
<tr>
<td>MSR3012/3024/3044/3064</td>
<td>In standalone mode: No</td>
</tr>
<tr>
<td></td>
<td>In IRF mode: Yes</td>
</tr>
<tr>
<td>MSR4060/4080</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Nonstop routing (NSR) backs up RIPng routing information from the active process to the standby process. After an active/standby switchover, NSR can complete route regeneration without tearing down adjacencies or impacting forwarding services.

NSR does not require the cooperation of neighboring devices to recover routing information, and it is typically used more often than GR.

**IMPORTANT:**

A device that has RIPng NSR enabled cannot act as GR restarter.

To enable RIPng NSR:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>sys tem-view N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter RIPng view.</td>
<td>ripng [ process-id ] [ vpn-instance vpn-instance-name ] N/A</td>
</tr>
<tr>
<td>3.</td>
<td>Enable RIPng NSR.</td>
<td>non-stop-routing</td>
</tr>
</tbody>
</table>

By default, RIPng NSR is disabled. RIPng NSR enabled for a RIPng process takes effect only on that process. As a best practice, enable RIPng NSR for each process if multiple RIPng processes exist.
Configuring RIPng FRR

A link or router failure on a path can cause packet loss and even routing loop until RIPng completes routing convergence based on the new network topology. FRR enables fast rerouting to minimize the impact of link or node failures.

Figure 94 Network diagram for RIPng FRR

As shown in Figure 94, configure FRR on Router B by using a routing policy to specify a backup next hop. When the primary link fails, RIPng directs packets to the backup next hop. At the same time, RIPng calculates the shortest path based on the new network topology. Then, the device forwards packets over that path after network convergence.

Configuration restrictions and guidelines

- RIPng FRR is available only when the state of the primary link (with Layer 3 interfaces staying up) changes from bidirectional to unidirectional or down.
- RIPng FRR is only effective for RIPng routes that are learned from directly connected neighbors.
- Equal-cost routes do not support RIPng FRR.

Configuration prerequisites

You must specify a next hop by using the apply ipv6 fast-reroute backup-interface command in a routing policy and reference the routing policy for FRR. For more information about routing policy configuration, see "Configuring routing policies."

Configuration procedure

Configuring RIPng FRR

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>ripng [ process-id ] [ vpn-instance vpn-instance-name ]</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>fast-reroute route-policy route-policy-name</td>
<td>By default, RIPng FRR is disabled.</td>
</tr>
</tbody>
</table>

Enabling BFD for RIPng FRR

By default, RIPng FRR does not use BFD to detect primary link failures. To speed up RIPng convergence, enable BFD single-hop echo detection for RIPng FRR to detect primary link failures.

To configure BFD for RIPng FRR:
Applying an IPsec profile

To protect routing information and prevent attacks, RIPng supports using an IPsec profile to authenticate protocol packets. For more information about IPsec profiles, see Security Configuration Guide.

Outbound RIPng packets carry the Security Parameter Index (SPI) defined in the relevant IPsec profile. A device compares the SPI carried in a received packet with the configured IPsec profile. If they match, the device accepts the packet. If they do not match, the device discards the packet and does not establish a neighbor relationship with the sending device.

You can configure an IPsec profile for a RIPng process or interface. The IPsec profile configured for a process applies to all packets in the process. The IPsec profile configured for an interface applies to packets on the interface. If an interface and its process each have an IPsec profile configured, the interface uses its own IPsec profile.

To apply an IPsec profile to a process:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter RIPng view.</td>
<td>ripng [ process-id ] [ vpn-instance vpn-instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Apply an IPsec profile to the process.</td>
<td>enable ipsec-profile profile-name</td>
</tr>
</tbody>
</table>

To apply an IPsec profile to an interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Apply an IPsec profile to the interface.</td>
<td>ripng ipsec-profile profile-name</td>
</tr>
</tbody>
</table>
Displaying and maintaining RIPng

Execute `display` commands in any view and `reset` commands in user view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display configuration information for a RIPng process.</td>
<td><code>display ripng [ process-id ]</code></td>
</tr>
<tr>
<td>Display routes in the RIPng database.</td>
<td><code>display ripng process-id database [ ipv6-address prefix-length ]</code></td>
</tr>
<tr>
<td>Display RIPng GR information.</td>
<td><code>display ripng [ process-id ] graceful-restart</code></td>
</tr>
<tr>
<td>Display interface information for a RIPng process.</td>
<td><code>display ripng process-id interface [ interface-type interface-number ]</code></td>
</tr>
<tr>
<td>Display neighbor information for a RIPng process.</td>
<td><code>display ripng process-id neighbor [ interface-type interface-number ]</code></td>
</tr>
<tr>
<td>Display RIPng NSR information.</td>
<td><code>display ripng [ process-id ] non-stop-routing</code></td>
</tr>
<tr>
<td>Display the routing information for a RIPng process.</td>
<td><code>display ripng process-id route [ ipv6-address prefix-length [ verbose ] ] [ peer ipv6-address ] [ statistics ]</code></td>
</tr>
<tr>
<td>Restart a RIPng process.</td>
<td><code>reset ripng process-id process</code></td>
</tr>
<tr>
<td>Clear statistics for a RIPng process.</td>
<td><code>reset ripng process-id statistics</code></td>
</tr>
</tbody>
</table>

RIPng configuration examples

Basic RIPng configuration example

Network requirements

As shown in Figure 95, Router A, Router B, and Router C learn IPv6 routing information through RIPng.

Configure Router B to filter the route (2::/64) learned from Router A. The route will not be added to the routing table of Router B, and Router B forwards only the route 4::/64 to Router A.

Figure 95 Network diagram

Configuration procedure

1. Configure IPv6 addresses for interfaces. (Details not shown.)
2. Configure basic RIPng:
   # Configure Router A.
   ```
   <RouterA> system-view
   [RouterA] ripng 1
   [RouterA-ripng-1] quit
   ```
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] ripng 1 enable
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] ripng 1 enable
[RouterA-GigabitEthernet1/0/2] quit

# Configure Router B.
<RouterB> system-view
[RouterB] ripng 1
[RouterB-ripng-1] quit
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] ripng 1 enable
[RouterB-GigabitEthernet1/0/1] quit
[RouterB] interface gigabitethernet 1/0/2
[RouterB-GigabitEthernet1/0/2] ripng 1 enable
[RouterB-GigabitEthernet1/0/2] quit

# Configure Router C.
<RouterC> system-view
[RouterC] ripng 1
[RouterC-ripng-1] quit
[RouterC] interface gigabitethernet 1/0/1
[RouterC-GigabitEthernet1/0/1] ripng 1 enable
[RouterC-GigabitEthernet1/0/1] quit
[RouterC] interface gigabitethernet 1/0/2
[RouterC-GigabitEthernet1/0/2] ripng 1 enable
[RouterC-GigabitEthernet1/0/2] quit
[RouterC] interface gigabitethernet 1/0/3
[RouterC-GigabitEthernet1/0/3] ripng 1 enable
[RouterC-GigabitEthernet1/0/3] quit

# Display the RIPng routing table on Router B.
[RouterB] display ripng 1 route
   Route Flags: A - Aging, S - Suppressed, G - Garbage-collect, D - Direct
   O - Optimal, F - Flush to RIB
   -----------------------------------------------------------------------------------
   Peer FE80::20F:E2FF:FE23:82F5 on GigabitEthernet1/0/1
   Destination 2::/64,
      via FE80::20F:E2FF:FE23:82F5, cost 1, tag 0, AOF, 6 secs
      Local route
   Peer FE80::20F:E2FF:FE00:100 on GigabitEthernet1/0/2
   Destination 4::/64,
      via FE80::20F:E2FF:FE00:100, cost 1, tag 0, AOF, 11 secs
      Destination 5::/64,
         via FE80::20F:E2FF:FE00:100, cost 1, tag 0, AOF, 11 secs
      Local route
   Destination 1::/64,
      via ::, cost 0, tag 0, DOF
   Destination 3::/64,
### Display the RIPng routing table on Router A.

```bash
[RouterA] display ripng 1 route
Route Flags: A - Aging, S - Suppressed, G - Garbage-collect, D – Direct
           O - Optimal, F - Flush to RIB
```

Peer FE80::200:2FF:FE64:8904 on GigabitEthernet1/0/1
Destination 3::/64,
           via FE80::200:2FF:FE64:8904, cost 1, tag 0, AOF, 31 secs
Destination 4::/64,
           via FE80::200:2FF:FE64:8904, cost 2, tag 0, AOF, 31 secs
Destination 5::/64,
           via FE80::200:2FF:FE64:8904, cost 2, tag 0, AOF, 31 secs
Local route
Destination 1::/64,
           via ::, cost 0, tag 0, DOF
Destination 1::/64,
           via ::, cost 0, tag 0, DOF

3. **Configure route filtering:**

   # Use IPv6 prefix lists on Router B to filter received and redistributed routes.

   ```bash
   [RouterB] ipv6 prefix-list aaa permit 4:: 64
   [RouterB] ipv6 prefix-list bbb deny 2:: 64
   [RouterB] ipv6 prefix-list bbb permit :: 0 less-equal 128
   [RouterB] ripng 1
   [RouterB-ripng-1] filter-policy prefix-list aaa export
   [RouterB-ripng-1] filter-policy prefix-list bbb import
   [RouterB-ripng-1] quit
   ```

   # Display the RIPng routing tables on Router B and Router A.

   ```bash
   [RouterB] display ripng 1 route
   Route Flags: A - Aging, S - Suppressed, G - Garbage-collect, D – Direct
           O - Optimal, F - Flush to RIB
   ```

   Peer FE80::1:1 on GigabitEthernet1/0/1

   Peer FE80::3:1 on GigabitEthernet1/0/2
   Destination 4::/64,
           via FE80::2:2, cost 1, tag 0, AOF, 11 secs
   Destination 5::/64,
           via FE80::2:2, cost 1, tag 0, AOF, 11 secs
   Local route
   Destination 1::/64,
           via ::, cost 0, tag 0, DOF
   Destination 3::/64,
           via ::, cost 0, tag 0, DOF
   [RouterA] display ripng 1 route
   Route Flags: A - Aging, S - Suppressed, G - Garbage-collect, D – Direct
RIPng route redistribution configuration example

Network requirements

As shown in Figure 96, Router B communicates with Router A through RIPng 100 and with Router C through RIPng 200.

Configure route redistribution on Router B, so the two RIPng processes can redistribute routes from each other.

Figure 96 Network diagram

Configuration procedure

1. Configure IPv6 addresses for interfaces. (Details not shown.)
2. Configure basic RIPng:

   # Enable RIPng 100 on Router A.
   <RouterA> system-view
   [RouterA] ripng 100
   [RouterA-ripng-100] quit
   [RouterA] interface gigabitethernet 1/0/1
   [RouterA-GigabitEthernet1/0/1] ripng 100 enable
   [RouterA-GigabitEthernet1/0/1] quit
   [RouterA-GigabitEthernet1/0/2] ripng 100 enable

   # Enable RIPng 200 on Router B.
   <RouterB> system-view
   [RouterB] ripng 100
   [RouterB-ripng-100] quit
   [RouterB] interface gigabitethernet 1/0/2
   [RouterB-GigabitEthernet1/0/2] ripng 100 enable
   [RouterB-GigabitEthernet1/0/2] quit
   [RouterB] ripng 200
   [RouterB-ripng-200] quit
   [RouterB] interface gigabitethernet 1/0/2
   [RouterB-GigabitEthernet1/0/2] ripng 200 enable

   # Enable RIPng 200 on Router C.
   <RouterC> system-view
[RouterC] ripng 200
[RouterC] interface gigabitethernet 1/0/1
[RouterC-GigabitEthernet1/0/1] ripng 200 enable
[RouterC-GigabitEthernet1/0/1] quit
[RouterC] interface gigabitethernet 1/0/2
[RouterC-GigabitEthernet1/0/2] ripng 200 enable
[RouterC-GigabitEthernet1/0/2] quit

# Display the routing table on Router A.
[RouterA] display ipv6 routing-table

Destinations : 7 Routes : 7

Destination: ::1/128 Protocol : Direct
NextHop : ::1 Preference: 0
Interface : InLoop0 Cost : 0

Destination: 1::/64 Protocol : Direct
NextHop : 1::1 Preference: 0
Interface : GE1/0/2 Cost : 0

Destination: 1::1/128 Protocol : Direct
NextHop : ::1 Preference: 0
Interface : InLoop0 Cost : 0

Destination: 2::/64 Protocol : Direct
NextHop : 2::1 Preference: 0
Interface : GE1/0/1 Cost : 0

Destination: 2::1/128 Protocol : Direct
NextHop : ::1 Preference: 0
Interface : InLoop0 Cost : 0

Destination: FE80::/10 Protocol : Direct
NextHop : :: Preference: 0
Interface : NULL0 Cost : 0

Destination: FF00::/8 Protocol : Direct
NextHop : :: Preference: 0
Interface : NULL0 Cost : 0

3. Configure RIPng route redistribution:

# Configure route redistribution between the two RIPng processes on Router B.
[RouterB] ripng 100
[RouterB-ripng-100] import-route ripng 200
[RouterB-ripng-100] quit
[RouterB] ripng 200
[RouterB-ripng-200] import-route ripng 100
[RouterB-ripng-200] quit

# Display the routing table on Router A.
### RIPng GR configuration example

#### Network requirements

As shown in Figure 97, Router A, Router B, and Router C learn IPv6 routing information through RIPng.

Configure Router A as the GR restarter. Configure Router B and Router C as the GR helpers to synchronize their routing tables with Router A by using GR.
Configuration procedure

1. Configure IPv6 addresses for interfaces. (Details not shown.)
2. Configure RIPng on the routers to ensure the following: (Details not shown.)
   - Router A, Router B, and Router C can communicate with each other at Layer 3.
   - Dynamic route update can be implemented among them with RIPng.
3. Enable RIPng GR on Router A.
   ```
   <RouterA> system-view
   [RouterA] ripng 1
   [RouterA-ripng-1] graceful-restart
   ```

Verifying the configuration

# Restart RIPng process 1 on Router A.
```
[RouterA-ripng-1] return
```
```
<RouterA> reset ripng 1 process
Reset RIPng process? [Y/N]:y
```

# Display GR information on Router A.
```
<RouterA> display ripng 1 graceful-restart
```
RIPng process: 1
Graceful Restart capability : Enabled
Current GR state : Normal
Graceful Restart period : 60  seconds
Graceful Restart remaining time: 0  seconds

RIPng NSR configuration example

Network requirements

As shown in Figure 98, Router S, Router A, and Router B learn IPv6 routing information through RIPng.

Enable RIPng NSR on Router S to ensure correct routing when an active/standby switchover occurs on Router S.
Configuration procedure

1. Configure IPv6 addresses for interfaces. (Details not shown.)
2. Configure RIPng on the routers to ensure the following: (Details not shown.)
   - Router S, Router A, and Router B can communicate with each other at Layer 3.
   - Dynamic route update can be implemented among them with RIPng.
3. Enable RIPng NSR on Router S.

   <RouterS> system-view
   [RouterS] ripng 1
   [RouterS-ripng-1] non-stop-routing
   [RouterS-ripng-1] quit

Verifying the configuration

# Perform an active/standby switchover on Router S.

   [RouterS] placement reoptimize

Predicted changes to the placement

<table>
<thead>
<tr>
<th>Program</th>
<th>Current location</th>
<th>New location</th>
</tr>
</thead>
<tbody>
<tr>
<td>lb</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>lsm</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>slsp</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>rib6</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>routepolicy</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>rib</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>staticroute6</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>staticroute</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>eviisis</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>ospf</td>
<td>0/0</td>
<td>1/0</td>
</tr>
</tbody>
</table>

Continue? [y/n]: y

Re-optimization of the placement start. You will be notified on completion

Re-optimization of the placement complete. Use 'display placement' to view the new placement

# During the switchover period, display RIPng neighbors on Router A to verify the neighbor relationship between Router A and Router S.

   [RouterA] display ripng 1 neighbor

   Neighbor Address: FE80::AE45:5CE7:422E:2867
   Interface : GigabitEthernet1/0/1
   Version : RIPng version 1 Last update: 00h00m23s
   Bad packets: 0 Bad routes : 0

# Display RIPng routes on Router A to verify if Router A has a route to the loopback interface on Router B.

   [RouterA] display ripng 1 route
Route Flags: A - Aging, S - Suppressed, G - Garbage-collect, D - Direct
O - Optimal, F - Flush to RIB

Peer FE80::AE45:5CE7:422E:2867 on GigabitEthernet1/0/1
Destination 1400:1::/64,
   via FE80::AE45:5CE7:422E:2867, cost 1, tag 0, AOF, 1 secs
Destination 4004::4/128,
   via FE80::AE45:5CE7:422E:2867, cost 2, tag 0, AOF, 1 secs
Local route
Destination 2002::2/128,
   via ::, cost 0, tag 0, DOF
Destination 1200:1::/64,
   via ::, cost 0, tag 0, DOF

# Display RIPng neighbors on Router B to verify the neighbor relationship between Router B and Router S.
[RouterB] display ripng 1 neighbor
Neighbor Address: FE80::20C:29FF:FECE:6277
   Interface : GigabitEthernet1/0/1
   Version    : RIPng version 1     Last update: 00h00m18s
   Bad packets: 0                   Bad routes : 0

# Display RIPng routes on Router B to verify if Router B has a route to the loopback interface on Router A.
[RouterB] display ripng 1 route
   Route Flags: A - Aging, S - Suppressed, G - Garbage-collect, D - Direct
               O - Optimal, F - Flush to RIB

Peer FE80::20C:29FF:FECE:6277 on GigabitEthernet1/0/1
Destination 2002::2/128,
   via FE80::20C:29FF:FECE:6277, cost 2, tag 0, AOF, 24 secs
Destination 1200:1::/64,
   via FE80::20C:29FF:FECE:6277, cost 1, tag 0, AOF, 24 secs
Local route
Destination 4004::4/128,
   via ::, cost 0, tag 0, DOF
Destination 1400:1::/64,
   via ::, cost 0, tag 0, DOF

The output shows the following when an active/standby switchover occurs on Router S:
- The neighbor relationships and routing information on Router A and Router B have not changed.
- The traffic from Router A to Router B has not been impacted.

Configuring RIPng FRR

Network requirements

As shown in Figure 99, Router A, Router B, and Router C run RIPng. Configure RIPng FRR so that when Link A becomes unidirectional, traffic can be switched to Link B immediately.
Table 22 Interface and IP address assignment

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router A</td>
<td>GigabitEthernet 1/0/1</td>
<td>1::1/64</td>
</tr>
<tr>
<td>Router A</td>
<td>GigabitEthernet 1/0/2</td>
<td>2::1/64</td>
</tr>
<tr>
<td>Router A</td>
<td>Loopback 0</td>
<td>10::1/128</td>
</tr>
<tr>
<td>Router B</td>
<td>GigabitEthernet 1/0/1</td>
<td>3::1/64</td>
</tr>
<tr>
<td>Router B</td>
<td>GigabitEthernet 1/0/2</td>
<td>2::2/64</td>
</tr>
<tr>
<td>Router B</td>
<td>Loopback 0</td>
<td>20::1/128</td>
</tr>
<tr>
<td>Router C</td>
<td>GigabitEthernet 1/0/1</td>
<td>1::2/64</td>
</tr>
<tr>
<td>Router C</td>
<td>GigabitEthernet 1/0/2</td>
<td>3::2/64</td>
</tr>
</tbody>
</table>

Configuration procedure

1. Configure IPv6 addresses for interfaces on the routers. (Details not shown.)

2. Configure RIPng on the routers to make sure Router A, Router B, and Router C can communicate with each other at the network layer. (Details not shown.)

3. Configure RIPng FRR:

   # Configure Router A.
   
   `<RouterA> system-view
   [RouterA] ipv6 prefix-list abc index 10 permit 20:: 128
   [RouterA] route-policy frr permit node 10
   [RouterA-route-policy-frr-10] if-match ipv6 address prefix-list abc
   [RouterA-route-policy-frr-10] apply ipv6 fast-reroute backup-interface gigabitethernet 1/0/1 backup-nexthop 1::2
   [RouterA-route-policy-frr-10] quit
   [RouterA] ripng 1
   [RouterA-ripng-1] fast-reroute route-policy frr
   [RouterA-ripng-1] quit
   
   # Configure Router B.
   
   `<RouterB> system-view
   [RouterB] ipv6 prefix-list abc index 10 permit 10:: 128
   [RouterB] route-policy frr permit node 10
   [RouterB-route-policy-frr-10] if-match ipv6 address prefix-list abc
   [RouterB-route-policy-frr-10] apply ipv6 fast-reroute backup-interface gigabitethernet 1/0/1 backup-nexthop 3::2
   [RouterB-route-policy-frr-10] quit
Verifying the configuration

# Display the route 20::1/128 on Router A to view the backup next hop information.
[RouterA] display ipv6 routing-table 20::1 128 verbose

Summary count : 1

Destination: 20::1/128
Protocol: RIPng
Process ID: 1
SubProtID: 0x0         Age: 00h17m42s
          Cost: 1            Preference: 100
          IpPre: N/A         QosLocalID: N/A
          Tag: 0              State: Inactive Adv
OrigTblID: 0x0         OrigVrf: default-vrf
TableID: 0xa           OrigAs: 0
NibID: 0x22000003      LastAs: 0
AttrID: 0xffffffff     Neighbor: FE80::34CD:9FF:FE2F:D02
Flags: 0x41            OrigNextHop: FE80::34CD:9FF:FE2F:D02
          Label: NULL       RealNextHop: FE80::34CD:9FF:FE2F:D02
          BkLabel: NULL      BkNextHop: FE80::7685:45FF:FEAD:102
          Tunnel ID: Invalid Interface: GigabitEthernet1/0/2
          BkTunnel ID: Invalid BkInterface: GigabitEthernet1/0/1
          FtnIndex: 0x0       TrafficIndex: N/A
          Connector: N/A

# Display the route 10::1/128 on Router B to view the backup next hop information.
[RouterB] display ipv6 routing-table 10::1 128 verbose

Summary count : 1

Destination: 10::/128
Protocol: RIPng
Process ID: 1
SubProtID: 0x0         Age: 00h22m34s
          Cost: 1            Preference: 100
          IpPre: N/A         QosLocalID: N/A
          Tag: 0              State: Inactive Adv
OrigTblID: 0x0         OrigVrf: default-vrf
TableID: 0xa           OrigAs: 0
NibID: 0x22000001      LastAs: 0
AttrID: 0xffffffff     Neighbor: FE80::34CC:E8FF:FE5B:C02
Flags: 0x41            OrigNextHop: FE80::34CC:E8FF:FE5B:C02
          Label: NULL       RealNextHop: FE80::34CC:E8FF:FE5B:C02
          BkLabel: NULL      BkNextHop: FE80::7685:45FF:FEAD:102
          Tunnel ID: Invalid Interface: GigabitEthernet1/0/2
          BkTunnel ID: Invalid BkInterface: GigabitEthernet1/0/1
RIPng IPsec profile configuration example

Network requirements

As shown in Figure 100, configure RIPng on the routers, and configure IPsec profiles on the routers to authenticate and encrypt protocol packets.

Figure 100 Network diagram

![Network diagram](image)

Configuration procedure

1. Configure IPv6 addresses for interfaces. (Details not shown.)
2. Configure RIPng basic functions:
   # Configure Router A.
   <RouterA> system-view
   [RouterA] ripng 1
   [RouterA-ripng-1] quit
   [RouterA] interface gigabitethernet 1/0/1
   [RouterA-GigabitEthernet1/0/1] ripng 1 enable
   [RouterA-GigabitEthernet1/0/1] quit
   # Configure Router B.
   <RouterB> system-view
   [RouterB] ripng 1
   [RouterB-ripng-1] quit
   [RouterB] interface gigabitethernet 1/0/1
   [RouterB-GigabitEthernet1/0/1] ripng 1 enable
   [RouterB-GigabitEthernet1/0/1] quit
   [RouterB] interface gigabitethernet 1/0/2
   [RouterB-GigabitEthernet1/0/2] ripng 1 enable
   [RouterB-GigabitEthernet1/0/2] quit
   # Configure Router C.
   <RouterC> system-view
   [RouterC] ripng 1
   [RouterC-ripng-1] quit
   [RouterC] interface gigabitethernet 1/0/1
   [RouterC-GigabitEthernet1/0/1] ripng 1 enable
   [RouterC-GigabitEthernet1/0/1] quit
   [RouterC] interface gigabitethernet 1/0/2
   [RouterC-GigabitEthernet1/0/2] ripng 1 enable
   [RouterC-GigabitEthernet1/0/2] quit
3. Configure RIPng IPsec profiles:
   o On Router A:
   # Create an IPsec transform set named protrf1.
   [RouterA] ipsec transform-set protrf1
   # Specify the ESP encryption and authentication algorithms.
# Specify the encapsulation mode as transport.
[RouterA-ipsec-transform-set-protrf1] encapsulation-mode transport
[RouterA-ipsec-transform-set-protrf1] quit

# Create a manual IPsec profile named profile001.
[RouterA] ipsec profile profile001 manual

# Reference IPsec transform set protrf1.
[RouterA-ipsec-profile-profile001-manual] transform-set protrf1

# Configure the inbound and outbound SPIs for ESP.
[RouterA-ipsec-profile-profile001-manual] sa spi inbound esp 256
[RouterA-ipsec-profile-profile001-manual] sa spi outbound esp 256

# Configure the inbound and outbound SA keys for ESP.
[RouterA-ipsec-profile-profile001-manual] sa string-key inbound esp simple abc
[RouterA-ipsec-profile-profile001-manual] sa string-key outbound esp simple abc
[RouterA-ipsec-profile-profile001-manual] quit

On Router B:

# Create an IPsec transform set named protrf1.
[RouterB] ipsec transform-set protrf1

# Specify the ESP encryption and authentication algorithms.
[RouterB-ipsec-transform-set-protrf1] esp encryption-algorithm 3des-cbc
[RouterB-ipsec-transform-set-protrf1] esp authentication-algorithm md5

# Specify the encapsulation mode as transport.
[RouterB-ipsec-transform-set-protrf1] encapsulation-mode transport
[RouterB-ipsec-transform-set-protrf1] quit

# Create a manual IPsec profile named profile001.
[RouterB] ipsec profile profile001 manual

# Reference IPsec transform set protrf1.
[RouterB-ipsec-profile-profile001-manual] transform-set protrf1

# Configure the inbound and outbound SPIs for ESP.
[RouterB-ipsec-profile-profile001-manual] sa spi inbound esp 256
[RouterB-ipsec-profile-profile001-manual] sa spi outbound esp 256

# Configure the inbound and outbound SA keys for ESP.
[RouterB-ipsec-profile-profile001-manual] sa string-key inbound esp simple abc
[RouterB-ipsec-profile-profile001-manual] sa string-key outbound esp simple abc
[RouterB-ipsec-profile-profile001-manual] quit

On Router C:

# Create an IPsec transform set named protrf1.
[RouterC] ipsec transform-set protrf1

# Specify the ESP encryption and authentication algorithms.
[RouterC-ipsec-transform-set-protrf1] esp encryption-algorithm 3des-cbc
[RouterC-ipsec-transform-set-protrf1] esp authentication-algorithm md5

# Specify the encapsulation mode as transport.
[RouterC-ipsec-transform-set-protrf1] encapsulation-mode transport
[RouterC-ipsec-transform-set-protrf1] quit

# Create a manual IPsec profile named profile001.
[RouterC] ipsec profile profile001 manual
# Reference IPsec transform set protrf1.
[RouterC-ipsec-profile-profile001-manual] transform-set protrf1

# Configure the inbound and outbound SPIs for ESP.
[RouterC-ipsec-profile-profile001-manual] sa spi inbound esp 256
[RouterC-ipsec-profile-profile001-manual] sa spi outbound esp 256

# Configure the inbound and outbound SA keys for ESP.
[RouterC-ipsec-profile-profile001-manual] sa string-key inbound esp simple abc
[RouterC-ipsec-profile-profile001-manual] sa string-key outbound esp simple abc
[RouterC-ipsec-profile-profile001-manual] quit

4. Apply the IPsec profiles to the RIPng process:
# Configure Router A.
[RouterA] ripng 1
[RouterA-ripng-1] enable ipsec-profile profile001
[RouterA-ripng-1] quit

# Configure Router B.
[RouterB] ripng 1
[RouterB-ripng-1] enable ipsec-profile profile001
[RouterB-ripng-1] quit

# Configure Router C.
[RouterC] ripng 1
[RouterC-ripng-1] enable ipsec-profile profile001
[RouterC-ripng-1] quit

Verifying the configuration

# Verify that RIPng packets between Routers A, B, and C are protected by IPsec. (Details not shown.)
Configuring OSPFv3

This chapter describes how to configure RFC 2740-compliant Open Shortest Path First version 3 (OSPFv3) for an IPv6 network. For more information about OSPFv2, see "Configuring OSPF."

Overview

OSPFv3 and OSPFv2 have the following in common:
- 32-bit router ID and area ID.
- Hello, Database Description (DD), Link State Request (LSR), Link State Update (LSU), Link State Acknowledgment (LSAck).
- Mechanisms for finding neighbors and establishing adjacencies.
- Mechanisms for advertising and aging LSAs.

OSPFv3 and OSPFv2 have the following differences:
- OSPFv3 runs on a per-link basis. OSPFv2 runs on a per-IP-subnet basis.
- OSPFv3 supports running multiple processes on an interface, but OSPFv2 does not support.
- OSPFv3 identifies neighbors by router ID. OSPFv2 identifies neighbors by IP address.

OSPFv3 packets

OSPFv3 uses the following packet types:
- **Hello**—Periodically sent to find and maintain neighbors, containing timer values, information about the DR, BDR, and known neighbors.
- **DD**—Describes the digest of each LSA in the LSDB, exchanged between two routers for data synchronization.
- **LSR**—Requests needed LSAs from the neighbor. After exchanging the DD packets, the two routers know which LSAs of the neighbor are missing from their LSDBs. They then send an LSR packet to each other, requesting the missing LSAs. The LSA packet contains the digest of the missing LSAs.
- **LSU**—Transmits the requested LSAs to the neighbor.
- **LSAck**—Acknowledges received LSU packets.

OSPFv3 LSA types

OSPFv3 sends routing information in LSAs. The following LSAs are commonly used:
- **Router LSA**—Type-1 LSA, originated by all routers. This LSA describes the collected states of the router’s interfaces to an area, and is flooded throughout a single area only.
- **Network LSA**—Type-2 LSA, originated for broadcast and NBMA networks by the DR. This LSA contains the list of routers connected to the network, and is flooded throughout a single area only.
- **Inter-Area-Prefix LSA**—Type-3 LSA, originated by ABRs and flooded throughout the LSA’s associated area. Each Inter-Area-Prefix LSA describes a route with IPv6 address prefix to a destination outside the area, yet still inside the AS.
- **Inter-Area-Router LSA**—Type-4 LSA, originated by ABRs and flooded throughout the LSA’s associated area. Each Inter-Area-Router LSA describes a route to ASBR.
• **AS External LSA**—Type-5 LSA, originated by ASBRs, and flooded throughout the AS, except stub areas and Not-So-Stubby Areas (NSSAs). Each AS External LSA describes a route to another AS. A default route can be described by an AS External LSA.

• **NSSA LSA**—Type-7 LSA, originated by ASBRs in NSSAs and flooded throughout a single NSSA. NSSA LSAs describe routes to other ASs.

• **Link LSA**—Type-8 LSA. A router originates a separate Link LSA for each attached link. Link LSAs have link-local flooding scope. Each Link LSA describes the IPv6 address prefix of the link and Link-local address of the router.

• **Intra-Area-Prefix LSA**—Type-9 LSA. Each Intra-Area-Prefix LSA contains IPv6 prefix information on a router, stub area, or transit area information, and has area flooding scope. It was introduced because Router LSAs and Network LSAs contain no address information.

• **Grace LSA**—Type-11 LSA, generated by a GR restarter at reboot and transmitted on the local link. The GR restarter describes the cause and interval of the reboot in the Grace LSA to notify its neighbors that it performs a GR operation.

### Protocols and standards

- RFC 5340, *OSPF for IPv6*
- RFC 2328, *OSPF Version 2*
- RFC 3101, *OSPF Not-So-Stubby Area (NSSA) Option*
- RFC 5187, *OSPFv3 Graceful Restart*

### OSPFv3 configuration task list

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>(Required.)</em> Enabling OSPFv3</td>
</tr>
<tr>
<td><em>(Optional.)</em> Configuring OSPFv3 area parameters:</td>
</tr>
<tr>
<td>- Configuring a stub area</td>
</tr>
<tr>
<td>- Configuring an NSSA area</td>
</tr>
<tr>
<td>- Configuring an OSPFv3 virtual link</td>
</tr>
<tr>
<td><em>(Optional.)</em> Configuring OSPFv3 network types:</td>
</tr>
<tr>
<td>- Configuring the OSPFv3 network type for an interface</td>
</tr>
<tr>
<td>- Configuring an NBMA or P2MP neighbor</td>
</tr>
<tr>
<td><em>(Optional.)</em> Configuring OSPFv3 route control:</td>
</tr>
<tr>
<td>- Configuring OSPFv3 route summarization</td>
</tr>
<tr>
<td>- Configuring OSPFv3 received route filtering</td>
</tr>
<tr>
<td>- Configuring Inter-Area-Prefix LSA filtering</td>
</tr>
<tr>
<td>- Setting an OSPFv3 cost for an interface</td>
</tr>
<tr>
<td>- Setting the maximum number of OSPFv3 ECMP routes</td>
</tr>
<tr>
<td>- Setting a preference for OSPFv3</td>
</tr>
<tr>
<td>- Configuring OSPFv3 route redistribution</td>
</tr>
<tr>
<td><em>(Optional.)</em> Tuning and optimizing OSPFv3 networks:</td>
</tr>
<tr>
<td>- Setting OSPFv3 timers</td>
</tr>
<tr>
<td>- Setting LSA transmission delay</td>
</tr>
<tr>
<td>- Setting SPF calculation interval</td>
</tr>
<tr>
<td>- Setting the LSA generation interval</td>
</tr>
</tbody>
</table>
### Tasks at a glance

- Setting a DR priority for an interface
- Ignoring MTU check for DD packets
- Disabling interfaces from receiving and sending OSPFv3 packets
- Enabling the logging of neighbor state changes
- Configuring OSPFv3 network management
- Setting the LSU transmit rate
- Configuring stub routers
- Configuring prefix suppression

(Optional.) Configuring OSPFv3 GR:
- Configuring GR rearter
- Configuring GR helper
- Triggering OSPFv3 GR

(Optional.) Configuring OSPFv3 NSR

(Optional.) Configuring BFD for OSPFv3

(Optional.) Configuring OSPFv3 FRR

(Optional.) Applying an IPsec profile

## Enabling OSPFv3

Before you enable OSPFv3, configure IPv6 addresses for interfaces to ensure IPv6 connectivity between neighboring nodes.

To enable an OSPFv3 process on a router:

1. Enable the OSPFv3 process globally.
2. Assign the OSPFv3 process a router ID.
3. Enable the OSPFv3 process on related interfaces.

The router ID uniquely identifies the router within an AS. If a router runs multiple OSPFv3 processes, you must specify a unique router ID for each process.

An OSPFv3 process ID has only local significance. Process 1 on a router can exchange packets with process 2 on another router.

To enable OSPFv3:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable an OSPFv3 process and enter its view.</td>
<td>ospf3 [ process-id</td>
</tr>
<tr>
<td>3.</td>
<td>Specify a router ID.</td>
<td>router-id router-id</td>
</tr>
<tr>
<td>4.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>5.</td>
<td>Enable an OSPFv3 process on the interface.</td>
<td>ospf3 process-id area area-id [ instance instance-id ]</td>
</tr>
</tbody>
</table>
Configuring OSPFv3 area parameters

OSPFv3 has the same stub area, NSSA area, and virtual link features as OSPFv2.

After you split an OSPFv3 AS into multiple areas, the LSA number is reduced and OSPFv3 applications are extended. To further reduce the size of routing tables and the number of LSAs, configure the non-backbone areas at an AS edge as stub areas.

A stub area cannot import external routes, but an NSSA area can import external routes into the OSPFv3 routing domain while retaining other stub area characteristics.

Non-backbone areas exchange routing information through the backbone area, so the backbone and non-backbone areas (including the backbone itself) must be fully meshed. If no connectivity can be achieved, configure virtual links.

Configuration prerequisites

Before you configure OSPFv3 area parameters, enable OSPFv3.

Configuring a stub area

All the routers attached to a stub area must be configured with the `stub` command. The `no-summary` keyword is only available on the ABR of the stub area.

If you use the `stub` command with the `no-summary` keyword on an ABR, the ABR advertises a default route in an Inter-Area-Prefix LSA into the stub area. No AS External LSA, Inter-Area-Prefix LSA, or other Inter-Area-Router LSA is advertised in the area. The stub area of this kind is called a totally stub area.

To configure an OSPFv3 stub area:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter OSPFv3 view.</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>Enter OSPFv3 area view.</td>
<td>N/A</td>
</tr>
<tr>
<td>4.</td>
<td>Configure the area as a stub area.</td>
<td>By default, no area is configured as a stub area.</td>
</tr>
<tr>
<td>5.</td>
<td>(Optional.) Set a cost for the default route advertised to the stub area.</td>
<td>The default setting is 1.</td>
</tr>
</tbody>
</table>

**Step**

- **1.** Enter system view.
  - Command: `system-view`
  - Remarks: N/A

**Step**

- **2.** Enter OSPFv3 view.
  - Command: `ospfv3 [ process-id | vpn-instance vpn-instance-name ]`
  - Remarks: N/A

**Step**

- **3.** Enter OSPFv3 area view.
  - Command: `area area-id`
  - Remarks: N/A

**Step**

- **4.** Configure the area as a stub area.
  - Command: `stub [ default-route-advertise-always | no-summary ]`
  - Remarks: By default, no area is configured as a stub area.

**Step**

- **5.** (Optional.) Set a cost for the default route advertised to the stub area.
  - Command: `default-cost cost-value`
  - Remarks: The default setting is 1.

Configuring an NSSA area

To configure an NSSA area, configure the `nssa` command on all the routers attached to the area.

To configure a totally NSSA area, configure the `nssa no-summary` command on the ABR. The ABR of a totally NSSA area does not advertise inter-area routes into the area.

To configure an NSSA area:
### Configuring an OSPFv3 virtual link

You can configure a virtual link to maintain connectivity between a non-backbone area and the backbone, or in the backbone itself.

**IMPORTANT:**
- Both ends of a virtual link are ABRs that must be configured with the `vlink-peer` command.
- Do not configure virtual links in the areas of a GR-capable process.

To configure a virtual link:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter OSPFv3 view.</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>Enter OSPFv3 area view.</td>
<td>N/A</td>
</tr>
</tbody>
</table>

### Configuring OSPFv3 network types

OSPFv3 classifies networks into the following types by the link layer protocol:
- **Broadcast**—When the link layer protocol is Ethernet or FDDI, OSPFv3 considers the network type as broadcast by default.
- **NBMA**—When the link layer protocol is ATM, Frame Relay, or X.25, OSPFv3 considers the network type as NBMA by default.
- **P2P**—When the link layer protocol is PPP, LAPB, HDLC, or POS, OSPFv3 considers the network type as P2P by default.

Follow these guidelines when you change the network type of an OSPFv3 interface:
- An NBMA network must be fully connected. Any two routers in the network must be directly reachable to each other through a virtual circuit. If no such direct link is available, you must change the network type through a command.
- If direct connections are not available between some routers in an NBMA network, the type of interfaces associated must be configured as P2MP, or as P2P for interfaces with only one neighbor.

**Configuration prerequisites**

Before you configure OSPFv3 network types, enable OSPFv3.

### Configuring the OSPFv3 network type for an interface

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td><code>interface interface-type interface-number</code></td>
</tr>
<tr>
<td>3.</td>
<td>Configure a network type for the OSPFv3 interface.</td>
<td>`ospfv3 network-type { broadcast</td>
</tr>
</tbody>
</table>

### Configuring an NBMA or P2MP neighbor

For NBMA and P2MP interfaces (only when in unicast mode), you must specify the link-local IP addresses of their neighbors because these interfaces cannot find neighbors through broadcasting hello packets. For NBMA interfaces, you can also specify DR priorities for neighbors.

To configure an NBMA or P2MP (unicast) neighbor and its DR priority:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td><code>interface interface-type interface-number</code></td>
</tr>
<tr>
<td>3.</td>
<td>Specify an NBMA or P2MP (unicast) neighbor and its DR priority.</td>
<td>`ospfv3 peer ipv6-address [ cost cost-value</td>
</tr>
</tbody>
</table>

### Configuring OSPFv3 route control

**Configuration prerequisites**

Before you configure OSPFv3 route control, perform the following tasks:
- Configure IPv6 addresses for interfaces to ensure IPv6 connectivity between neighboring nodes.
• Enable OSPFv3.

Configuring OSPFv3 route summarization

Route summarization enables an ABR or ASBR to summarize contiguous networks into a single network and advertise it to other areas.

Configuring route summarization on an ABR

If contiguous network segments exist in an area, you can summarize them into one network segment on the ABR. The ABR will advertise only the summary route. Any LSA on the specified network segment will not be advertised, reducing the LSDB size in other areas.

To configure route summarization on an ABR:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>ospfv3 [ process-id</td>
<td>vpn-instance vpn-instance-name ] *</td>
</tr>
<tr>
<td>3.</td>
<td>area area-id</td>
<td>N/A</td>
</tr>
<tr>
<td>4.</td>
<td>abr-summary ipv6-address prefix-length [ not-advertise ] [ cost cost-value ]</td>
<td>By default, route summarization is not configured on an ABR.</td>
</tr>
</tbody>
</table>

Configuring route summarization on an ASBR

Perform this task to enable an ASBR to summarize external routes within the specified address range into a single route.

An ASBR can summarize routes in the following LSAs:
• Type-5 LSAs.
• Type-7 LSAs in an NSSA area.
• Type-5 LSAs translated by the ASBR (also an ABR) from Type-7 LSAs in an NSSA area.

If the ASBR (ABR) is not a translator, it cannot summarize routes in Type-5 LSAs translated from Type-7 LSAs.

To configure route summarization on an ASBR:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>ospfv3 [ process-id</td>
<td>vpn-instance vpn-instance-name ] *</td>
</tr>
<tr>
<td>3.</td>
<td>asbr-summary ipv6-address prefix-length [ not-advertise ] [ cost cost-value</td>
<td>By default, route summarization is not configured on an ABR.</td>
</tr>
</tbody>
</table>

Configuring OSPFv3 received route filtering

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
</tbody>
</table>
### Configuring Inter-Area-Prefix LSA filtering

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter OSPFv3 view.</td>
<td>ospfv3 [ process-id</td>
</tr>
<tr>
<td>3.</td>
<td>Enter OSPFv3 area view.</td>
<td>area area-id</td>
</tr>
<tr>
<td>4.</td>
<td>Configure OSPFv3 to filter Inter-Area-Prefix LSAs.</td>
<td>filter ( ipv6-acl-number</td>
</tr>
</tbody>
</table>

### Setting an OSPFv3 cost for an interface

You can set an OSPFv3 cost for an interface with one of the following methods:

- Set the cost value in interface view.
- Set a bandwidth reference value for the interface, and OSPFv3 computes the cost automatically based on the bandwidth reference value by using the following formula:
  Interface OSPFv3 cost = Bandwidth reference value (100 Mbps) / Interface bandwidth (Mbps)
  - If the calculated cost is greater than 65535, the value of 65535 is used.
  - If the calculated cost is smaller than 1, the value of 1 is used.
- If no cost is set for an interface, OSPFv3 automatically computes the cost for the interface.

To set an OSPFv3 cost for an interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Set an OSPFv3 cost for the interface.</td>
<td>ospfv3 cost cost-value [ instance instance-id ]</td>
</tr>
</tbody>
</table>

To set a bandwidth reference value:
### Setting the maximum number of OSPFv3 ECMP routes

Perform this task to implement load sharing over ECMP routes.

To set the maximum number of ECMP routes:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter OSPFv3 view.</td>
<td>ospfv3 [ process-id</td>
</tr>
<tr>
<td>3.</td>
<td>Set the maximum number of ECMP routes.</td>
<td>maximum load-balancing number</td>
</tr>
</tbody>
</table>

### Setting a preference for OSPFv3

A router can run multiple routing protocols. The system assigns a priority for each protocol. When these routing protocols find the same route, the route found by the protocol with the highest priority is selected.

To set a preference for OSPFv3:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter OSPFv3 view.</td>
<td>ospfv3 [ process-id</td>
</tr>
<tr>
<td>3.</td>
<td>Set a preference for OSPFv3.</td>
<td>preference [ ase</td>
</tr>
</tbody>
</table>

### Configuring OSPFv3 route redistribution

Because OSPFv3 is a link state routing protocol, it cannot directly filter LSAs to be advertised. OSPFv3 filters only redistributed routes. Only routes that are not filtered out can be advertised in LSAs.

Executing the **import-route** or **default-route-advertise** command on a router makes it become an ASBR.
IMPORTANT:
The `import-route bgp4+` command redistributes only EBGP routes. Because the `import-route bgp4+ allow-ibgp` command redistributes both EBGP and IBGP routes, and might cause routing loops, use it with caution.

Redistributing routes from another routing protocol

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>2.</td>
<td>Enter OSPFv3 view.</td>
<td>`ospfv3 [ process-id</td>
</tr>
<tr>
<td>3.</td>
<td>Configure OSPFv3 to redistribute routes from other routing protocols.</td>
<td>`import-route protocol [ as-number ] [ process-id</td>
</tr>
<tr>
<td>4.</td>
<td>(Optional.) Configure OSPFv3 to filter redistributed routes.</td>
<td>`filter-policy { ipv6-acl-number</td>
</tr>
</tbody>
</table>

Redistributing a default route

The `import-route` command cannot redistribute a default external route. Perform this task to redistribute a default route.

To redistribute a default route:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>2.</td>
<td>Enter OSPFv3 view.</td>
<td>`ospfv3 [ process-id</td>
</tr>
</tbody>
</table>

Setting tags for redistributed routes

Perform this task to set tags for redistributed routes to identify information about protocols. For example, when redistributing IPv6 BGP routes, OSPFv3 uses tags to identify AS IDs.

To set a tag for redistributed routes:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
</tbody>
</table>
Tuning and optimizing OSPFv3 networks

This section describes configurations of OSPFv3 timers, interface DR priority, and the logging of neighbor state changes.

Configuration prerequisites

Before you tune and optimize OSPFv3 networks, perform the following tasks:

- Configure IPv6 addresses for interfaces to ensure IPv6 connectivity between neighboring nodes.
- Enable OSPFv3.

Setting OSPFv3 timers

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter interface view.</td>
<td><code>interface interface-type interface-number</code></td>
<td>N/A</td>
</tr>
<tr>
<td>3. Set the hello interval.</td>
<td><code>ospfv3 timer hello seconds [ instance instance-id ]</code></td>
<td>By default, the hello interval on P2P and broadcast interfaces is 10 seconds.</td>
</tr>
<tr>
<td>4. Set the dead interval.</td>
<td><code>ospfv3 timer dead seconds [ instance instance-id ]</code></td>
<td>By default, the dead interval on P2P and broadcast interfaces is 40 seconds. The dead interval set on neighboring interfaces cannot be too short. Otherwise, a neighbor is easily considered down.</td>
</tr>
<tr>
<td>5. Set the poll interval.</td>
<td><code>ospfv3 timer poll seconds [ instance instance-id ]</code></td>
<td>By default, the poll interval is 120 seconds.</td>
</tr>
<tr>
<td>6. Set the LSA retransmission interval.</td>
<td><code>ospfv3 timer retransmit interval [ instance instance-id ]</code></td>
<td>The default setting is 5 seconds. The LSA retransmission interval cannot be too short. Otherwise, unnecessary retransmissions will occur.</td>
</tr>
</tbody>
</table>

Setting LSA transmission delay

Each LSA in the LSDB has an age that is incremented by 1 every second, but the age does not change during transmission. Therefore, it is necessary to add a transmission delay into the age time, especially for low-speed links.

To set the LSA transmission delay on an interface:
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter interface view.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3. Set the LSA transmission delay.</td>
<td>ospfv3 trans-delay seconds [ instance instance-id ]</td>
<td>By default, the LSA transmission delay is 1 second.</td>
</tr>
</tbody>
</table>

### Setting SPF calculation interval

LSDB changes result in SPF calculations. When the topology changes frequently, a large amount of network and router resources are occupied by SPF calculation. You can adjust the SPF calculation interval to reduce the impact.

For a stable network, the minimum interval is used. If network changes become frequent, the SPF calculation interval is incremented by the incremental interval × 2^n−2 for each calculation until the maximum interval is reached. The value n is the number of calculation times.

To set SPF calculation interval:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter OSPFv3 view.</td>
<td>ospfv3 [ process-id</td>
<td>vpn-instance vpn-instance-name ] *</td>
</tr>
</tbody>
</table>
  • The maximum interval is 5 seconds.  
  • The minimum interval is 50 milliseconds.  
  • The incremental interval is 200 milliseconds. |

### Setting the LSA generation interval

You can adjust the LSA generation interval to protect network resources and routers from being over consumed by frequent network changes.

For a stable network, the minimum interval is used. If network changes become frequent, the LSA generation interval is incremented by the incremental interval × 2^n−2 for each generation until the maximum interval is reached. The value n is the number of generation times.

To set the LSA generation interval:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter OSPFv3 view.</td>
<td>ospfv3 [ process-id</td>
<td>vpn-instance vpn-instance-name ] *</td>
</tr>
<tr>
<td>3. Set the LSA generation interval.</td>
<td>lsa-generation-interval maximum-interval [ minimum-interval [ incremental-interval ] ]</td>
<td>By default, the maximum interval is 5 seconds, the minimum interval is 0 milliseconds, and the incremental interval is 0 milliseconds.</td>
</tr>
</tbody>
</table>
Setting a DR priority for an interface

The router priority is used for DR election. Interfaces having the priority 0 cannot become a DR or BDR.

To configure a DR priority for an interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
</tbody>
</table>

Ignoring MTU check for DD packets

When LSAs are few in DD packets, it is unnecessary to check the MTU in DD packets to improve efficiency.

To ignore MTU check for DD packets:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Ignore MTU check for DD packets.</td>
<td>ospfv3 mtu-ignore [ instance instance-id ]</td>
</tr>
</tbody>
</table>

Disabling interfaces from receiving and sending OSPFv3 packets

After an OSPFv3 interface is set to silent, direct routes of the interface can still be advertised in Intra-Area-Prefix LSAs through other interfaces, but other OSPFv3 packets cannot be advertised. No neighboring relationship can be established on the interface. This feature can enhance the adaptability of OSPFv3 networking.

To disable interfaces from receiving and sending OSPFv3 packets:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter OSPFv3 view.</td>
<td>ospfv3 [ process-id</td>
</tr>
</tbody>
</table>
Step | Command | Remarks
--- | --- | ---
3. Disable interfaces from receiving and sending OSPFv3 packets. | `silent-interface { interface-type interface-number | all }` | By default, the interfaces are able to receive and send OSPFv3 packets. This command disables only the interfaces associated with the current process. However, multiple OSPFv3 processes can disable the same interface from receiving and sending OSPFv3 packets.

Enabling the logging of neighbor state changes

With this feature enabled, the router delivers logs about neighbor state changes to its information center. The information center processes logs according to user-defined output rules (whether to output logs and where to output). For more information about the information center, see *Network Management and Monitoring Configuration Guide*.

To enable the logging of neighbor state changes:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter OSPFv3 view.</td>
<td>`ospfv3 [ process-id</td>
<td>vpn-instance vpn-instance-name ]`</td>
</tr>
<tr>
<td>3. Enable the logging of neighbor state changes.</td>
<td><code>log-peer-change</code></td>
<td>By default, this feature is enabled.</td>
</tr>
</tbody>
</table>

Configuring OSPFv3 network management

This task involves the following configurations:

- Bind an OSPFv3 process to MIB so that you can use network management software to manage the specified OSPFv3 process.
- Enable SNMP notifications for OSPFv3 to report important events.
- Set the SNMP notification output interval and the maximum number of SNMP notifications that can be output at each interval.

To report critical OSPFv3 events to an NMS, enable SNMP notifications for OSPFv3. For SNMP notifications to be sent correctly, you must also configure SNMP on the device. For more information about SNMP configuration, see the network management and monitoring configuration guide for the device.

The standard OSPFv3 MIB provides only single-instance MIB objects. To identify multiple OSPFv3 processes in the standard OSPFv3 MIB, you must assign a unique context name to each OSPFv3 process.

Context is a method introduced to SNMPv3 for multiple-instance management. For SNMPv1/v2c, you must specify a community name as a context name for protocol identification.

To configure OSPFv3 network management:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
</tbody>
</table>
### Setting the LSU transmit rate

Sending large numbers of LSU packets affects router performance and consumes a large amount of network bandwidth. You can configure the router to send LSU packets at an interval and to limit the maximum number of LSU packets sent out of an OSPFv3 interface at each interval.

To set the LSU transmit rate:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>ospfv3 [ process-id</td>
<td>vpn-instance vpn-instance-name ] *</td>
</tr>
<tr>
<td>3.</td>
<td>transmit-pacing interval interval count count</td>
<td>By default, an OSPFv3 interface sends a maximum of three LSU packets every 20 milliseconds.</td>
</tr>
</tbody>
</table>

### Configuring stub routers

A stub router is used for traffic control. It reports its status as a stub router to neighboring OSPFv3 routers. The neighboring routers can have a route to the stub router, but they do not use the stub router to forward data.

Use either of the following methods to configure a router as a stub router:

- Clear the R-bit of the Option field in Type-1 LSAs. When the R-bit is clear, the OSPFv3 router can participate in OSPFv3 topology distribution without forwarding traffic.
Use the OSPFv3 max-metric router LSA feature. This feature enables OSPFv3 to advertise its locally generated Type-1 LSAs with a maximum cost of 65535. Neighbors do not send packets to the stub router as long as they have a route with a smaller cost.

To configure a router as a stub router:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>ospfv3 [ process-id</td>
<td>vpn-instance vpn-instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Method 1: stub-router r-bit [ include-stub</td>
<td>on-startup { seconds</td>
</tr>
<tr>
<td></td>
<td>Method 2: stub-router max-metric [ external-lsa [ max-metric-value ]</td>
<td>summary-lsa [ max-metric-value ]</td>
</tr>
</tbody>
</table>

Configuring prefix suppression

By default, an OSPFv3 interface advertises all of its prefixes in LSAs. To speed up OSPFv3 convergence, you can suppress interfaces from advertising all of their prefixes. This feature helps improve network security by preventing IP routing to the suppressed networks.

When prefix suppression is enabled:

- OSPFv3 does not advertise the prefixes of suppressed interfaces in Type-8 LSAs.
- On broadcast and NBMA networks, the DR does not advertise the prefixes of suppressed interfaces in Type-9 LSAs that reference Type-2 LSAs.
- On P2P and P2MP networks, OSPFv3 does not advertise the prefixes of suppressed interfaces in Type-9 LSAs that reference Type-1 LSAs.

**IMPORTANT:**
As a best practice, configure prefix suppression on all OSPFv3 routers if you want to use prefix suppression.

**Configuring prefix suppression for an OSPFv3 process**

Enabling prefix suppression for an OSPFv3 process does not suppress the prefixes of loopback interfaces and passive interfaces.

To configure prefix suppression for an OSPFv3 process:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>ospfv3 [ process-id</td>
<td>vpn-instance vpn-instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>prefix-suppression</td>
<td>By default, prefix suppression is disabled for an OSPFv3 process.</td>
</tr>
</tbody>
</table>
Configuring prefix suppression for an interface

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter interface</td>
<td><code>interface interface-type interface-number</code></td>
<td>N/A</td>
</tr>
<tr>
<td>3. Enable prefix</td>
<td><code>ospfv3 prefix-suppression [ disable ]</code> [ instance instance-id ]</td>
<td>By default, prefix suppression is disabled for an interface.</td>
</tr>
</tbody>
</table>

Configuring OSPFv3 GR

GR ensures forwarding continuity when a routing protocol restarts or an active/standby switchover occurs.

Two routers are required to complete a GR process. The following are router roles in a GR process:

- **GR restarter**—Graceful restarting router. It must be Graceful Restart capable.
- **GR helper**—The neighbor of the GR restarter. It helps the GR restarter to complete the GR process.

To prevent service interruption after a master/backup switchover, a GR restarter running OSPFv3 must perform the following tasks:

- Keep the GR restarter forwarding entries stable during reboot.
- Establish all adjacencies and obtain complete topology information after reboot.

After the active/standby switchover, the GR restarter sends a Grace LSA to tell its neighbors that it performs a GR. Upon receiving the Grace LSA, the neighbors with the GR helper capability enter the helper mode (and are called GR helpers). Then, the GR restarter retrieves its adjacencies and LSDB with the help of the GR helpers.

Configuring GR restarter

You can configure the GR restarter capability on a GR restarter.

⚠️ IMPORTANT: You cannot enable OSPFv3 NSR on a device that acts as GR restarter.

To configure GR restarter:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter OSPFv3 view.</td>
<td>`ospfv3 [ process-id</td>
<td>vpn-instance <code>vpn-instance-name ] *</code></td>
</tr>
<tr>
<td>3. Enable the GR</td>
<td>`graceful-restart enable [ global</td>
<td>planned-only ] *`</td>
</tr>
<tr>
<td>4. (Optional.) Set the GR interval.</td>
<td><code>graceful-restart interval interval</code></td>
<td>By default, the GR interval is 120 seconds.</td>
</tr>
</tbody>
</table>
Configuring GR helper

You can configure the GR helper capability on a GR helper.

To configure GR helper:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter OSPFv3 view.</td>
<td>ospfv3 [ process-id</td>
</tr>
<tr>
<td>3.</td>
<td>Enable the GR helper capability.</td>
<td>graceful-restart helper enable [ planned-only ]</td>
</tr>
<tr>
<td>4.</td>
<td>Enable strict LSA checking.</td>
<td>graceful-restart helper strict-lsa-checking</td>
</tr>
</tbody>
</table>

Triggering OSPFv3 GR

OSPFv3 GR is triggered by an active/standby switchover or when the following command is executed.

To trigger OSPFv3 GR, perform the following command in user view:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trigger OSPFv3 GR.</td>
<td>reset ospfv3 [ process-id ] process graceful-restart</td>
</tr>
</tbody>
</table>

Configuring OSPFv3 NSR

The following matrix shows the feature and hardware compatibility:

<table>
<thead>
<tr>
<th>Hardware</th>
<th>OSPFv3 NSR compatibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSR954(JH296A/JH297A/JH298A/JH299A/JH373A)</td>
<td>No</td>
</tr>
<tr>
<td>MSR958(JH300A/JH301A)</td>
<td>No</td>
</tr>
</tbody>
</table>
| MSR1002-4/1003-8S | • In standalone mode: No  
• In IRF mode: Yes |
| MSR2003 | • In standalone mode: No  
• In IRF mode: Yes |
| MSR2004-24/2004-48 | • In standalone mode: No  
• In IRF mode: Yes |
| MSR3012/3024/3044/3064 | • In standalone mode: No  
• In IRF mode: Yes |
| MSR4060/4080 | Yes |

Nonstop routing (NSR) backs up OSPFv3 link state information from the active process to the standby process. After an active/standby switchover, NSR can complete link state recovery and route regeneration without tearing down adjacencies or impacting forwarding services.
NSR does not require the cooperation of neighboring devices to recover routing information, and it is typically used more often than GR.

**IMPORTANT:**
A device that has OSPFv3 NSR enabled cannot act as GR restarter.

To enable OSPFv3 NSR:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter OSPFv3 view.</td>
<td>ospfv3 [ process-id</td>
</tr>
<tr>
<td>3.</td>
<td>Enable OSPFv3 NSR.</td>
<td>non-stop-routing</td>
</tr>
</tbody>
</table>

By default, OSPFv3 NSR is disabled. This command takes effect only for the current process. As a best practice, enable OSPFv3 NSR for each process if multiple OSPFv3 processes exist. Support for this command depends on the device model. For more information, see Layer 3—IP Routing Command Reference.

**Configuring BFD for OSPFv3**

Bidirectional forwarding detection (BFD) provides a mechanism to quickly detect the connectivity of links between OSPFv3 neighbors, improving the convergence speed of OSPFv3. For more information about BFD, see High Availability Configuration Guide.

After discovering neighbors by sending hello packets, OSPFv3 notifies BFD of the neighbor addresses, and BFD uses these addresses to establish sessions. Before a BFD session is established, it is in the down state. In this state, BFD control packets are sent at an interval of no less than 1 second to reduce BFD control packet traffic. After the BFD session is established, BFD control packets are sent at the negotiated interval, thereby implementing fast fault detection.

To configure BFD for OSPFv3, you need to configure OSPFv3 first.

To configure BFD for OSPFv3:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter OSPFv3 view.</td>
<td>ospfv3 [ process-id</td>
</tr>
<tr>
<td>3.</td>
<td>Specify a router ID.</td>
<td>router-id router-id</td>
</tr>
<tr>
<td>4.</td>
<td>Quit the OSPFv3 view.</td>
<td>quit</td>
</tr>
<tr>
<td>5.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>6.</td>
<td>Enable an OSPFv3 process on the interface.</td>
<td>ospfv3 process-id area area-id [ instance instance-id ]</td>
</tr>
<tr>
<td>7.</td>
<td>Enable BFD on the interface.</td>
<td>ospfv3 bfd enable [ instance instance-id ]</td>
</tr>
</tbody>
</table>

By default, BFD is disabled on the OSPFv3 interface.
Configuring OSPFv3 FRR

A primary link failure can cause packet loss and even a routing loop until OSPFv3 completes routing convergence based on the new network topology. OSPFv3 FRR enables fast rerouting to minimize the failover time.

Figure 101 Network diagram for OSPFv3 FRR

As shown in Figure 101, configure FRR on Router B. OSPFv3 FRR automatically calculates a backup next hop or specifies a backup next hop by using a routing policy. When the primary link fails, OSPFv3 directs packets to the backup next hop. At the same time, OSPFv3 calculates the shortest path based on the new network topology. It forwards packets over the path after network convergence.

You can configure OSPFv3 FRR to calculate a backup next hop by using the loop free alternate (LFA) algorithm, or specify a backup next hop by using a routing policy.

Configuration prerequisites

Before you configure OSPFv3 FRR, perform the following tasks:

- Configure IPv6 addresses for interfaces to ensure IP connectivity between neighboring nodes.
- Enable OSPFv3.
- Make sure the backup next hop is reachable.

Configuration guidelines

Do not use the fast-reroute lfa command together with the vlink-peer command.

Configuration procedure

Configuring OSPFv3 FRR to calculate a backup next hop using the LFA algorithm

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>(Optional.) Disable LFA on an interface.</td>
<td>ospfv3 fast-reroute lfa-backup exclude</td>
</tr>
<tr>
<td>4.</td>
<td>Return to system view.</td>
<td>quit</td>
</tr>
<tr>
<td>5.</td>
<td>Enter OSPFv3 view.</td>
<td>ospfv3 [ process-id ] vpn-instance</td>
</tr>
</tbody>
</table>
### Step Command Remarks

6. Enable OSPFv3 FRR to calculate a backup next hop by using the LFA algorithm.  
   **fast-reroute lfa [ abr-only ]**  
   By default, OSPFv3 FRR is disabled.  
   If abr-only is specified, the route to the ABR is selected as the backup path.

---

### Configuring OSPFv3 FRR to specify a backup next hop using a routing policy

Before you perform this task, use the **apply ipv6 fast-reroute backup-interface** command to specify a backup next hop in the routing policy to be used. For more information about the **apply ipv6 fast-reroute backup-interface** command and routing policy configuration, see "Configuring routing policies."

To configure OSPFv3 FRR to specify a backup next hop using a routing policy:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>(Optional.) Disable LFA on an interface.</td>
<td>ospfv3 fast-reroute lfa-backup exclude</td>
</tr>
<tr>
<td>4.</td>
<td>Return to system view.</td>
<td>quit</td>
</tr>
<tr>
<td>5.</td>
<td>Enter OSPFv3 view.</td>
<td>ospfv3 [ process-id ] vpn-instance vpn-instance-name ] *</td>
</tr>
<tr>
<td>6.</td>
<td>Enable OSPFv3 FRR to specify a backup next hop by using a routing policy.</td>
<td>fast-reroute route-policy route-policy-name</td>
</tr>
</tbody>
</table>

---

### Configuring BFD for OSPFv3 FRR

By default, OSPFv3 FRR does not use BFD to detect primary link failures. To speed up OSPFv3 convergence, enable BFD for OSPFv3 FRR to detect primary link failures.

To configure BFD control packet mode for OSPFv3 FRR:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Enable BFD control packet mode for OSPFv3 FRR.</td>
<td>ospfv3 primary-path-detect bfd ctrl [ instance instance-id ]</td>
</tr>
</tbody>
</table>

To configure BFD echo packet mode for OSPFv3 FRR:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
| 2.   | Configure the source IPv6 address of BFD echo packets. | bfd echo-source-ipv6 ipv6-address | By default, the source IPv6 address of BFD echo packets is not configured.  
   The source IPv6 address cannot be |
Applying an IPsec profile

To protect routing information and prevent attacks, OSPFv3 can authenticate protocol packets by using an IPsec profile. For more information about IPsec profiles, see Security Configuration Guide.

Outbound OSPFv3 packets carry the Security Parameter Index (SPI) defined in the relevant IPsec profile. A device compares the SPI carried in a received packet with the configured IPsec profile. If they match, the device accepts the packet. Otherwise, the device discards the packet and will not establish a neighbor relationship with the sending device.

You can configure an IPsec profile for an area, an interface, a virtual link, or a sham link.

- To implement area-based IPsec protection, configure the same IPsec profile on the routers in the target area.
- To implement interface-based IPsec protection, configure the same IPsec profile on the interfaces between two neighboring routers.
- To implement virtual link-based IPsec protection, configure the same IPsec profile on the two routers connected over the virtual link.
- To implement sham link-based IPsec protection, configure the same IPsec profile on the two routers connected over the sham link. For more information about sham links, see MPLS Configuration Guide.
- If an interface and its area each have an IPsec profile configured, the interface uses its own IPsec profile.
- If a virtual link and area 0 each have an IPsec profile configured, the virtual link uses its own IPsec profile.
- If a sham link and its area have an IPsec profile configured, the sham link uses its own IPsec profile.

To apply an IPsec profile to an area:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter OSPFv3 view.</td>
<td>ospfv3 [ process-id</td>
<td>vpn-instance vpn-instance-name ] *</td>
</tr>
<tr>
<td>3. Enter OSPFv3 area view.</td>
<td>area area-id</td>
<td>N/A</td>
</tr>
<tr>
<td>4. Apply an IPsec profile to the area.</td>
<td>enable ipsec-profile profile-name</td>
<td>By default, no IPsec profile is applied.</td>
</tr>
</tbody>
</table>

To apply an IPsec profile to an interface:
Step | Command | Remarks
---|---|---
1. Enter system view. | system-view | N/A
2. Enter interface view. | interface interface-type interface-number | N/A
3. Apply an IPsec profile to the interface. | ospfv3 ipsec-profile profile-name | By default, no IPsec profile is applied.

To apply an IPsec profile to a virtual link:

Step | Command | Remarks
---|---|---
1. Enter system view. | system-view | N/A
2. Enter OSPFv3 view. | ospfv3 [ process-id | vpn-instancevpn-instance-name ] * | N/A
3. Enter OSPFv3 area view. | area area-id | N/A
4. Apply an IPsec profile to a virtual link. | vlink-peer router-id [ dead seconds | hello seconds | instance instance-id | retransmit seconds | trans-delay seconds | ipsec-profile profile-name ] * | By default, no IPsec profile is applied.

To apply an IPsec profile to a sham link:

Step | Command | Remarks
---|---|---
1. Enter system view. | system-view | N/A
2. Enter OSPFv3 view. | ospfv3 [ process-id | vpn-instancevpn-instance-name ] * | N/A
3. Enter OSPFv3 area view. | area area-id | N/A
4. Apply an IPsec profile to a sham link. | sham-link source-ipv6-address destination-ipv6-address [ cost cost-value | dead dead-interval | hello hello-interval | instance instance-id | ipsec-profile profile-name | retransmit retrans-interval | trans-delay delay ] * | By default, no IPsec profile is applied.

Displaying and maintaining OSPFv3

Execute **display** commands in any view and **reset** commands in user view.

Task | Command
---|---
Display information about the routes to OSPFv3 ABR and ASBR. | display ospfv3 [ process-id ] abr-asbr
Display summary route information on the OSPFv3 ABR. | display ospfv3 [ process-id ] [ area area-id ] abr-summary [ ipv6-address prefix-length ] [ verbose ]
Display summary route information on the OSPFv3 ASBR. | display ospfv3 [ process-id ] asbr-summary [ ipv6-address prefix-length ] [ verbose ]
Display OSPFv3 log information. | display ospfv3 [ process-id ] event-log { isa-flush | peer | spf }
Display OSPFv3 process information. | display ospfv3 [ process-id ] [ verbose ]
Display OSPFv3 GR information. | display ospfv3 [ process-id ] graceful-restart [ verbose ]
<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display OSPFv3 NSR information.</td>
<td><code>display ospfv3 [ process-id ] non-stop-routing</code></td>
</tr>
<tr>
<td>Display OSPFv3 interface information.</td>
<td>`display ospfv3 [ process-id ] interface [ interface-type interface-number</td>
</tr>
<tr>
<td>Display OSPFv3 LSDB information.</td>
<td>`display ospfv3 [ process-id ] lsdb [ { external</td>
</tr>
<tr>
<td>Display OSPFv3 next hop information.</td>
<td><code>display ospfv3 [ process-id ] nexthop</code></td>
</tr>
<tr>
<td>Display OSPFv3 neighbor information.</td>
<td>`display ospfv3 [ process-id ] area area-id peer [ [ interface-type interface-number ]</td>
</tr>
<tr>
<td>Display OSPFv3 request list information.</td>
<td>`display ospfv3 [ process-id ] area area-id request-queue [ interface-type interface-number ]</td>
</tr>
<tr>
<td>Display OSPFv3 retransmission list information.</td>
<td>`display ospfv3 [ process-id ] area area-id retrans-queue [ interface-type interface-number ]</td>
</tr>
<tr>
<td>Display OSPFv3 routing information.</td>
<td><code>display ospfv3 [ process-id ] routing [ ipv6-address prefix-length ]</code></td>
</tr>
<tr>
<td>Display OSPFv3 topology information.</td>
<td>`display ospfv3 [ process-id ] area area-id spf-tree</td>
</tr>
<tr>
<td>Display OSPFv3 statistics.</td>
<td><code>display ospfv3 [ process-id ] statistics [ error ]</code></td>
</tr>
<tr>
<td>Display OSPFv3 virtual link information.</td>
<td><code>display ospfv3 [ process-id ] vlink</code></td>
</tr>
<tr>
<td>Restart an OSPFv3 process.</td>
<td><code>reset ospfv3 [ process-id ] process [ graceful-restart ]</code></td>
</tr>
<tr>
<td>Restart OSPFv3 route redistribution.</td>
<td><code>reset ospfv3 [ process-id ] redistribution</code></td>
</tr>
<tr>
<td>Clear OSPFv3 statistics.</td>
<td><code>reset ospfv3 [ process-id ] statistics</code></td>
</tr>
</tbody>
</table>

**NOTE:**
Support for the `display ospfv3 [ process-id ] non-stop-routing` command depends on the device model. For more information, see *Layer 3—IP Routing Command Reference*.

**OSPFv3 configuration examples**

**OSPFv3 stub area configuration example**

**Network requirements**

As shown in Figure 102:
- Enable OSPFv3 on all routers.
- Split the AS into three areas.
- Configure Router B and Router C as ABRs to forward routing information between areas.
- Configure Area 2 as a stub area to reduce LSAs in the area without affecting route reachability.
Configuration procedure

1. Configure IPv6 addresses for interfaces. (Details not shown.)
2. Configure basic OSPFv3:

   # On Router A, enable OSPFv3 and specify the router ID as 1.1.1.1.
   <RouterA> system-view
   [RouterA] ospfv3 1
   [RouterA-ospfv3-1] router-id 1.1.1.1
   [RouterA-ospfv3-1] quit
   [RouterA] interface gigabitethernet 1/0/1
   [RouterA-GigabitEthernet1/0/1] ospfv3 1 area 1
   [RouterA-GigabitEthernet1/0/1] quit
   [RouterA] interface gigabitethernet 1/0/2
   [RouterA-GigabitEthernet1/0/2] ospfv3 1 area 1
   [RouterA-GigabitEthernet1/0/2] quit

   # On Router B, enable OSPFv3 and specify the router ID as 2.2.2.2.
   <RouterB> system-view
   [RouterB] ospfv3 1
   [RouterB-ospfv3-1] router-id 2.2.2.2
   [RouterB-ospfv3-1] quit
   [RouterB] interface gigabitethernet 1/0/1
   [RouterB-GigabitEthernet1/0/1] ospfv3 1 area 0
   [RouterB-GigabitEthernet1/0/1] quit
   [RouterB] interface gigabitethernet 1/0/2
   [RouterB-GigabitEthernet1/0/2] ospfv3 1 area 1
   [RouterB-GigabitEthernet1/0/2] quit

   # On Router C, enable OSPFv3 and specify the router ID as 3.3.3.3.
   <RouterC> system-view
   [RouterC] ospfv3 1
   [RouterC-ospfv3-1] router-id 3.3.3.3
   [RouterC-ospfv3-1] quit
   [RouterC] interface gigabitethernet 1/0/1
   [RouterC-GigabitEthernet1/0/1] ospfv3 1 area 0
   [RouterC-GigabitEthernet1/0/1] quit
   [RouterC] interface gigabitethernet 1/0/2
   [RouterC-GigabitEthernet1/0/2] ospfv3 1 area 2
# On Router D, enable OSPFv3 and specify the router ID as 4.4.4.4.

```
<RouterD> system-view
[RouterD] ospfv3 1
[RouterD-ospfv3-1] router-id 4.4.4.4
[RouterD-ospfv3-1] quit
[RouterD] interface gigabitethernet 1/0/2
[RouterD-GigabitEthernet1/0/2] ospfv3 1 area 2
[RouterD-GigabitEthernet1/0/2] quit
```

# Display OSPFv3 neighbors on Router B.

```
[RouterB] display ospfv3 peer
```

```
Area: 0.0.0.0
-------------------------------------------------------------
Router ID       Pri State             Dead-Time InstID Interface
3.3.3.3         1   Full/BDR          00:00:40  0      GE1/0/1

Area: 0.0.0.1
-------------------------------------------------------------
Router ID       Pri State             Dead-Time InstID Interface
1.1.1.1         1   Full/DR           00:00:40  0      GE1/0/2
```

# Display OSPFv3 neighbors on Router C.

```
[RouterC] display ospfv3 peer
```

```
Area: 0.0.0.0
-------------------------------------------------------------
Router ID       Pri State             Dead-Time InstID Interface
2.2.2.2         1   Full/DR           00:00:40  0      GE1/0/1

Area: 0.0.0.2
-------------------------------------------------------------
Router ID       Pri State             Dead-Time InstID Interface
4.4.4.4         1   Full/BDR          00:00:40  0      GE1/0/2
```

# Display OSPFv3 neighbors on Router D.

```
[RouterD] dis ospfv3 routing
```

```
OSPFv3 Process 1 with Router ID 4.4.4.4
-------------------------------------------------------------
I  - Intra area route,  E1 - Type 1 external route,  N1 - Type 1 NSSA route
IA - Inter area route,  E2 - Type 2 external route,  N2 - Type 2 NSSA route
*  - Selected route

*Destination: 2001::/64
Type    : IA                                        Cost    : 2
```
Nexthop : FE80::42EA:A7FF:FE51:206  Interface: GE1/0/2
AdvRouter : 3.3.3.3  Area : 0.0.0.2
Preference : 10

*Destination: 2001:1::/64
Type : IA  Cost : 3
Nexthop : FE80::42EA:A7FF:FE51:206  Interface: GE1/0/2
AdvRouter : 3.3.3.3  Area : 0.0.0.2
Preference : 10

*Destination: 2001:2::/64
Type : I  Cost : 1
Nexthop : ::  Interface: GE0/1
AdvRouter : 3.3.3.3  Area : 0.0.0.2
Preference : 10

*Destination: 2001:3::/64
Type : IA  Cost : 4
Nexthop : FE80::42EA:A7FF:FE51:206  Interface: GE1/0/2
AdvRouter : 3.3.3.3  Area : 0.0.0.2
Preference : 10

Total: 4
Intra area: 1  Inter area: 3  ASE: 0  NSSA: 0

3. Configure Area 2 as a stub area:
   # Configure Router D.
   [RouterD] ospfv3
   [RouterD-ospfv3-1] area 2
   [RouterD-ospfv3-1-area-0.0.0.2] stub
   [RouterD-ospfv3-1-area-0.0.0.2] quit
   [RouterD-ospfv3-1] quit

   # Configure Router C, and specify the cost of the default route sent to the stub area as 10.
   [RouterC] ospfv3
   [RouterC-ospfv3-1] area 2
   [RouterC-ospfv3-1-area-0.0.0.2] stub
   [RouterC-ospfv3-1-area-0.0.0.2] default-cost 10

   # Display OSPFV3 routing table on Router D.
   [RouterD]display ospfv3 routing

   OSPFv3 Process 1 with Router ID 4.4.4.4
   ----------------------------------------------------------------------
   I - Intra area route,  E1 - Type 1 external route,  N1 - Type 1 NSSA route
   IA - Inter area route,  E2 - Type 2 external route,  N2 - Type 2 NSSA route
   * - Selected route

   *Destination: ::/0
   Type : IA  Cost : 11
   Nexthop : FE80::42EA:A7FF:FE51:206  Interface: GE1/0/2
AdvRouter : 3.3.3.3  Area   : 0.0.0.2  Preference : 10

*Destination: 2001::/64
Type       : IA  Cost     : 2
Nexthop    : FE80::42EA:A7FF:FE51:206  Interface: GE1/0/2
AdvRouter  : 3.3.3.3  Area   : 0.0.0.2  Preference : 10

*Destination: 2001:1::/64
Type       : IA  Cost     : 3
Nexthop    : FE80::42EA:A7FF:FE51:206  Interface: GE1/0/2
AdvRouter  : 3.3.3.3  Area   : 0.0.0.2  Preference : 10

*Destination: 2001:2::/64
Type       : I  Cost     : 1
Nexthop    : ::  Interface: GE1/0/2
AdvRouter  : 4.4.4.4  Area   : 0.0.0.2  Preference : 10

*Destination: 2001:3::/64
Type       : IA  Cost     : 4
Nexthop    : FE80::42EA:A7FF:FE51:206  Interface: GE1/0/2
AdvRouter  : 3.3.3.3  Area   : 0.0.0.2  Preference : 10

Total: 5
Intra area: 1  Inter area: 4  ASE: 0  NSSA: 0

The output shows that a default route is added and its cost is the cost of a direct route plus the configured cost.

4. Configure Area 2 as a totally stub area to further reduce the stub area routing table size:

  # Configure Area 2 as a totally stub area on Router C.
  [RouterC-ospfv3-1-area-0.0.0.2] stub no-summary

  # Display OSPFv3 routing table on Router D.
  [Sysname]display ospfv3 routing

  OSPFv3 Process 1 with Router ID 4.4.4.4

  I - Intra area route,  E1 - Type 1 external route,  N1 - Type 1 NSSA route
  IA - Inter area route,  E2 - Type 2 external route,  N2 - Type 2 NSSA route
  * - Selected route

  *Destination: ::/0
  Type       : IA  Cost     : 11
  Nexthop    : FE80::42EA:A7FF:FE51:206  Interface: GE1/0/2
  AdvRouter  : 3.3.3.3  Area   : 0.0.0.2  Preference : 10
*Destination: 2001:2::/64
  Type       : I                                         Cost     : 1
  Nexthop    : ::                                        Interface: GE1/0/2
  AdvRouter  : 4.4.4.4                                   Area     : 0.0.0.2
  Preference : 10
  Total: 2
  Intra area: 1         Inter area: 1         ASE: 0         NSSA: 0

The output shows that route entries are reduced. All indirect routes are removed, except the default route.

**OSPFv3 NSSA area configuration example**

**Network requirements**

As shown in Figure 103:
- Configure OSPFv3 on all routers and split the AS into three areas.
- Configure Router B and Router C as ABRs to forward routing information between areas.
- Configure Area 1 as an NSSA area and configure Router A as an ASBR to redistribute static routes into the AS.

**Figure 103 Network diagram**

**Configuration procedure**

1. Configure IPv6 addresses for interfaces. (Details not shown.)
2. Configure basic OSPFv3 (see "OSPFv3 stub area configuration example").
3. Configure Area 1 as an NSSA area:
   ```
   # Configure Router A.
   <RouterA> system-view
   [RouterA] ospfv3
   [RouterA-ospfv3-1] area 1
   [RouterA-ospfv3-1-area-0.0.0.1] nssa
   [RouterA-ospfv3-1-area-0.0.0.1-area-0.0.0.1] quit
   [RouterA-ospfv3-1-area-0.0.0.1-area-0.0.0.1] quit
   # Configure Router B.
   <RouterB> system-view
   [RouterB] ospfv3
   ```
[RouterB-ospfv3-1] area 1
[RouterB-ospfv3-1-area-0.0.0.1] nssa
[RouterB-ospfv3-1-area-0.0.0.1] quit
[RouterB-ospfv3-1] quit

# Display OSPFv3 routing information on Router A.
[RouterA]display ospfv3 routing

OSPFv3 Process 1 with Router ID 1.1.1.1

I - Intra area route,  E1 - Type 1 external route,  N1 - Type 1 NSSA route
IA - Inter area route,  E2 - Type 2 external route,  N2 - Type 2 NSSA route
* - Selected route

*Destination: 2001::/64
Type       : IA                                        Cost     : 2
Nexthop    : FE80::42EA:A2FF:FE03:106                  Interface: GE1/0/2
AdvRouter  : 2.2.2.2                                   Area     : 0.0.0.1
Preference : 10

*Destination: 2001:1::/64
Type       : I                                         Cost     : 1
Nexthop    : ::                                        Interface: GE1/0/2
AdvRouter  : 1.1.1.1                                   Area     : 0.0.0.1
Preference : 10

*Destination: 2001:2::/64
Type       : IA                                        Cost     : 3
Nexthop    : FE80::42EA:A2FF:FE03:106                  Interface: GE1/0/2
AdvRouter  : 2.2.2.2                                   Area     : 0.0.0.1
Preference : 10

*Destination: 2001:3::/64
Type       : I                                         Cost     : 1
Nexthop    : ::                                        Interface: GE1/0/2
AdvRouter  : 1.1.1.1                                   Area     : 0.0.0.1
Preference : 10

Total: 4
Intra area: 2         Inter area: 2         ASE: 0         NSSA: 0

4. Configure route redistribution:

# Configure an IPv6 static route, and configure OSPFv3 to redistribute the static route on Router A.
[RouterA] ipv6 route-static 1234:: 64 null 0
[RouterA] ospfv3 1
[RouterA-ospfv3-1] import-route static
[RouterA-ospfv3-1] quit

# Display OSPFv3 routing information on Router D.
[Sysname]display ospfv3 routing
OSPFv3 Process 1 with Router ID 4.4.4.4

I - Intra area route,   E1 - Type 1 external route,   N1 - Type 1 NSSA route
IA - Inter area route,   E2 - Type 2 external route,   N2 - Type 2 NSSA route
* - Selected route

*Destination: ::/0
Type : IA                          Cost : 11
Nexthop : FE80::42EA:A7FF:FE51:206  Interface: GE1/0/2
AdvRouter : 3.3.3.3                  Area : 0.0.0.2
Preference : 10

*Destination: 2001:2::/64
Type : I                          Cost : 1
Nexthop : ::                         Interface: GE1/0/2
AdvRouter : 4.4.4.4                  Area : 0.0.0.2
Preference : 10

Total: 2
Intra area: 1   Inter area: 1   ASE: 0   NSSA: 0

The output shows an AS external route imported from the NSSA area exists on Router D.

OSPFv3 DR election configuration example

Network requirements

As shown in Figure 104:

- Configure router priority 100 for Router A, the highest priority on the network, so it will become the DR.
- Configure router priority 2 for Router C, the second highest priority on the network, so it will become the BDR.
- Configure router priority 0 for Router B, so it cannot become a DR or BDR.
- Router D uses the default router priority 1.

Figure 104 Network diagram
Configuration procedure

1. Configure IPv6 addresses for interfaces. (Details not shown.)

2. Configure basic OSPFv3:

   # On Router A, enable OSPFv3, and specify the router ID as 1.1.1.1.
   <RouterA> system-view
   [RouterA] ospfv3
   [RouterA-ospfv3-1] router-id 1.1.1.1
   [RouterA-ospfv3-1] quit
   [RouterA] interface gigabitethernet 1/0/1
   [RouterA-GigabitEthernet1/0/1] ospfv3 1 area 0
   [RouterA-GigabitEthernet1/0/1] quit

   # On Router B, enable OSPFv3, and specify the router ID as 2.2.2.2.
   <RouterB> system-view
   [RouterB] ospfv3
   [RouterB-ospfv3-1] router-id 2.2.2.2
   [RouterB-ospfv3-1] quit
   [RouterB] interface gigabitethernet 1/0/1
   [RouterB-GigabitEthernet1/0/1] ospfv3 1 area 0
   [RouterB-GigabitEthernet1/0/1] quit

   # On Router C, enable OSPFv3, and specify the router ID as 3.3.3.3.
   <RouterC> system-view
   [RouterC] ospfv3
   [RouterC-ospfv3-1] router-id 3.3.3.3
   [RouterC-ospfv3-1] quit
   [RouterC] interface gigabitethernet 1/0/1
   [RouterC-GigabitEthernet1/0/1] ospfv3 1 area 0
   [RouterC-GigabitEthernet1/0/1] quit

   # On Router D, enable OSPFv3, and specify the router ID as 4.4.4.4.
   <RouterD> system-view
   [RouterD] ospfv3
   [RouterD-ospfv3-1] router-id 4.4.4.4
   [RouterD-ospfv3-1] quit
   [RouterD] interface gigabitethernet 1/0/1
   [RouterD-GigabitEthernet1/0/1] ospfv3 1 area 0
   [RouterD-GigabitEthernet1/0/1] quit

   # Display neighbors on Router A. The routers have the same default router priority 1, so Router
   D (the router with the highest router ID) is elected as the DR, and Router C is the BDR.
   [RouterA] display ospfv3 peer

     OSPFv3 Process 1 with Router ID 1.1.1.1

      Area: 0.0.0.0

-------------------------------------------------------------------------
Router ID Pri State Dead-Time InstID Interface
2.2.2.2 0 2-Way/DROther 00:00:36 0 GE1/0/1
3.3.3.3 2 Full/BDR 00:00:35 0 GE1/0/1
4.4.4.4 1 Full/DR 00:00:33 0 GE1/0/1

# Display neighbors on Router D. The neighbor states are all full.
Configure router priorities for interfaces:

3. Configure router priorities for interfaces:

# Set the router priority to 100 for the interface GigabitEthernet 1/0/1 of Router A.
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] ospfv3 dr-priority 100
[RouterA-GigabitEthernet1/0/1] quit

# Set the router priority to 0 for the interface GigabitEthernet 1/0/1 of Router B.
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] ospfv3 dr-priority 0
[RouterB-GigabitEthernet1/0/1] quit

# Set the router priority to 2 for the interface GigabitEthernet 1/0/1 of Router C.
[RouterC] interface gigabitethernet 1/0/1
[RouterC-GigabitEthernet1/0/1] ospfv3 dr-priority 2
[RouterC-GigabitEthernet1/0/1] quit

# Display neighbors on Router A. The output shows that the router priorities have been changed, but the DR and BDR are not changed.
[RouterA] display ospfv3 peer

OSPFv3 Process 1 with Router ID 1.1.1.1

Area: 0.0.0.0

<table>
<thead>
<tr>
<th>Router ID</th>
<th>Pri State</th>
<th>Dead-Time</th>
<th>InstID</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2.2.2</td>
<td>1 2-Way/DROther</td>
<td>00:00:36</td>
<td>0</td>
<td>GE1/0/1</td>
</tr>
<tr>
<td>3.3.3.3</td>
<td>1 Full/BDR</td>
<td>00:00:35</td>
<td>0</td>
<td>GE1/0/1</td>
</tr>
<tr>
<td>4.4.4.4</td>
<td>1 Full/DR</td>
<td>00:00:33</td>
<td>0</td>
<td>GE1/0/1</td>
</tr>
</tbody>
</table>

# Display neighbors on Router D.
[RouterD] display ospfv3 peer

OSPFv3 Process 1 with Router ID 4.4.4.4

Area: 0.0.0.0

<table>
<thead>
<tr>
<th>Router ID</th>
<th>Pri State</th>
<th>Dead-Time</th>
<th>InstID</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.1</td>
<td>1 Full/DROther</td>
<td>00:00:30</td>
<td>0</td>
<td>GE1/0/1</td>
</tr>
<tr>
<td>2.2.2.2</td>
<td>1 Full/DROther</td>
<td>00:00:37</td>
<td>0</td>
<td>GE1/0/1</td>
</tr>
<tr>
<td>3.3.3.3</td>
<td>1 Full/BDR</td>
<td>00:00:31</td>
<td>0</td>
<td>GE1/0/1</td>
</tr>
</tbody>
</table>

The output shows that the DR is still Router D.

4. Enable DR/BDR election:
# Perform the **shutdown** and **undo shutdown** commands on each interface to enable a new DR/BD election. (Details not shown.)

# Display neighbors on Router A. The output shows that Router C becomes the BDR.

```
[RouterA] display ospfv3 peer

OSPFv3 Process 1 with Router ID 1.1.1.1

Area: 0.0.0.0

<table>
<thead>
<tr>
<th>Router ID</th>
<th>Pri</th>
<th>State</th>
<th>Dead-Time</th>
<th>InstID</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2.2.2</td>
<td>0</td>
<td>Full/DROther</td>
<td>00:00:36</td>
<td>0</td>
<td>GE1/0/1</td>
</tr>
<tr>
<td>3.3.3.3</td>
<td>2</td>
<td>Full/BDR</td>
<td>00:00:35</td>
<td>0</td>
<td>GE1/0/1</td>
</tr>
<tr>
<td>4.4.4.4</td>
<td>1</td>
<td>Full/DROther</td>
<td>00:00:33</td>
<td>0</td>
<td>GE1/0/1</td>
</tr>
</tbody>
</table>
```

# Display neighbors on Router D.

```
[RouterD] display ospfv3 peer

OSPFv3 Process 1 with Router ID 4.4.4.4

Area: 0.0.0.0

<table>
<thead>
<tr>
<th>Router ID</th>
<th>Pri</th>
<th>State</th>
<th>Dead-Time</th>
<th>InstID</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.1</td>
<td>100</td>
<td>Full/DR</td>
<td>00:00:30</td>
<td>0</td>
<td>GE1/0/1</td>
</tr>
<tr>
<td>2.2.2.2</td>
<td>0</td>
<td>2-Way/DROther</td>
<td>00:00:37</td>
<td>0</td>
<td>GE1/0/1</td>
</tr>
<tr>
<td>3.3.3.3</td>
<td>2</td>
<td>Full/BDR</td>
<td>00:00:31</td>
<td>0</td>
<td>GE1/0/1</td>
</tr>
</tbody>
</table>
```

The output shows that Router A becomes the DR.

### OSPFv3 route redistribution configuration example

**Network requirements**

As shown in Figure 105:

- Router A, Router B, and Router C are in Area 2.
- OSPFv3 process 1 and OSPFv3 process 2 run on Router B. Router B communicates with Router A and Router C through OSPFv3 process 1 and OSPFv3 process 2.
- Configure OSPFv3 process 2 to redistribute direct routes and the routes from OSPFv3 process 1 on Router B, and set the default metric for redistributed routes to 3. Router C can then learn the routes destined for 1::0/64 and 2::0/64, and Router A cannot learn the routes destined for 3::0/64 or 4::0/64.

**Figure 105 Network diagram**
Configuration procedure

1. Configure IPv6 addresses for interfaces. (Details not shown.)
2. Configure basic OSPFv3:

   # Enable OSPFv3 process 1 on Router A.
   <RouterA> system-view
   [RouterA] ospfv3 1
   [RouterA-ospfv3-1] router-id 1.1.1.1
   [RouterA-ospfv3-1] quit
   [RouterA] interface gigabitethernet 1/0/2
   [RouterA-GigabitEthernet1/0/2] ospfv3 1 area 2
   [RouterA-GigabitEthernet1/0/2] quit
   [RouterA] interface gigabitethernet 1/0/1
   [RouterA-GigabitEthernet1/0/1] ospfv3 1 area 2
   [RouterA-GigabitEthernet1/0/1] quit

   # Enable OSPFv3 process 1 and OSPFv3 process 2 on Router B.
   <RouterB> system-view
   [RouterB] ospfv3 1
   [RouterB-ospfv3-1] router-id 2.2.2.2
   [RouterB-ospfv3-1] quit
   [RouterB] interface gigabitethernet 1/0/2
   [RouterB-GigabitEthernet1/0/2] ospfv3 1 area 2
   [RouterB-GigabitEthernet1/0/2] quit
   [RouterB] ospfv3 2
   [RouterB-ospfv3-2] router-id 3.3.3.3
   [RouterB-ospfv3-2] quit
   [RouterB] interface gigabitethernet 1/0/1
   [RouterB-GigabitEthernet1/0/1] ospfv3 2 area 2
   [RouterB-GigabitEthernet1/0/1] quit

   # Enable OSPFv3 process 2 on Router C.
   <RouterC> system-view
   [RouterC] ospfv3 2
   [RouterC-ospfv3-2] router-id 4.4.4.4
   [RouterC-ospfv3-2] quit
   [RouterC] interface gigabitethernet 1/0/2
   [RouterC-GigabitEthernet1/0/2] ospfv3 2 area 2
   [RouterC-GigabitEthernet1/0/2] quit
   [RouterC] interface gigabitethernet 1/0/1
   [RouterC-GigabitEthernet1/0/1] ospfv3 2 area 2
   [RouterC-GigabitEthernet1/0/1] quit

   # Display the routing table on Router C.
   [RouterC] display ipv6 routing-table

   Destinations : 7 Routes : 7

   Destination: ::1/128                          Protocol : Direct
   NextHop     : ::1                             Preference: 0
   Interface   : InLoop0                         Cost     : 0
3. Configure OSPFv3 route redistribution:

# Configure OSPFv3 process 2 to redistribute direct routes and the routes from OSPFv3 process 1 on Router B.

[RouterB] ospfv3 2
[RouterB-ospfv3-2] import-route ospfv3 1
[RouterB-ospfv3-2] import-route direct
[RouterB-ospfv3-2] quit

# Display the routing table on Router C.

[RouterC] display ipv6 routing-table

Destinations : 9 Routes : 9

Destination: ::1/128  Protocol : Direct
NextHop : ::1 Preference: 0
Interface : InLoop0 Cost : 0

Destination: 1::/64  Protocol : O_ASE2
NextHop : FE80::200:CFF:FE01:1C03 Preference: 150
Interface : GE1/0/2 Cost : 3

Destination: 2::/64  Protocol : O_ASE2
NextHop : FE80::200:CFF:FE01:1C03 Preference: 150
Interface : GE1/0/2 Cost : 3

Destination: 3::/64  Protocol : Direct
**OSPFv3 route summarization configuration example**

**Network requirements**

As shown in Figure 106:

- Router A, Router B, and Router C are in Area 2.
- OSPFv3 process 1 and OSPFv3 process 2 run on Router B. Router B communicates with Router A and Router C through OSPFv3 process 1 and OSPFv3 process 2, respectively.
- On Router A, configure IPv6 addresses 2:1:1::1/64, 2:1:2::1/64, and 2:1:3::1/64 for GigabitEthernet 1/0/1.
- On Router B, configure OSPFv3 process 2 to redistribute direct routes and the routes from OSPFv3 process 1. Router C can then learn the routes destined for 2::/64, 2:1:1::/64, 2:1:2::/64, and 2:1:3::/64.
- On Router B, configure route summarization to advertise only summary route 2::/16 to Router C.

Figure 106 Network diagram
Configuration procedure

1. Configure IPv6 addresses for interfaces. (Details not shown.)

2. Configure OSPFv3:

   # Enable OSPFv3 process 1 on Router A.
   <RouterA> system-view
   [RouterA] ospfv3 1
   [RouterA-ospfv3-1] router-id 1.1.1.1
   [RouterA-ospfv3-1] quit
   [RouterA] interface gigabitethernet 1/0/2
   [RouterA-GigabitEthernet1/0/2] ospfv3 1 area 2
   [RouterA-GigabitEthernet1/0/2] quit
   [RouterA] interface gigabitethernet 1/0/1
   [RouterA-GigabitEthernet1/0/1] ipv6 address 2:1:1::1 64
   [RouterA-GigabitEthernet1/0/1] ipv6 address 2:1:2::1 64
   [RouterA-GigabitEthernet1/0/1] ipv6 address 2:1:3::1 64
   [RouterA-GigabitEthernet1/0/1] ospfv3 1 area 2
   [RouterA-GigabitEthernet1/0/1] quit

   # Enable OSPFv3 process 1 and OSPFv3 process 2 on Router B.
   <RouterB> system-view
   [RouterB] ospfv3 1
   [RouterB-ospfv3-1] router-id 2.2.2.2
   [RouterB-ospfv3-1] quit
   [RouterB] interface gigabitethernet 1/0/2
   [RouterB-GigabitEthernet1/0/2] ospfv3 1 area 2
   [RouterB-GigabitEthernet1/0/2] quit
   [RouterB] ospfv3 2
   [RouterB-ospfv3-2] router-id 3.3.3.3
   [RouterB-ospfv3-2] quit
   [RouterB] interface gigabitethernet 1/0/1
   [RouterB-GigabitEthernet1/0/1] ipv6 address 2:1:1::1 64
   [RouterB-GigabitEthernet1/0/1] ipv6 address 2:1:2::1 64
   [RouterB-GigabitEthernet1/0/1] ipv6 address 2:1:3::1 64
   [RouterB-GigabitEthernet1/0/1] ospfv3 1 area 2
   [RouterB-GigabitEthernet1/0/1] quit

   # Enable OSPFv3 process 2 on Router C.
   <RouterC> system-view
   [RouterC] ospfv3 2
   [RouterC-ospfv3-2] router-id 4.4.4.4
   [RouterC-ospfv3-2] quit
   [RouterC] interface gigabitethernet 1/0/2
   [RouterC-GigabitEthernet1/0/2] ospfv3 2 area 2
   [RouterC-GigabitEthernet1/0/2] quit
   [RouterC] interface gigabitethernet 1/0/1
   [RouterC-GigabitEthernet1/0/1] ospfv3 2 area 2
   [RouterC-GigabitEthernet1/0/1] quit

3. Configure OSPFv3 route redistribution:

   # Configure OSPFv3 process 2 to redistribute direct routes and the routes from OSPFv3 process 1 on Router B.
   [RouterB] ospfv3 2
   [RouterB-ospfv3-2] import-route ospfv3 1
   [RouterB-ospfv3-2] import-route direct
[RouterB-ospfv3-2] quit

# Display the routing table on Router C.
[RouterC] display ipv6 routing-table

Destinations : 12 Routes : 12

Destination: ::1/128 Protocol : Direct
NextHop    : ::1 Preference: 0
Interface  : InLoop0 Cost      : 0

Destination: 1::/64 Protocol : O_ASE2
NextHop    : FE80::200:CFF:FE01:1C03 Preference: 150
Interface  : GE1/0/2 Cost      : 1

Destination: 2::/64 Protocol : O_ASE2
NextHop    : FE80::200:CFF:FE01:1C03 Preference: 150
Interface  : GE1/0/2 Cost      : 1

Destination: 2:1:1::/64 Protocol : O_ASE2
NextHop    : FE80::200:CFF:FE01:1C03 Preference: 150
Interface  : GE1/0/2 Cost      : 1

Destination: 2:1:2::/64 Protocol : O_ASE2
NextHop    : FE80::200:CFF:FE01:1C03 Preference: 150
Interface  : GE1/0/2 Cost      : 1

Destination: 2:1:3::/64 Protocol : O_ASE2
NextHop    : FE80::200:CFF:FE01:1C03 Preference: 150
Interface  : GE1/0/2 Cost      : 1

Destination: 3::/64 Protocol : Direct
NextHop    : 3::2 Preference: 0
Interface  : GE1/0/2 Cost      : 0

Destination: 3::2/128 Protocol : Direct
NextHop    : ::1 Preference: 0
Interface  : InLoop0 Cost      : 0

Destination: 4::/64 Protocol : Direct
NextHop    : 4::1 Preference: 0
Interface  : GE1/0/1 Cost      : 0

Destination: 4:1/128 Protocol : Direct
NextHop    : ::1 Preference: 0
Interface  : InLoop0 Cost      : 0

Destination: FE80::/10 Protocol : Direct
NextHop    : :: Preference: 0
Configure ASBR route summarization:

# On Router B, configure OSPFv3 process 2 to advertise a summary route 2::/16.

[RouterB] ospfv3 2
[RouterB-ospfv3-2] asbr-summary 2:: 16
[RouterB-ospfv3-2] quit

# Display the routing table on Router C.

[RouterC] display ipv6 routing-table

Destinations : 9 Routes : 9

Destination: ::1/128 Protocol : Direct
NextHop : ::1 Preference: 0
Interface : InLoop0 Cost : 0

Destination: 1::/64 Protocol : O_ASE2
NextHop : FE80::200:CFF:FE01:1C03 Preference: 150
Interface : GE1/0/2 Cost : 1

Destination: 2::/16 Protocol : O_ASE2
NextHop : FE80::200:CFF:FE01:1C03 Preference: 150
Interface : GE1/0/2 Cost : 1

Destination: 3::/64 Protocol : Direct
NextHop : 3::2 Preference: 0
Interface : GE1/0/2 Cost : 0

Destination: 3::2/128 Protocol : Direct
NextHop : ::1 Preference: 0
Interface : InLoop0 Cost : 0

Destination: 4::/64 Protocol : Direct
NextHop : 4::1 Preference: 0
Interface : GE1/0/1 Cost : 0

Destination: 4::1/128 Protocol : Direct
NextHop : ::1 Preference: 0
Interface : InLoop0 Cost : 0

Destination: FE80::/10 Protocol : Direct
NextHop : :: Preference: 0
Interface : NULL0 Cost : 0

Destination: FF00::/8 Protocol : Direct
OSPFv3 GR configuration example

Network requirements

As shown in Figure 107:

- Router A, Router B, and Router C that reside in the same AS and the same OSPFv3 routing domain are GR capable.
- Router A acts as the GR restarter. Router B and Router C act as GR helpers, and synchronize their LSDBs with Router A through GR.

![Figure 107 Network diagram](image)

Configuration procedure

1. Configure IPv6 addresses for interfaces. (Details not shown.)
2. Configure basic OSPFv3:

   # On Router A, enable OSPFv3 process 1, enable GR, and set the router ID to 1.1.1.1.

   ```
   <RouterA> system-view
   [RouterA] ospfv3 1
   [RouterA-ospfv3-1] router-id 1.1.1.1
   [RouterA-ospfv3-1] graceful-restart enable
   [RouterA-ospfv3-1] quit
   [RouterA] interface gigabitethernet 1/0/1
   [RouterA-GigabitEthernet1/0/1] ospfv3 1 area 1
   [RouterA-GigabitEthernet1/0/1] quit
   # On Router B, enable OSPFv3 and set the router ID to 2.2.2.2. (By default, GR helper is enabled on a router.)
   <RouterB> system-view
   [RouterB] ospfv3 1
   [RouterB-ospfv3-1] router-id 2.2.2.2
   [RouterB-ospfv3-1] quit
   [RouterB] interface gigabitethernet 1/0/1
   [RouterB-GigabitEthernet1/0/1] ospfv3 1 area 1
   [RouterB-GigabitEthernet1/0/1] quit
   ```
# On Router C, enable OSPFv3 and set the router ID to 3.3.3.3. (By default, GR helper is enabled on a router.)

```bash
<RouterC> system-view
[RouterC] ospfv3 1
[RouterC-ospfv3-1] router-id 3.3.3.3
[RouterC-ospfv3-1] quit
[RouterC] interface gigabitethernet 1/0/1
[RouterC-GigabitEthernet1/0/1] ospfv3 1 area 1
[RouterC-GigabitEthernet1/0/1] quit
```

Verifying the configuration

# Perform an active/standby switchover on Router A to trigger an OSPFv3 GR operation. (Details not shown.)

**OSPFv3 NSR configuration example**

**Network requirements**

As shown in Figure 108, Router S, Router A, and Router B belong to the same AS and OSPFv3 routing domain. Enable OSPFv3 NSR on Router S to ensure correct routing when an active/standby switchover occurs on Router S.

**Figure 108 Network diagram**

![Network diagram](image)

**Configuration procedure**

1. Configure IP addresses and subnet masks for interfaces on the routers. (Details not shown.)
2. Configure OSPFv3 on the routers to ensure that Router S, Router A, and Router B can communicate with each other at Layer 3. (Details not shown.)
3. Configure OSPFv3:
   # On Router A, enable OSPFv3 and set the router ID to 1.1.1.1.
   ```bash
   <RouterA> system-view
   [RouterA] ospfv3 1
   [RouterA-ospfv3-1] router-id 1.1.1.1
   [RouterA-ospfv3-1] quit
   [RouterA] interface gigabitethernet 1/0/1
   [RouterA-GigabitEthernet1/0/1] ospfv3 1 area 1
   [RouterA-GigabitEthernet1/0/1] quit
   ```
   # On Router B, enable OSPFv3 and set the router ID to 2.2.2.2.
   ```bash
   <RouterB> system-view
   [RouterB] ospfv3 1
   [RouterB-ospfv3-1] router-id 2.2.2.2
   [RouterB-ospfv3-1] quit
   [RouterB] interface gigabitethernet 1/0/1
   [RouterB-GigabitEthernet1/0/1] ospfv3 1 area 1
   [RouterB-GigabitEthernet1/0/1] quit
   ```
   # On Router S, enable OSPFv3, set the router ID to 3.3.3.3, and enable NSR.
   ```bash
   ```
Verifying the configuration

# Verify the following:

- When an active/standby switchover occurs on Router S, the neighbor relationships and routing information on Router A and Router B have not changed. (Details not shown.)
- The traffic from Router A to Router B has not been impacted. (Details not shown.)

BFD for OSPFv3 configuration example

Network requirements

As shown in Figure 109:

- Configure OSPFv3 on Router A, Router B and Router C and configure BFD over the link Router A<—>L2 Switch<—>Router B.
- After the link Router A<—>L2 Switch<—>Router B fails, BFD can quickly detect the failure and notify OSPFv3 of the failure. Then Router A and Router B communicate through Router C.

Table 23 Interface and IP address assignment

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IPv6 address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router A</td>
<td>GE1/0/1</td>
<td>2001::1/64</td>
</tr>
<tr>
<td>Router A</td>
<td>GE1/0/2</td>
<td>2001::2/64</td>
</tr>
<tr>
<td>Router B</td>
<td>GE1/0/1</td>
<td>2001::3/64</td>
</tr>
<tr>
<td>Router B</td>
<td>GE1/0/2</td>
<td>2001::3/64</td>
</tr>
</tbody>
</table>
Configuration procedure

1. Configure IPv6 addresses for interfaces. (Details not shown.)
2. Configure basic OSPFv3:
   
   # Enable OSPFv3 and set the router ID to 1.1.1.1 on Router A.
   
   ```
   <RouterA> system-view
   [RouterA] ospfv3 1
   [RouterA-ospfv3-1] router-id 1.1.1.1
   [RouterA-ospfv3-1] quit
   [RouterA] interface gigabitethernet 1/0/1
   [RouterA-GigabitEthernet1/0/1] ospfv3 1 area 0
   [RouterA-GigabitEthernet1/0/1] quit
   [RouterA] interface gigabitethernet 1/0/2
   [RouterA-GigabitEthernet1/0/2] ospfv3 1 area 0
   [RouterA-GigabitEthernet1/0/2] quit
   ```
   
   # Enable OSPFv3 and set the router ID to 2.2.2.2 on Router B.
   
   ```
   <RouterB> system-view
   [RouterB] ospfv3 1
   [RouterB-ospfv3-1] router-id 2.2.2.2
   [RouterB-ospfv3-1] quit
   [RouterB] interface gigabitethernet 1/0/1
   [RouterB-GigabitEthernet1/0/1] ospfv3 1 area 0
   [RouterB-GigabitEthernet1/0/1] quit
   [RouterB] interface gigabitethernet 1/0/2
   [RouterB-GigabitEthernet1/0/2] ospfv3 1 area 0
   [RouterB-GigabitEthernet1/0/2] quit
   ```
   
   # Enable OSPFv3 and set the router ID to 3.3.3.3 on Router C.
   
   ```
   <RouterC> system-view
   [RouterC] ospfv3 1
   [RouterC-ospfv3-1] router-id 3.3.3.3
   [RouterC-ospfv3-1] quit
   [RouterC] interface gigabitethernet 1/0/1
   [RouterC-GigabitEthernet1/0/1] ospfv3 1 area 0
   [RouterC-GigabitEthernet1/0/1] quit
   [RouterC] interface gigabitethernet 1/0/2
   [RouterC-GigabitEthernet1/0/2] ospfv3 1 area 0
   [RouterC-GigabitEthernet1/0/2] quit
   ```

3. Configure BFD:
   
   # Enable BFD and configure BFD parameters on Router A.
   
   ```
   [RouterA] bfd session init-mode active
   [RouterA] interface gigabitethernet 1/0/1
   [RouterA-GigabitEthernet1/0/1] ospfv3 bfd enable
   ```
# Enable BFD and configure BFD parameters on Router B.

```
[RouterB] bfd session init-mode active
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] ospfv3 bfd enable
[RouterB-GigabitEthernet1/0/1] bfd min-transmit-interval 500
[RouterB-GigabitEthernet1/0/1] bfd min-receive-interval 500
[RouterB-GigabitEthernet1/0/1] bfd detect-multiplier 6
```

Verifying the configuration

```
# Display the BFD information on Router A.
<RouterA> display bfd session

Total Session Num: 1 Up Session Num: 1 Init Mode: Active

IPv6 Session Working Under Ctrl Mode:

Local Discr: 1441 Remote Discr: 1450
Source IP: FE80::20F:FF:FE00:1202 (link-local address of GigabitEthernet1/0/1 on Router A)
Destination IP: FE80::20F:FF:FE00:1200 (link-local address of GigabitEthernet1/0/1 on Router B)
Session State: Up Interface: GE1/0/1
Hold Time: 2319ms
```

```
# Display routes destined for 2001:4::/64 on Router A.
<RouterA> display ipv6 routing-table 2001:4::0 64

Summary Count : 1

Destination: 2001:4::/64 Protocol : O_INTRA
NextHop : FE80::20F:FF:FE00:1200 Preference: 10
Interface : GE1/0/1 Cost : 1
```

The output shows that Router A communicates with Router B through GigabitEthernet 1/0/1.

```
# Display routes destined for 2001:4::0/64 on Router A.
<RouterA> display ipv6 routing-table 2001:4::0 64

Summary Count : 1

Destination: 2001:4::/64 Protocol : O_INTRA
NextHop : FE80::BAAF:67FF:FE27:DCD0 Preference: 10
Interface : GE1/0/2 Cost : 2
```

The output shows that Router A communicates with Router B through GigabitEthernet 1/0/2.
OSPFv3 FRR configuration example

Network requirements

As shown in Figure 110, Router A, Router B, and Router C reside in the same OSPFv3 domain. Configure OSPFv3 FRR so that when Link A fails, traffic is immediately switched to Link B.

Figure 110 Network diagram

Table 24 Interface and IP address assignment

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router A</td>
<td>GE1/0/1</td>
<td>1::1/64</td>
<td>Router B</td>
<td>GE1/0/1</td>
<td>3::1/64</td>
</tr>
<tr>
<td></td>
<td>GE1/0/2</td>
<td>2::1/64</td>
<td></td>
<td>GE1/0/2</td>
<td>2::2/64</td>
</tr>
<tr>
<td></td>
<td>Loop0</td>
<td>10::1/128</td>
<td></td>
<td>Loop0</td>
<td>20::1/128</td>
</tr>
<tr>
<td>Router C</td>
<td>GE1/0/1</td>
<td>1::2/64</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>GE1/0/2</td>
<td>3::2/64</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Configuration procedure

1. Configure IPv6 addresses for interfaces on the routers. (Details not shown.)
2. Configure OSPFv3 on the routers to ensure that Router A, Router B, and Router C can communicate with each other at the network layer. (Details not shown.)
3. Configure OSPFv3 FRR:

   You can enable OSPFv3 FRR to either calculate a backup next hop by using the LFA algorithm, or specify a backup next hop by using a routing policy.

   - (Method 1.) Enable OSPFv3 FRR to calculate a backup next hop by using the LFA algorithm:

     # Configure Router A.

     <RouterA> system-view

     [RouterA] ospfv3 1

     [RouterA-ospfv3-1] fast-reroute lfa

     [RouterA-ospfv3-1] quit

     # Configure Router B.

     <RouterB> system-view

     [RouterB] ospfv3 1

     [RouterB-ospfv3-1] fast-reroute lfa

     [RouterB-ospfv3-1] quit

   - (Method 2.) Enable OSPFv3 FRR to specify a backup next hop by using a routing policy:

     # Configure Router A.

     <RouterA> system-view
[RouterA] ipv6 prefix-list abc index 10 permit 10::128
[RouterA] route-policy frr permit node 10
[RouterA-route-policy-frr-10] if-match ipv6 address prefix-list abc
[RouterA-route-policy-frr-10] apply ipv6 fast-reroute backup-interface gigabitethernet 1/0/1 backup-nexthop 1::2
[RouterA-route-policy-frr-10] quit
[RouterA] ospfv3 1
[RouterA-ospfv3-1] fast-reroute route-policy frr
[RouterA-ospfv3-1] quit

# Configure Router B.
<RouterB> system-view
[RouterB] ipv6 prefix-list abc index 10 permit 20::128
[RouterB] route-policy frr permit node 10
[RouterB-route-policy-frr-10] if-match ipv6 address prefix-list abc
[RouterB-route-policy-frr-10] apply ipv6 fast-reroute backup-interface gigabitethernet 1/0/1 backup-nexthop 3::2
[RouterB-route-policy-frr-10] quit
[RouterB] ospfv3 1
[RouterB-ospfv3-1] fast-reroute route-policy frr
[RouterB-ospfv3-1] quit

Verifying the configuration

# Display the route 20::1/128 on Router A to view the backup next hop information.
[RouterA] display ipv6 routing-table 20::1 128 verbose

Summary count : 1

Destination: 20::1/128
   Protocol: O_INTRA
   Process ID: 1
   SubProtID: 0x1                                      Age: 00h03m45s
      Cost: 6                                          Preference: 10
      IpPre: N/A                                      QosLocalID: N/A
      Tag: 0                                           State: Active Adv
      OrigTblID: 0x0                                    OrigVrf: default-vrf
      TableID: 0xa                                      OrigAs: 0
      NibID: 0x23000005                                LastAs: 0
      AttrID: 0xffffffff                               Neighbor: ::
      Flags: 0x10041                                   OrigNextHop: FE80::7685:45FF:FEAD:102
      Label: NULL                                      RealNextHop: FE80::7685:45FF:FEAD:102
      BkLabel: NULL                                    BkNextHop: FE80::34CD:9FF:FE2F:D02
      Tunnel ID: Invalid                               Interface: GigabitEthernet1/0/2
      BkTunnel ID: Invalid                             BkInterface: GigabitEthernet1/0/1
      FtnIndex: 0x0                                    TrafficIndex: N/A
      Connector: N/A

# Display the route 10::1/128 on Router B to view the backup next hop information.
[RouterB] display ipv6 routing-table 10::1 128 verbose

Summary count : 1
OSPFv3 IPsec profile configuration example

Network requirements

As shown in Figure 111, all routers run OSPFv3, and the AS is divided into two areas. Configure IPsec profiles on the routers to authenticate and encrypt protocol packets.

Figure 111 Network diagram

Configuration procedure

1. Configure IPv6 addresses for interfaces. (Details not shown.)
2. Configure OSPFv3 basic features:
   # On Router A, enable OSPFv3 and specify the router ID as 1.1.1.1.
   <RouterA> system-view
   [RouterA] ospfv3 1
   [RouterA-ospfv3-1] router-id 1.1.1.1
   [RouterA-ospfv3-1] quit
   [RouterA] interface gigabitethernet 1/0/2
On Router B, enable OSPFv3 and specify the router ID as 2.2.2.2.

```
<RouterB> system-view
[RouterB] ospfv3 1
[RouterB-ospfv3-1] router-id 2.2.2.2
[RouterB-ospfv3-1] quit
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] ospfv3 1 area 0
[RouterB-GigabitEthernet1/0/1] quit
[RouterB] interface gigabitethernet 1/0/2
[RouterB-GigabitEthernet1/0/2] ospfv3 1 area 1
[RouterB-GigabitEthernet1/0/2] quit
```

On Router C, enable OSPFv3 and specify the router ID as 3.3.3.3.

```
<RouterC> system-view
[RouterC] ospfv3 1
[RouterC-ospfv3-1] router-id 3.3.3.3
[RouterC-ospfv3-1] quit
[RouterC] interface gigabitethernet 1/0/1
[RouterC-GigabitEthernet1/0/1] ospfv3 1 area 0
[RouterC-GigabitEthernet1/0/1] quit
```

3. Configure OSPFv3 IPsec profiles:
   - **On Router A:**
     - # Create an IPsec transform set named trans.
       ```
       [RouterA] ipsec transform-set trans
       ```
     - # Specify the encapsulation mode as transport.
       ```
       [RouterA-ipsec-transform-set-trans] encapsulation-mode transport
       ```
     - # Specify the ESP encryption and authentication algorithms.
       ```
       ```
       ```
       ```
     - # Specify the AH authentication algorithm.
       ```
       [RouterA-ipsec-transform-set-trans] ah authentication-algorithm md5
       ```
     - # Create a manual IPsec profile named profile001.
       ```
       [RouterA] ipsec profile profile001 manual
       ```
     - # Use IPsec transform set trans.
       ```
       [RouterA-ipsec-profile-profile001-manual] transform-set trans
       ```
     - # Configure the inbound and outbound SPIs for AH.
       ```
       [RouterA-ipsec-profile-profile001-manual] sa spi inbound ah 100000
       ```
       ```
       [RouterA-ipsec-profile-profile001-manual] sa spi outbound ah 100000
       ```
     - # Configure the inbound and outbound SPIs for ESP.
       ```
       [RouterA-ipsec-profile-profile001-manual] sa spi inbound esp 200000
       ```
       ```
       [RouterA-ipsec-profile-profile001-manual] sa spi outbound esp 200000
       ```
     - # Configure the inbound and outbound SA keys for AH.
       ```
       [RouterA-ipsec-profile-profile001-manual] sa string-key inbound ah simple abc
       ```
       ```
       [RouterA-ipsec-profile-profile001-manual] sa string-key outbound ah simple abc
       ```
     - # Configure the inbound and outbound SA keys for ESP.
On Router B:

# Create an IPsec transform set named trans.
[RouterB] ipsec transform-set trans

# Specify the encapsulation mode as transport.
[RouterB-ipsec-transform-set-trans] encapsulation-mode transport

# Specify the ESP encryption and authentication algorithms.
[RouterB-ipsec-transform-set-trans] esp encryption-algorithm 3des-cbc
[RouterB-ipsec-transform-set-trans] esp authentication-algorithm md5

# Specify the AH authentication algorithm.
[RouterB-ipsec-transform-set-trans] ah authentication-algorithm md5

# Create a manual IPsec profile named profile001.
[RouterB] ipsec profile profile001 manual

# Use IPsec transform set trans.
[RouterB-ipsec-profile-profile001-manual] transform-set trans

# Configure the inbound and outbound SPIs for AH.
[RouterB-ipsec-profile-profile001-manual] sa spi inbound ah 100000
[RouterB-ipsec-profile-profile001-manual] sa spi outbound ah 100000

# Configure the inbound and outbound SPIs for ESP.
[RouterB-ipsec-profile-profile001-manual] sa spi inbound esp 200000
[RouterB-ipsec-profile-profile001-manual] sa spi outbound esp 200000

# Configure the inbound and outbound SA keys for AH.
[RouterB-ipsec-profile-profile001-manual] sa string-key inbound ah simple abc
[RouterB-ipsec-profile-profile001-manual] sa string-key outbound ah simple abc

# Configure the inbound and outbound SA keys for ESP.
[RouterB-ipsec-profile-profile001-manual] sa string-key inbound esp simple 123
[RouterB-ipsec-profile-profile001-manual] sa string-key outbound esp simple 123

# Create a manual IPsec profile named profile002.
[RouterB] ipsec profile profile002 manual

# Use IPsec transform set trans.
[RouterB-ipsec-profile-profile002-manual] transform-set trans

# Configure the inbound and outbound SPIs for AH.
[RouterB-ipsec-profile-profile002-manual] sa spi inbound ah 400000
[RouterB-ipsec-profile-profile002-manual] sa spi outbound ah 400000

# Configure the inbound and outbound SPIs for ESP.
[RouterB-ipsec-profile-profile002-manual] sa spi inbound esp 256
[RouterB-ipsec-profile-profile002-manual] sa spi outbound esp 256

# Configure the inbound and outbound SA keys for AH.
[RouterB-ipsec-profile-profile002-manual] sa string-key inbound ah simple hello
[RouterB-ipsec-profile-profile002-manual] sa string-key outbound ah simple hello

# Configure the inbound and outbound SA keys for ESP.
[RouterB-ipsec-profile-profile002-manual] sa string-key inbound esp simple byebye
4. Apply the IPsec profiles to areas:

   # Configure Router A.
   [RouterA] ospfv3 1
   [RouterA-ospfv3-1] area 1
   [RouterA-ospfv3-1-area-0.0.0.1] enable ipsec-profile profile001
   [RouterA-ospfv3-1-area-0.0.0.1] quit
   [RouterA-ospfv3-1] quit

   # Configure Router B.
   [RouterB] ospfv3 1
   [RouterB-ospfv3-1] area 0
   [RouterB-ospfv3-1-area-0.0.0.0] enable ipsec-profile profile002
   [RouterB-ospfv3-1-area-0.0.0.0] quit
   [RouterB-ospfv3-1-area-0.0.0.1] enable ipsec-profile profile001
   [RouterB-ospfv3-1-area-0.0.0.1] quit
# Configure Router C.

[RouterC] ospfv3 1
[RouterC-ospfv3-1] area 0
[RouterC-ospfv3-1-area-0.0.0.0] enable ipsec-profile profile002
[RouterC-ospfv3-1-area-0.0.0.0] quit
[RouterC-ospfv3-1] quit

Verifying the configuration

# Verify that OSPFv3 packets between Routers A, B, and C are protected by IPsec. (Details not shown.)
Configuring IPv6 IS-IS

Overview

IPv6 IS-IS supports all IPv4 IS-IS features except that it advertises IPv6 routing information. This chapter describes only IPv6 IS-IS specific configuration tasks. For information about IS-IS, see "Configuring IS-IS."

Intermediate System-to-Intermediate System (IS-IS) supports multiple network protocols, including IPv6. To support IPv6, the IETF added two type-length-values (TLVs) and a new network layer protocol identifier (NLPID).

The TLVs are as follows:

- **IPv6 Reachability**—Contains routing prefix and metric information to describe network reachability and has a type value of 236 (0xEC).
- **IPv6 Interface Address**—Same as the "IP Interface Address" TLV in IPv4 ISIS, except that the 32-bit IPv4 address is translated to the 128-bit IPv6 address.

The new NLPID is an 8-bit field that identifies which network layer protocol is supported. For IPv6, the NLPID is 142 (0x8E), which must be carried in hello packets sent by IPv6 IS-IS.

Configuring basic IPv6 IS-IS

Before you configure basic IPv6 IS-IS, complete the following tasks:

- Configure IPv6 addresses for interfaces to ensure IPv6 connectivity between neighboring nodes.
- Enable IS-IS.

Basic IPv6 IS-IS configuration can implement the interconnection of IPv6 networks.

To configure basic IPv6 IS-IS:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable an IS-IS process and enter IS-IS view.</td>
<td>isis [ process-id ] [ vpn-instance vpn-instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the network entity title (NET) for the IS-IS process.</td>
<td>network-entity net</td>
</tr>
<tr>
<td>4.</td>
<td>Create the IPv6 address family and enter its view.</td>
<td>address-family ipv6 [ unicast ]</td>
</tr>
<tr>
<td>5.</td>
<td>Return to IS-IS view.</td>
<td>quit</td>
</tr>
<tr>
<td>6.</td>
<td>Return to system view.</td>
<td>quit</td>
</tr>
<tr>
<td>7.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>8.</td>
<td>Enable IPv6 for IS-IS on the interface.</td>
<td>isis ipv6 enable [ process-id ]</td>
</tr>
</tbody>
</table>
## Configuring IPv6 IS-IS route control

Before you configure IPv6 IS-IS route control, complete basic IPv6 IS-IS configuration.

To configure IPv6 IS-IS route control:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter IS-IS view.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>isis [process-id] [vpn-instance vpn-instance-name]</code></td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>Enter IS-IS IPv6 address family view.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>address-family ipv6 [unicast]</code></td>
<td>N/A</td>
</tr>
<tr>
<td>4.</td>
<td>Specify a preference for IPv6 IS-IS routes.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>`preference {route-policy route-policy-name</td>
<td>preference} *`</td>
</tr>
<tr>
<td>5.</td>
<td>Configure an IPv6 IS-IS summary route.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>`summary ipv6-pref fix prefix-length [avoid-feedback</td>
<td>generate_null0_route</td>
</tr>
<tr>
<td>6.</td>
<td>Configure IPv6 IS-IS to advertise a default route.</td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td>Configure IPv6 IS-IS to filter redistributed routes.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>`filter-policy {ipv6-acl-number</td>
<td>prefix-list prefix-list-name</td>
</tr>
<tr>
<td>8.</td>
<td>Configure IPv6 IS-IS to filter received routes.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>`filter-policy {ipv6-acl-number</td>
<td>prefix-list prefix-list-name</td>
</tr>
<tr>
<td>9.</td>
<td>Configure IPv6 IS-IS to redistribute routes from another routing protocol.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>`import-route protocol [as-number</td>
<td>process-id] [allow-ibgp] [allow-direct</td>
</tr>
<tr>
<td>10.</td>
<td>Configure the maximum number of redistributed Level 1/Level 2 IPv6 routes.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>import-route limit number</code></td>
<td>The default setting varies by device model. For more information, see <em>Layer 3—IP Routing Command Reference</em>.</td>
</tr>
<tr>
<td>11.</td>
<td>Configure route advertisement from Level-2 to Level-1.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>`import-route isisv6 level-2 into level-1 [filter-policy {ipv6-acl-number</td>
<td>prefix-list prefix-list-name</td>
</tr>
<tr>
<td>12.</td>
<td>Configure route advertisement from Level-1 to Level-2.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>`import-route isisv6 level-1 into level-2 [filter-policy {ipv6-acl-number</td>
<td>prefix-list prefix-list-name</td>
</tr>
<tr>
<td>13.</td>
<td>Specify the maximum number of ECMP routes for load balancing.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>maximum load-balancing number</code></td>
<td>By default, the maximum number of ECMP routes is 32.</td>
</tr>
</tbody>
</table>
## Configuring IPv6 IS-IS link cost

### Configuring an IPv6 IS-IS cost for an interface

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter IS-IS view.</td>
<td>isis [ process-id ] [ vpn-instance vpn-instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Specify an IS-IS cost style.</td>
<td>cost-style { narrow</td>
</tr>
<tr>
<td>4.</td>
<td>Enter IPv6 address family view.</td>
<td>address-family ipv6 [ unicast ]</td>
</tr>
<tr>
<td>5.</td>
<td>Enable IPv6 IS-IS MTR.</td>
<td>multi-topology [ compatible ]</td>
</tr>
<tr>
<td>6.</td>
<td>Return to IS-IS view.</td>
<td>quit</td>
</tr>
<tr>
<td>7.</td>
<td>Return to system view.</td>
<td>quit</td>
</tr>
<tr>
<td>8.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>10.</td>
<td>Specify an IPv6 cost for the IS-IS interface.</td>
<td>isis ipv6 cost</td>
</tr>
</tbody>
</table>

### Configuring a global IPv6 IS-IS cost

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter IS-IS view.</td>
<td>isis [ process-id ] [ vpn-instance vpn-instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Specify an IS-IS cost style.</td>
<td>cost-style { wide</td>
</tr>
<tr>
<td>4.</td>
<td>Enter IPv6 address family view.</td>
<td>address-family ipv6 [ unicast ]</td>
</tr>
<tr>
<td>5.</td>
<td>Enable IPv6 IS-IS MTR.</td>
<td>multi-topology [ compatible ]</td>
</tr>
</tbody>
</table>

### Enabling automatic link cost calculation

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter IS-IS view.</td>
<td>isis [ process-id ] [ vpn-instance vpn-instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Specify an IS-IS cost style.</td>
<td>cost-style { wide</td>
</tr>
<tr>
<td>4.</td>
<td>Enter IPv6 address family view.</td>
<td>address-family ipv6 [ unicast ]</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>5.</td>
<td>multi-topology [ compatible ]</td>
<td>By default, IPv6 IS-IS MTR is disabled.</td>
</tr>
<tr>
<td>6.</td>
<td>auto-cost enable</td>
<td>By default, automatic IPv6 IS-IS cost calculation is disabled.</td>
</tr>
<tr>
<td>7.</td>
<td>bandwidth-reference [ value ]</td>
<td>The default setting is 100 Mbps.</td>
</tr>
</tbody>
</table>

### Tuning and optimizing IPv6 IS-IS networks

#### Configuration prerequisites

Before you tune and optimize IPv6 IS-IS networks, complete basic IPv6 IS-IS tasks.

#### Assigning a convergence priority to IPv6 IS-IS routes

A topology change causes IS-IS routing convergence. To improve convergence speed, you can assign convergence priorities to IPv6 IS-IS routes. Convergence priority levels are critical, high, medium, and low. The higher the convergence priority, the faster the convergence speed.

By default, IPv6 IS-IS host routes have medium convergence priority, and other IPv6 IS-IS routes have low convergence priority.

To assign a convergence priority to specific IPv6 IS-IS routes:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>isis [ process-id ] [ vpn-instance vpn-instance-name ]</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>cost-style { wide</td>
<td>wide-compatible</td>
</tr>
<tr>
<td>4.</td>
<td>address-family ipv6 [ unicast ]</td>
<td>N/A</td>
</tr>
<tr>
<td>5.</td>
<td>multi-topology [ compatible ]</td>
<td>By default, IPv6 IS-IS MTR is disabled.</td>
</tr>
<tr>
<td>6.</td>
<td>Assign a convergence priority to specific IPv6 IS-IS routes.</td>
<td>By default, IPv6 IS-IS routes, except IPv6 IS-IS host routes, have the low convergence priority.</td>
</tr>
</tbody>
</table>

- Method 1: prefix-priority { critical | high | medium } { prefix-list prefix-list-name | tag tag-value }
- Method 2: prefix-priority route-policy route-policy-name
Setting the LSDB overload bit

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter IS-IS view.</td>
<td>isis [ process-id ] [ vpn-instance vpn-instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Specify an IS-IS cost style.</td>
<td>cost-style { wide</td>
</tr>
<tr>
<td>4.</td>
<td>Enter IPv6 address family view.</td>
<td>address-family ipv6 [ unicast ]</td>
</tr>
<tr>
<td>5.</td>
<td>Enable IPv6 IS-IS MTR.</td>
<td>multi-topology [ compatible ]</td>
</tr>
</tbody>
</table>

Configuring a tag value on an interface

When IS-IS advertises an IPv6 prefix with a tag value, it adds the tag to the IPv6 reachability information TLV, regardless of the link cost style.

To configure a tag value on an interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Configure a tag value on the interface.</td>
<td>isis ipv6 tag tag</td>
</tr>
</tbody>
</table>

Controlling SPF calculation interval

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter IS-IS view.</td>
<td>isis [ process-id ] [ vpn-instance vpn-instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Specify an IS-IS cost style.</td>
<td>cost-style { wide</td>
</tr>
<tr>
<td>4.</td>
<td>Enter IPv6 address family view.</td>
<td>address-family ipv6 [ unicast ]</td>
</tr>
<tr>
<td>5.</td>
<td>Enable IPv6 IS-IS MTR.</td>
<td>multi-topology [ compatible ]</td>
</tr>
</tbody>
</table>
### Enabling IPv6 IS-IS ISPF

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>isis [ process-id ] [ vpn-instance vpn-instance-name ]</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>cost-style { wide</td>
<td>wide-compatible</td>
</tr>
<tr>
<td>4.</td>
<td>address-family ipv6 [ unicast ]</td>
<td>N/A</td>
</tr>
<tr>
<td>5.</td>
<td>multi-topology [ compatible ]</td>
<td>By default, IPv6 IS-IS MTR is disabled.</td>
</tr>
<tr>
<td>6.</td>
<td>ispf enable</td>
<td>By default, IPv6 IS-IS ISPF is enabled.</td>
</tr>
</tbody>
</table>

#### Enabling prefix suppression

Perform this task to disable an interface from advertising its prefix in LSPs. This enhances network security by preventing IP routing to the interval nodes and speeds up network convergence.

To enable prefix suppression:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>isis ipv6 prefix-suppression</td>
<td>By default, prefix suppression is disabled on an interface.</td>
</tr>
</tbody>
</table>

#### Configuring BFD for IPv6 IS-IS

Bidirectional forwarding detection (BFD) can quickly detect faults between IPv6 IS-IS neighbors to improve the convergence speed of IPv6 IS-IS. For more information about BFD, see *High Availability Configuration Guide*.

To configure BFD for IPv6 IS-IS:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
</tbody>
</table>
### Configuring IPv6 IS-IS FRR

**IMPORTANT:**
ECMP routes do not support FRR.

A link or router failure on a path can cause packet loss and routing loop. IPv6 IS-IS FRR enables fast rerouting to minimize the failover time.

**Figure 112 Network diagram for IPv6 IS-IS FRR**

In Figure 112, after you enable FRR on Router B, IPv6 IS-IS FRR automatically calculates or designates a backup next hop when a link failure is detected. In this way, packets are directed to the backup next hop to reduce traffic recovery time. Meanwhile, IPv6 IS-IS calculates the shortest path based on the new network topology, and forwards packets over the path after network convergence.

You can assign a backup next hop for IPv6 IS-IS FRR in the following ways:
- Enable IPv6 IS-IS FRR to calculate a backup next hop through Loop Free Alternate (LFA) calculation.
- Designate a backup next hop with a routing policy for routes matching specific criteria.

### Configuration prerequisites

Before you configure IPv6 IS-IS FRR, complete the following tasks:
- Configure IPv6 addresses for interfaces to ensure IP connectivity between neighboring nodes.
- Enable IPv6 IS-IS.
- Make sure the backup next hop is reachable.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td><code>isis [ process-id ] [ vpn-instance vpn-instance-name ]</code></td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td><code>network-entity net</code></td>
<td>By default, no NET is configured.</td>
</tr>
<tr>
<td>4.</td>
<td><code>address-family ipv6 [ unicast ]</code></td>
<td>N/A</td>
</tr>
<tr>
<td>5.</td>
<td><code>quit</code></td>
<td>N/A</td>
</tr>
<tr>
<td>6.</td>
<td><code>interface interface-type interface-number</code></td>
<td>N/A</td>
</tr>
<tr>
<td>7.</td>
<td><code>isis ipv6 enable [ process-id ]</code></td>
<td>By default, IPv6 is disabled for IS-IS on an interface.</td>
</tr>
<tr>
<td>8.</td>
<td><code>isis ipv6 bfd enable</code></td>
<td>By default, BFD for IPv6 IS-IS is disabled.</td>
</tr>
</tbody>
</table>
**Configuration procedure**

### Configuring IPv6 IS-IS FRR to calculate a backup next hop through LFA calculation

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>(Optional.) Disable LFA calculation on the interface.</td>
<td>isis ipv6 fast-reroute lfa-backup exclude</td>
</tr>
<tr>
<td>4.</td>
<td>Return to system view.</td>
<td>quit</td>
</tr>
<tr>
<td>5.</td>
<td>Enter IS-IS IPv6 unicast address family view.</td>
<td>a isis [ process-id ] [ vpn-instance vpn-instance-name ] b address-family ipv6 [ unicast ]</td>
</tr>
<tr>
<td>6.</td>
<td>Enable IPv6 IS-IS FRR to calculate a backup next hop through LFA calculation.</td>
<td>fast-reroute lfa</td>
</tr>
</tbody>
</table>

### Configuring IPv6 IS-IS FRR using a routing policy

You can use the `apply ipv6 fast-reroute backup-interface` command to specify a backup next hop in a routing policy for routes matching specific criteria. You can also perform this task to reference the routing policy for IPv6 IS-IS FRR. For more information about the `apply ipv6 fast-reroute backup-interface` command and routing policy configurations, see "Configuring routing policies."

To configure IPv6 IS-IS FRR using a routing policy:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>(Optional.) Disable LFA calculation on the interface.</td>
<td>isis ipv6 fast-reroute lfa-backup exclude</td>
</tr>
<tr>
<td>4.</td>
<td>Return to system view.</td>
<td>quit</td>
</tr>
<tr>
<td>5.</td>
<td>Enter IS-IS IPv6 unicast address family view.</td>
<td>isis [ process-id ] [ vpn-instance vpn-instance-name ] address-family ipv6 [ unicast ]</td>
</tr>
<tr>
<td>6.</td>
<td>Enable IPv6 IS-IS FRR using a routing policy.</td>
<td>fast-reroute route-policy route-policy-name</td>
</tr>
</tbody>
</table>
### Enabling BFD for IPv6 IS-IS FRR

By default, IPv6 IS-IS FRR does not use BFD to detect primary link failures. To speed up IPv6 IS-IS convergence, enable BFD for IPv6 IS-IS FRR to detect primary link failures.

To enable BFD control packet mode for IPv6 IS-IS FRR:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>isis ipv6 primary-path-detect bfd ctrl</td>
<td>By default, BFD control packet mode for IPv6 IS-IS FRR is disabled.</td>
</tr>
</tbody>
</table>

To enable BFD echo packet mode for IPv6 IS-IS FRR:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>bfd echo-source-ipv6 ip-address</td>
<td>By default, the source IPv6 address of BFD echo packets is not configured. The source IPv6 address cannot be on the same network segment as any local interface's IP address. For more information, see High Availability Command Reference.</td>
</tr>
<tr>
<td>3.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>4.</td>
<td>isis ipv6 primary-path-detect bfd echo</td>
<td>By default, BFD echo packet mode for IPv6 IS-IS FRR is disabled.</td>
</tr>
</tbody>
</table>

### Enabling IPv6 IS-IS MTR

On a network, IPv4 and IPv6 topologies must be consistent so that both IPv6 IS-IS and IPv4 IS-IS can use the SPF algorithm to perform route calculation. If they are different, routers supporting both IPv4 and IPv6 might send IPv6 packets to routers that do not support IPv6, resulting in packet loss.

To resolve this issue, configure IPv6 IS-IS Multi-Topology Routing (MTR) to perform route calculation separately in IPv4 and IPv6 topologies.
As shown in Figure 113, the numbers refer to the link costs. Router A, Router B, and Router D support both IPv4 and IPv6. Router C supports only IPv4 and cannot forward IPv6 packets.

Enable IPv6 IS-IS MTR on Router A, Router B, Router C, and Router D to make them perform route calculation separately in IPv4 and IPv6 topologies. With this configuration, Router A does not forward IPv6 packets destined to Router D through Router B, avoiding packet loss.

For more information about MTR and IS-IS MTR, see "Configuring MTR" and "Configuring IS-IS."

Configuration prerequisites
Before you configure IPv6 IS-IS MTR, configure basic IPv4 and IPv6 IS-IS functions, and establish IS-IS neighbors.

Configuration procedure
To enable IPv6 IS-IS MTR:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter IS-IS view.</td>
<td>isis [ process-id ] [ vpn-instance vpn-instance-name ]</td>
</tr>
<tr>
<td>3.</td>
<td>Specify an IS-IS cost style.</td>
<td>cost-style { wide</td>
</tr>
<tr>
<td>4.</td>
<td>Enter IPv6 address family view.</td>
<td>address-family ipv6 [ unicast ]</td>
</tr>
<tr>
<td>5.</td>
<td>Enable IPv6 IS-IS MTR.</td>
<td>multi-topology [ compatible ]</td>
</tr>
</tbody>
</table>

Displaying and maintaining IPv6 IS-IS

Execute display commands in any view. For other display and reset commands, see "Configuring IS-IS."

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display information about routes redistributed by IPv6 IS-IS.</td>
<td>display isis redistribute ipv6 [ ipv6-address mask-length ] [ level-1</td>
</tr>
<tr>
<td>Display IPv6 IS-IS routing information.</td>
<td>display isis route ipv6 [ ipv6-address ] [ [ level-1</td>
</tr>
</tbody>
</table>
### IPv6 IS-IS configuration examples

#### IPv6 IS-IS basic configuration example

**Network requirements**

As shown in Figure 114, Router A, Router B, Router C, and Router D, all enabled with IPv6, reside in the same AS. Configure IPv6 IS-IS on the routers so that they can reach each other.

Router A and Router B are Level-1 routers, Router D is a Level-2 router, and Router C is a Level-1-2 router.

**Figure 114 Network diagram**

![Network Diagram](image)

**Configuration procedure**

1. Configure IPv6 addresses for interfaces. (Details not shown.)
2. Configure IPv6 IS-IS:
   
   ```
   # Configure Router A.
   <RouterA> system-view
   [RouterA] isis 1
   [RouterA-isis-1] is-level level-1
   [RouterA-isis-1] network-entity 10.0000.0000.0001.00
   [RouterA-isis-1] address-family ipv6
   [RouterA-isis-1-ipv6] quit
   [RouterA-isis-1] quit
   [RouterA] interface gigabitethernet 1/0/1
   [RouterA-GigabitEthernet1/0/1] isis ipv6 enable 1
   [RouterA-GigabitEthernet1/0/1] quit
   
   # Configure Router B.
   <RouterB> system-view
   [RouterB] isis 1
   [RouterB-isis-1] is-level level-1
   [RouterB-isis-1] network-entity 10.0000.0000.0002.00
   ```
# Configure Router C.

<RouterC> system-view
[RouterC] isis 1
[RouterC-isis-1] network-entity 10.0000.0000.0003.00
[RouterC-isis-1] address-family ipv6
[RouterC-isis-1-ipv6] quit
[RouterC-isis-1] quit
[RouterC] interface gigabitethernet 1/0/1
[RouterC-GigabitEthernet1/0/1] isis ipv6 enable 1
[RouterC-GigabitEthernet1/0/1] quit
[RouterC] interface gigabitethernet 1/0/2
[RouterC-GigabitEthernet1/0/2] isis ipv6 enable 1
[RouterC-GigabitEthernet1/0/2] quit
[RouterC] interface gigabitethernet 1/0/3
[RouterC-GigabitEthernet1/0/3] isis ipv6 enable 1
[RouterC-GigabitEthernet1/0/3] quit

# Configure Router D.

<RouterD> system-view
[RouterD] isis 1
[RouterD-isis-1] is-level level-2
[RouterD-isis-1] network-entity 20.0000.0000.0004.00
[RouterD-isis-1] address-family ipv6
[RouterD-isis-1-ipv6] quit
[RouterD-isis-1] quit
[RouterD] interface gigabitethernet 1/0/1
[RouterD-GigabitEthernet1/0/1] isis ipv6 enable 1
[RouterD-GigabitEthernet1/0/1] quit
[RouterD] interface gigabitethernet 1/0/2
[RouterD-GigabitEthernet1/0/2] isis ipv6 enable 1
[RouterD-GigabitEthernet1/0/2] quit

Verifying the configuration

# Display the IPv6 IS-IS routing table on Router A.
[RouterA] display isis route ipv6

Route information for IS-IS(1)
---------------------------------

Level-1 IPv6 Forwarding Table
---------------------------------

   Destination : ::  PrefixLen: 0
   Flag         : R/-/-  Cost     : 10
<table>
<thead>
<tr>
<th>Destination</th>
<th>PrefixLen</th>
<th>Flag</th>
<th>Cost</th>
<th>Next Hop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>::</td>
<td>0</td>
<td>R/-/-</td>
<td>10</td>
<td>FE80::200:FF:FE0F:4</td>
<td>GE1/0/1</td>
</tr>
<tr>
<td>2001:1::</td>
<td>64</td>
<td>D/L/-</td>
<td>10</td>
<td>FE80::200:FF:FE0F:4</td>
<td>GE1/0/1</td>
</tr>
<tr>
<td>2001:2::</td>
<td>64</td>
<td>R/-/-</td>
<td>20</td>
<td>Direct</td>
<td>GE1/0/1</td>
</tr>
<tr>
<td>2001:3::</td>
<td>64</td>
<td>R/-/-</td>
<td>20</td>
<td>FE80::200:FF:FE0F:4</td>
<td>GE1/0/1</td>
</tr>
</tbody>
</table>

Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set

# Display the IPv6 IS-IS routing table on Router B.

```bash
[RouterB] display isis route ipv6
```

```plaintext
Route information for IS-IS(1)
-------------------------------

Level-1 IPv6 Forwarding Table
-------------------------------
```
Level-1 IPv6 Forwarding Table
---------------------------------

Destination : 2001:1::  PrefixLen: 64
Flag        : D/L/-   Cost     : 10
Next Hop    : Direct   Interface: GE1/0/2

Destination : 2001:2::  PrefixLen: 64
Flag        : D/L/-   Cost     : 10
Next Hop    : Direct   Interface: GE1/0/1

Destination : 2001:3::  PrefixLen: 64
Flag        : D/L/-   Cost     : 10
Next Hop    : Direct   Interface: GE1/0/3

Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set

Level-2 IPv6 Forwarding Table
---------------------------------

Destination : 2001:1::  PrefixLen: 64
Flag        : D/L/-   Cost     : 10
Next Hop    : Direct   Interface: GE1/0/2

Destination : 2001:2::  PrefixLen: 64
Flag        : D/L/-   Cost     : 10
Next Hop    : Direct   Interface: GE1/0/1

Destination : 2001:3::  PrefixLen: 64
Flag        : D/L/-   Cost     : 10
Next Hop    : Direct   Interface: GE1/0/3

Destination : 2001:4::1  PrefixLen: 64
Flag        : R/-/-   Cost     : 10
Next Hop    : FE80::20F:E2FF:FE3E:FA3D   Interface: GE1/0/3

Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set

# Display the IPv6 IS-IS routing table on Router D.
[RouterD] display isis route ipv6

Route information for IS-IS(1)
---------------------------------

Level-2 IPv6 Forwarding Table
---------------------------------

Destination : 2001:1::  PrefixLen: 64
Flag        : R/-/-   Cost     : 20
Next Hop    : FE80::200:FF:FE0F:4   Interface: GE1/0/1

487
BFD for IPv6 IS-IS configuration example

Network requirements

As shown in Figure 115:

- Configure IPv6 IS-IS on Router A, Router B, and Router C so that they can reach each other.
- Enable BFD on GigabitEthernet 1/0/1 of Router A and Router B.

When the link between Router B and the Layer-2 switch fails, BFD can quickly detect the failure and notify IPv6 IS-IS of the failure. Then Router A and Router B communicate through Router C.

Figure 115 Network diagram

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IPv6 address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router A</td>
<td>GE1/0/1</td>
<td>2001::1/64</td>
</tr>
<tr>
<td>Router A</td>
<td>GE1/0/2</td>
<td>2001:2::1/64</td>
</tr>
<tr>
<td>Router B</td>
<td>GE1/0/1</td>
<td>2001:2::1/64</td>
</tr>
<tr>
<td>Router B</td>
<td>GE1/0/2</td>
<td>2001:3::2/64</td>
</tr>
<tr>
<td>Router C</td>
<td>GE1/0/1</td>
<td>2001:2::2/64</td>
</tr>
<tr>
<td>Router C</td>
<td>GE1/0/2</td>
<td>2001:3::1/64</td>
</tr>
</tbody>
</table>
1. Configure IPv6 addresses for interfaces. (Details not shown.)
2. Configure IPv6 IS-IS:
   # Configure Router A.
   <RouterA> system-view
   [RouterA] isis 1
   [RouterA-isis-1] is-level level-1
   [RouterA-isis-1] network-entity 10.0000.0000.0001.00
   [RouterA-isis-1] address-family ipv6
   [RouterA-isis-1-ipv6] quit
   [RouterA-isis-1] quit
   [RouterA] interface gigabitethernet 1/0/1
   [RouterA-GigabitEthernet1/0/1] isis ipv6 enable 1
   [RouterA-GigabitEthernet1/0/1] quit
   [RouterA] interface gigabitethernet 1/0/2
   [RouterA-GigabitEthernet1/0/2] isis ipv6 enable 1
   [RouterA-GigabitEthernet1/0/2] quit

   # Configure Router B.
   <RouterB> system-view
   [RouterB] isis 1
   [RouterB-isis-1] is-level level-1
   [RouterB-isis-1] network-entity 10.0000.0000.0002.00
   [RouterB-isis-1] address-family ipv6
   [RouterB-isis-1-ipv6] quit
   [RouterB-isis-1] quit
   [RouterB] interface gigabitethernet 1/0/1
   [RouterB-GigabitEthernet1/0/1] isis ipv6 enable 1
   [RouterB-GigabitEthernet1/0/1] quit
   [RouterB] interface gigabitethernet 1/0/2
   [RouterB-GigabitEthernet1/0/2] isis ipv6 enable 1
   [RouterB-GigabitEthernet1/0/2] quit

   # Configure Router C.
   <RouterC> system-view
   [RouterC] isis 1
   [RouterC-isis-1] network-entity 10.0000.0000.0003.00
   [RouterC-isis-1] address-family ipv6
   [RouterC-isis-1-ipv6] quit
   [RouterC-isis-1] quit
   [RouterC] interface gigabitethernet 1/0/1
   [RouterC-GigabitEthernet1/0/1] isis ipv6 enable 1
   [RouterC-GigabitEthernet1/0/1] quit
   [RouterC] interface gigabitethernet 1/0/2
   [RouterC-GigabitEthernet1/0/2] isis ipv6 enable 1
   [RouterC-GigabitEthernet1/0/2] quit

3. Configure BFD functions:
   # Enable BFD and configure BFD parameters on Router A.
   [RouterA] bfd session init-mode active
   [RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] isis ipv6 bfd enable
[RouterA-GigabitEthernet1/0/1] bfd min-transmit-interval 500
[RouterA-GigabitEthernet1/0/1] bfd min-receive-interval 500
[RouterA-GigabitEthernet1/0/1] bfd detect-multiplier 7
[RouterA-GigabitEthernet1/0/1] return

# Enable BFD and configure BFD parameters on Router B.
[RouterB] bfd session init-mode active
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] isis ipv6 bfd enable
[RouterB-GigabitEthernet1/0/1] bfd min-transmit-interval 500
[RouterB-GigabitEthernet1/0/1] bfd min-receive-interval 500
[RouterB-GigabitEthernet1/0/1] bfd detect-multiplier 6

Verifying the configuration

# Display BFD session information on Router A.
<RouterA> display bfd session

Total Session Num: 1   Up Session Num: 1   Init Mode: Active

IPv6 Session Working Under Ctrl Mode:

<table>
<thead>
<tr>
<th>Local Discr: 1441</th>
<th>Remote Discr: 1450</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP: FE80::20F:FF:FE00:1202 (link-local address of GigabitEthernet1/0/1 on Router A)</td>
<td></td>
</tr>
<tr>
<td>Destination IP: FE80::20F:FF:FE00:1200 (link-local address of GigabitEthernet1/0/1 on Router B)</td>
<td></td>
</tr>
<tr>
<td>Session State: Up</td>
<td>Interface: GE1/0/1</td>
</tr>
<tr>
<td>Hold Time: 2319ms</td>
<td></td>
</tr>
</tbody>
</table>

# Display routes destined for 2001:4::0/64 on Router A.
<RouterA> display ipv6 routing-table 2001:4::0 64

Summary Count : 2

Destination: 2001:4::/64     Protocol  : IS_L1
NextHop    : FE80::20F:FF:FE00:1200     Preference: 15
Interface  : GE1/0/1     Cost      : 10

The output shows that Router A and Router B communicate through GigabitEthernet 1/0/1. Then the link over GigabitEthernet 1/0/1 fails.

# Display routes destined for 2001:4::0/64 on Router A.
<RouterA> display ipv6 routing-table 2001:4::0 64

Summary Count : 1

Destination: 2001:4::/64     Protocol  : IS_L1
NextHop    : FE80::BAAF:67FF:FE27:DCD0     Preference: 15
Interface  : GE1/0/2     Cost      : 20

The output shows that Router A and Router B communicate through GigabitEthernet 1/0/2.
IPv6 IS-IS FRR configuration example

Network requirements

As shown in Figure 116, Router A, Router B, and Router C reside in the same IS-IS routing domain.

- Run IPv6 IS-IS on all the routers to interconnect them with each other.
- Configure IPv6 IS-IS FRR so that when Link A fails, traffic can be switched to Link B immediately.

Figure 116 Network diagram

![Network Diagram]

Table 26 Interface and IP address assignment

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router A</td>
<td>GE1/0/1</td>
<td>1::1/64</td>
<td>Router B</td>
<td>GE1/0/1</td>
<td>3::1/64</td>
</tr>
<tr>
<td></td>
<td>GE1/0/2</td>
<td>2::1/64</td>
<td></td>
<td>GE1/0/2</td>
<td>2::2/64</td>
</tr>
<tr>
<td></td>
<td>Loop0</td>
<td>10::1/128</td>
<td></td>
<td>Loop0</td>
<td>20::1/128</td>
</tr>
<tr>
<td>Router C</td>
<td>GE1/0/1</td>
<td>1::2/64</td>
<td></td>
<td>GE1/0/2</td>
<td>3::2/64</td>
</tr>
</tbody>
</table>

Configuration procedure

1. Configure IPv6 addresses for interfaces on the routers and enable IPv6 IS-IS. (Details not shown.)
2. Configure IPv6 IS-IS FRR:
   Enable IPv6 IS-IS FRR to calculate a backup next hop through LFA calculation, or designate a backup next hop by using a routing policy.
   - (Method 1.) Enable IPv6 IS-IS FRR to calculate a backup next hop through LFA calculation:
     # Configure Router A.
     <RouterA> system-view
     [RouterA] isis 1
     [RouterA-isis-1] address-family ipv6
     [RouterA-isis-1-ipv6] fast-reroute lfa
     # Configure Router B.
     <RouterB> system-view
     [RouterB] isis 1
     [RouterB-isis-1] address-family ipv6
     [RouterB-isis-1-ipv6] fast-reroute lfa
   - (Method 2.) Enable IPv6 IS-IS FRR to designate a backup next hop by using a routing policy:
     # Configure Router A.
Verifying the configuration

# Display the route 20::1/128 on Router A to view the backup next hop information.

[RouterA] display ipv6 routing-table 20::1 128 verbose

Summary count : 1

Destination: 20::1/128  
Protocol: IS_L1 
Process ID: 1

SubProtID: 0x1   Age: 00h27m45s
Cost: 10  
IpPre: N/A  
Tag: 0  
OrigTblID: 0xa  
TableID: 0xa  
NibID: 0x24000005  
AttrID: 0xffffffff  
Flags: 0x10041  
Label: NULL  
BkLabel: NULL  
Tunnel ID: Invalid  
BkTunnel ID: Invalid  
FtnIndex: 0x0  
RealNextHop: FE80::34CD:9FF:FE2F:D02  
BkNextHop: FE80::7685:45FF:FEAD:102  
Interface: GigabitEthernet1/0/2  
BkInterface: GigabitEthernet1/0/1  
TrafficIndex: N/A
# Display the route 10::1/128 on Router B to view the backup next hop information.

```
[RouterB] display ipv6 routing-table 10::1 128 verbose
```

Summary count : 1

<table>
<thead>
<tr>
<th>Destination: 10::1/128</th>
<th>Protocol: IS_L1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process ID: 1</td>
<td>SubProtID: 0x1</td>
</tr>
<tr>
<td></td>
<td>Age: 00h33m23s</td>
</tr>
<tr>
<td>Cost: 10</td>
<td>Preference: 15</td>
</tr>
<tr>
<td>IpPre: N/A</td>
<td>QosLocalID: N/A</td>
</tr>
<tr>
<td>Tag: 0</td>
<td>State: Active Adv</td>
</tr>
<tr>
<td>OrigTblID: 0xa</td>
<td>OrigVrf: default-vrf</td>
</tr>
<tr>
<td>TableID: 0xa</td>
<td>OrigAs: 0</td>
</tr>
<tr>
<td>NibID: 0x24000006</td>
<td>LastAs: 0</td>
</tr>
<tr>
<td>AttrID: 0xffffffff</td>
<td>Neighbor: ::</td>
</tr>
<tr>
<td>Flags: 0x10041</td>
<td>OrigNextHop: FE80::34CC:E8FF:FE5B:C02</td>
</tr>
<tr>
<td>Label: NULL</td>
<td>RealNextHop: FE80::34CC:E8FF:FE5B:C02</td>
</tr>
<tr>
<td>BkLabel: NULL</td>
<td>BkNextHop: FE80::7685:45FF:FEAD:102</td>
</tr>
<tr>
<td>Tunnel ID: Invalid</td>
<td>Interface: GigabitEthernet1/0/2</td>
</tr>
<tr>
<td>BkTunnel ID: Invalid</td>
<td>BkInterface: GigabitEthernet1/0/1</td>
</tr>
<tr>
<td>FtnIndex: 0x0</td>
<td>TrafficIndex: N/A</td>
</tr>
<tr>
<td>Connector: N/A</td>
<td></td>
</tr>
</tbody>
</table>
Configuring IPv6 PBR

Overview

Policy-based routing (PBR) uses user-defined policies to route packets. A policy can specify parameters for packets that match specific criteria such as ACLs or that have specific lengths. The parameters include the next hop, output interface, default next hop, and default output interface.

A device forwards received packets using the following process:

1. The device uses PBR to forward matching packets.
2. If the packets do not match the PBR policy or the PBR-based forwarding fails, the device uses the routing table, excluding the default route, to forward the packets.
3. If the routing table-based forwarding fails, the device uses the default next hop or default output interface defined in PBR to forward packets.
4. If the default next hop or default output interface-based forwarding fails, the device uses the default route to forward packets.

PBR includes local PBR and interface PBR.
- Local PBR guides the forwarding of locally generated packets, such as the ICMP packets generated by using the ping command.
- Interface PBR guides the forwarding of packets received on an interface only.

Policy

An IPv6 policy includes match criteria and actions to be taken on the matching packets. A policy can have one or multiple nodes as follows:
- Each node is identified by a node number. A smaller node number has a higher priority.
- A node contains if-match and apply clauses. An if-match clause specifies a match criterion, and an apply clause specifies an action.
- A node has a match mode of permit or deny.

An IPv6 policy compares packets with nodes in priority order. If a packet matches the criteria on a node, it is processed by the action on the node. Otherwise, it goes to the next node for a match. If the packet does not match the criteria on any node, it is forwarded according to the routing table.

if-match clause

IPv6 PBR supports the following types of if-match clauses:
- if-match acl—Sets an ACL match criterion.
- if-match packet-length—Sets a packet length match criterion.

You can specify multiple if-match clauses for a node, but only one if-match clause of each type. A packet that matches all the if-match clauses of a node matches the node.

apply clause

IPv6 PBR supports the types of apply clauses shown in Table 27. You can specify multiple apply clauses for a node, but some of them might not be executed. The following apply clauses determine the packet forwarding paths in a descending order:
- apply access-vpn vpn-instance
- apply next-hop
- apply output-interface
• apply default-next-hop
• apply default-output-interface

Table 27 Priorities and meanings of apply clauses

<table>
<thead>
<tr>
<th>Clause</th>
<th>Meaning</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>apply precedence</td>
<td>Sets an IP precedence.</td>
<td>This clause is always executed.</td>
</tr>
</tbody>
</table>
| apply loadshare { next-hop | output-interface | default-next-hop | default-output-interface } | Enables load sharing among multiple next hops, output interfaces, default next hops, and default output interfaces. | Multiple next hops, output interfaces, default next hops, or default output interfaces operate in either primary/backup or load sharing mode. For example:
  - **Primary/backup mode**—The first configured output interface is used. When the primary output interface fails, the first configured backup output interface takes over.
  - **Load sharing mode**—Multiple output interfaces load share traffic on a per-packet basis in turn, according to the configuration order. Multiple next hops load share traffic according to their weights.
  By default, the primary/backup mode applies. |
| apply access-vpn vpn-instance | Sets VPN instances. | If a packet matches a forwarding entry of a specified VPN instance, it is forwarded in the VPN instance. |
| apply next-hop and apply output-interface | Sets next hops and sets output interfaces. | Only the **apply next-hop** clause is executed when both are configured. |
| apply default-next-hop and apply default-output-interface | Sets default next hops and sets default output interfaces. | Only the **apply default-next-hop** clause is executed when both are configured. They take effect only when no next hop or output interface is set or the next hop and output interface are invalid, and the IPv6 packet does not match any route in the routing table. |
| apply continue | Compares packets with the next node upon failure on the current node. | The **apply continue** clause applies when the **apply access-vpn vpn-instance**, **apply next-hop**, **apply output-interface**, **apply default-next-hop**, and **apply default-output-interface** clauses are not configured or become invalid. For example, the specified next hop is unreachable, the specified output interface is down, or the packets cannot be forwarded in the specified VPN instance. |

Relationship between the match mode and clauses on the node

<table>
<thead>
<tr>
<th>Does a packet match all the if-match clauses on the node?</th>
<th>Match mode</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Yes</strong></td>
<td><strong>In permit mode</strong></td>
</tr>
<tr>
<td></td>
<td>• If the node is configured with <strong>apply</strong> clauses, IPv6 PBR executes the <strong>apply</strong> clauses on the node.</td>
</tr>
<tr>
<td></td>
<td>o If the IPv6 PBR-based forwarding succeeds, IPv6 PBR does not compare the</td>
</tr>
</tbody>
</table>
Does a packet match all the if-match clauses on the node?

<table>
<thead>
<tr>
<th>Match mode</th>
<th>In permit mode</th>
<th>In deny mode</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>packet with the next node.</td>
<td></td>
</tr>
<tr>
<td>o</td>
<td>If the IPv6 PBR-based forwarding fails and the <strong>apply continue</strong> clause is not configured, IPv6 PBR does not compare the packet with the next node.</td>
<td></td>
</tr>
<tr>
<td>o</td>
<td>If the IPv6 PBR-based forwarding fails and the <strong>apply continue</strong> clause is configured, IPv6 PBR compares the packet with the next node.</td>
<td></td>
</tr>
<tr>
<td>•</td>
<td>If the node is configured with no <strong>apply</strong> clauses, the packet is forwarded according to the routing table.</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>IPv6 PBR compares the packet with the next node.</td>
<td>IPv6 PBR compares the packet with the next node.</td>
</tr>
</tbody>
</table>

A node that has no **if-match** clauses matches any packet.

**PBR and Track**

PBR can work with the Track feature to dynamically adapt the availability status of an **apply** clause to the link status of a tracked object. The tracked object can be a next hop, output interface, default next hop, or default output interface.

- When the track entry associated with an object changes to **Negative**, the **apply** clause is invalid.
- When the track entry changes to **Positive** or **NotReady**, the **apply** clause is valid.

For more information about Track-PBR collaboration, see *High Availability Configuration Guide*.

**Command and hardware compatibility**

Commands and descriptions for centralized devices apply to the following routers:

- MSR1002-4/1003-8S.
- MSR2003.
- MSR3012/3024/3044/3064.
- MSR958(JH300A/JH301A).

Commands and descriptions for distributed devices apply to MSR4060 and MSR4080 routers.
IPv6 PBR configuration task list

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Required.) Configuring an IPv6 policy:</td>
</tr>
<tr>
<td>• Creating an IPv6 node</td>
</tr>
<tr>
<td>• Setting match criteria for an IPv6 node</td>
</tr>
<tr>
<td>• Configuring actions for an IPv6 node</td>
</tr>
<tr>
<td>(Required.) Configuring IPv6 PBR:</td>
</tr>
<tr>
<td>• Configuring IPv6 local PBR</td>
</tr>
<tr>
<td>• Configuring IPv6 interface PBR</td>
</tr>
</tbody>
</table>

Configuring an IPv6 policy

Creating an IPv6 node

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create an IPv6 policy or policy node and enter its view.</td>
<td>ipv6 policy-based-route policy-name [ deny</td>
</tr>
</tbody>
</table>

Setting match criteria for an IPv6 node

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter IPv6 policy node view.</td>
<td>ipv6 policy-based-route policy-name [ deny</td>
</tr>
<tr>
<td>3.</td>
<td>Set an ACL match criterion.</td>
<td>if-match acl { ipv6-acl-number</td>
</tr>
<tr>
<td>4.</td>
<td>Set a packet length match criterion.</td>
<td>if-match packet-length min-len max-len</td>
</tr>
</tbody>
</table>

NOTE:
An ACL match criterion uses the specified ACL to match packets if the action in the ACL rule is permit. If the specified ACL does not exist or the action in the ACL rule is deny, no packet is matched.

Configuring actions for an IPv6 node

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>2.</td>
<td>Enter IPv6 policy node view.</td>
<td>\texttt{ipv6 policy-based-route policy-name [ deny</td>
</tr>
<tr>
<td>3.</td>
<td>Set an IP precedence.</td>
<td>\texttt{apply precedence { type</td>
</tr>
<tr>
<td>4.</td>
<td>Set VPN instances.</td>
<td>\texttt{apply access-vpn vpn-instance vpn-instance-name&amp;&lt;1-n&gt;}</td>
</tr>
<tr>
<td>5.</td>
<td>Set next hops for permitted IPv6 packets.</td>
<td>\texttt{apply next-hop [ vpn-instance vpn-instance-name</td>
</tr>
<tr>
<td>6.</td>
<td>Enable load sharing among multiple next hops.</td>
<td>\texttt{apply loadshare next-hop}</td>
</tr>
<tr>
<td>7.</td>
<td>Set output interfaces.</td>
<td>\texttt{apply output-interface { interface-type interface-number { track track-entry-number } }}&amp;&lt;1-n&gt;</td>
</tr>
<tr>
<td>8.</td>
<td>Enable load sharing among multiple output interfaces.</td>
<td>\texttt{apply loadshare output-interface}</td>
</tr>
<tr>
<td>9.</td>
<td>Set default next hops.</td>
<td>\texttt{apply default-next-hop [ vpn-instance vpn-instance-name</td>
</tr>
<tr>
<td>10.</td>
<td>Enable load sharing among multiple default next hops.</td>
<td>\texttt{apply loadshare default-next-hop}</td>
</tr>
<tr>
<td>11.</td>
<td>Set default output interfaces.</td>
<td>\texttt{apply default-output-interface { interface-type interface-number { track track-entry-number } }}&amp;&lt;1-n&gt;</td>
</tr>
</tbody>
</table>
### Configuring IPv6 PBR

#### Configuring IPv6 local PBR

Configure IPv6 PBR by applying a policy locally. IPv6 PBR uses the policy to guide the forwarding of locally generated packets. The specified policy must already exist. Otherwise, the IPv6 local PBR configuration fails.

You can apply only one policy locally. Before you apply a new policy, you must first remove the current policy.

IPv6 local PBR might affect local services, such as ping and Telnet. Do not configure IPv6 local PBR unless doing so is required.

To configure IPv6 local PBR:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>ipv6 local policy-based-route policy-name</td>
<td>By default, no policy is locally applied.</td>
</tr>
</tbody>
</table>

#### Configuring IPv6 interface PBR

Configure IPv6 PBR by applying an IPv6 policy to an interface. IPv6 PBR uses the policy to guide the forwarding of IPv6 packets received on the interface. The specified policy must already exist. Otherwise, the IPv6 interface PBR configuration fails.

You can apply only one policy to an interface. Before you apply a new policy, you must first remove the current policy from the interface.

You can apply a policy to multiple interfaces.

To configure IPv6 interface PBR:
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter interface view.</td>
<td><code>interface interface-type interface-number</code></td>
<td>N/A</td>
</tr>
<tr>
<td>3. Apply an IPv6 policy to the interface.</td>
<td><code>ipv6 policy-based-route policy-name</code></td>
<td>By default, no IPv6 policy is applied to the interface.</td>
</tr>
</tbody>
</table>

## Displaying and maintaining IPv6 PBR

Execute `display` commands in any view and `reset` commands in user view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display IPv6 PBR policy information.</td>
<td><code>display ipv6 policy-based-route [ policy policy-name ]</code></td>
</tr>
<tr>
<td>Display IPv6 PBR configuration.</td>
<td><code>display ipv6 policy-based-route setup</code></td>
</tr>
<tr>
<td>Display IPv6 local PBR configuration and statistics (centralized devices in standalone mode).</td>
<td><code>display ipv6 policy-based-route local</code></td>
</tr>
<tr>
<td>Display IPv6 local PBR configuration and statistics (distributed devices in standalone mode/centralized devices in IRF mode).</td>
<td><code>display ipv6 policy-based-route local [ slot slot-number ]</code></td>
</tr>
<tr>
<td>Display IPv6 local PBR configuration and statistics (distributed devices in IRF mode).</td>
<td><code>display ipv6 policy-based-route local [ chassis chassis-number slot slot-number ]</code></td>
</tr>
<tr>
<td>Display IPv6 interface PBR configuration and statistics (centralized devices in standalone mode).</td>
<td><code>display ipv6 policy-based-route interface interface-type interface-number</code></td>
</tr>
<tr>
<td>Display IPv6 interface PBR configuration and statistics (distributed devices in standalone mode/centralized devices in IRF mode).</td>
<td><code>display ipv6 policy-based-route interface interface-type interface-number [ slot slot-number ]</code></td>
</tr>
<tr>
<td>Display IPv6 interface PBR configuration and statistics (distributed devices in IRF mode).</td>
<td><code>display ipv6 policy-based-route interface interface-type interface-number [ chassis chassis-number slot slot-number ]</code></td>
</tr>
<tr>
<td>Clear IPv6 PBR statistics.</td>
<td><code>reset ipv6 policy-based-route statistics [ policy policy-name ]</code></td>
</tr>
</tbody>
</table>

## IPv6 PBR configuration examples

### Packet type-based IPv6 local PBR configuration example

#### Network requirements

As shown in Figure 117, configure IPv6 PBR on Router A to forward all TCP packets to the next hop 1::2. Router A forwards other packets according to the routing table.
Figure 117 Network diagram

### Configuration procedure

1. **Configure Router A:**
   
   ```
   # Configure the IPv6 addresses of GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.
   <RouterA> system-view
   [RouterA] interface gigabitethernet 1/0/1
   [RouterA-GigabitEthernet1/0/1] ipv6 address 1::1 64
   [RouterA-GigabitEthernet1/0/1] quit
   [RouterA] interface gigabitethernet 1/0/2
   [RouterA-GigabitEthernet1/0/2] ipv6 address 2::1 64
   [RouterA-GigabitEthernet1/0/2] quit
   
   # Configure ACL 3001 to match TCP packets.
   [RouterA] acl ipv6 advanced 3001
   [RouterA-acl-ipv6-adv-3001] rule permit tcp
   [RouterA-acl-ipv6-adv-3001] quit
   
   # Configure Node 5 for policy aaa to forward TCP packets to next hop 1::2.
   [RouterA] ipv6 policy-based-route aaa permit node 5
   [RouterA-pbr6-aaa-5] if-match acl 3001
   [RouterA-pbr6-aaa-5] apply next-hop 1::2
   [RouterA-pbr6-aaa-5] quit
   
   # Configure IPv6 local PBR by applying policy aaa to Router A.
   [RouterA] ipv6 local policy-based-route aaa
   ```

2. **On Router B, configure the IPv6 address of GigabitEthernet 1/0/1.**

   ```
   <RouterB> system-view
   [RouterB] interface gigabitethernet 1/0/1
   [RouterB-GigabitEthernet1/0/1] ipv6 address 1::2 64
   ```

3. **On Router C, configure the IPv6 address of GigabitEthernet 1/0/2.**

   ```
   <RouterC> system-view
   [RouterC-GigabitEthernet1/0/2] ipv6 address 2::2 64
   ```

### Verifying the configuration

1. **Telnet to Router B on Router A. The operation succeeds.**
2. **Telnet to Router C on Router A. The operation fails.**
3. **Ping Router C from Router A. The operation succeeds.**

Telnet uses TCP, and ping uses ICMP. The results show the following:

- All TCP packets sent from Router A are forwarded to the next hop 1::2.
- Other packets are forwarded through GigabitEthernet 1/0/2.
- The IPv6 local PBR configuration is effective.
Packet type-based IPv6 interface PBR configuration example

Network requirements

As shown in Figure 118, configure IPv6 PBR on Router A to forward all TCP packets received on GigabitEthernet 1/0/1 to the next hop 1::2. Router A forwards other IPv6 packets according to the routing table.

Figure 118 Network diagram

Configuration procedure

1. Configure Router A:
   # Configure RIPng.
   `<RouterA> system-view
   [RouterA] ripng 1
   [RouterA-ripng-1] quit
   [RouterA] interface gigabitethernet 1/0/2
   [RouterA-GigabitEthernet1/0/2] ipv6 address 1::1 64
   [RouterA-GigabitEthernet1/0/2] ripng 1 enable
   [RouterA-GigabitEthernet1/0/2] quit
   [RouterA] interface gigabitethernet 1/0/3
   [RouterA-GigabitEthernet1/0/3] ipv6 address 2::1 64
   [RouterA-GigabitEthernet1/0/3] ripng 1 enable
   [RouterA-GigabitEthernet1/0/3] quit
   # Configure ACL 3001 to match TCP packets.
   [RouterA] acl ipv6 advanced 3001
   [RouterA-acl-ipv6-adv-3001] rule permit tcp
   [RouterA-acl-ipv6-adv-3001] quit
   # Configure Node 5 for policy aaa to forward TCP packets to next hop 1::2.
   [RouterA] ipv6 policy-based-route aaa permit node 5
2. Configure IPv6 interface PBR by applying policy aaa to GigabitEthernet 1/0/1.

   [RouterA] interface gigabitethernet 1/0/1
   [RouterA-GigabitEthernet1/0/1] ipv6 address 10::2 64
   [RouterA-GigabitEthernet1/0/1] undo ipv6 nd ra halt
   [RouterA-GigabitEthernet1/0/1] ripng 1 enable
   [RouterA-GigabitEthernet1/0/1] ipv6 policy-based-route aaa
   [RouterA-GigabitEthernet1/0/1] quit

3. Configure RIPng on Router C.

   <RouterC> system-view
   [RouterC] ripng 1
   [RouterC-ripng-1] quit
   [RouterC] interface gigabitethernet 1/0/3
   [RouterC-GigabitEthernet1/0/3] ipv6 address 2::2 64
   [RouterC-GigabitEthernet1/0/3] ripng 1 enable
   [RouterC-GigabitEthernet1/0/3] quit

Verifying the configuration

# On Host A, Telnet to Router B that is directly connected to Router A. The operation succeeds.
# On Host A, Telnet to Router C that is directly connected to Router A. The operation fails.
# Ping Router C from Host A. The operation succeeds.

Telnet uses TCP, and ping uses ICMP. The results show the following:

- All TCP packets arriving on GigabitEthernet 1/0/1 of Router A are forwarded to the next hop 1::2.
- Other packets are forwarded through GigabitEthernet 1/0/3.
- The IPv6 interface PBR configuration is effective.

Packet length-based IPv6 interface PBR configuration example

Network requirements

As shown in Figure 119, configure IPv6 interface PBR to guide the forwarding of packets received on GigabitEthernet 1/0/1 of Router A as follows:

- Set the next hop of packets with a length of 64 to 100 bytes to 150::2/64.
- Set the next hop of packets with a length of 101 to 1000 bytes to 151::2/64.

Router A forwards other packets according to the routing table.
Figure 119 Network diagram

Configuration procedure

1. Configure Router A:
   # Configure RIPng.
   <RouterA> system-view
   [RouterA] ripng 1
   [RouterA-ripng-1] quit
   [RouterA] interface gigabitethernet 1/0/2
   [RouterA-GigabitEthernet1/0/2] ipv6 address 150::1 64
   [RouterA-GigabitEthernet1/0/2] ripng 1 enable
   [RouterA-GigabitEthernet1/0/2] quit
   [RouterA] interface gigabitethernet 1/0/3
   [RouterA-GigabitEthernet1/0/3] ipv6 address 151::1 64
   [RouterA-GigabitEthernet1/0/3] ripng 1 enable
   [RouterA-GigabitEthernet1/0/3] quit
   # Configure Node 10 for policy lab1
to forward packets with a length of 64 to 100 bytes to the
next hop 150::2/64.
   [RouterA] ipv6 policy-based-route lab1 permit node 10
   [RouterA-pbr6-lab1-10] if-match packet-length 64 100
   [RouterA-pbr6-lab1-10] apply next-hop 150::2
   [RouterA-pbr6-lab1-10] quit
   # Configure Node 20 for policy lab1
to forward packets with a length of 101 to 1000 bytes to the
next hop 151::2/64.
   [RouterA] ipv6 policy-based-route lab1 permit node 20
   [RouterA-pbr6-lab1-20] if-match packet-length 101 1000
   [RouterA-pbr6-lab1-20] apply next-hop 151::2
   [RouterA-pbr6-lab1-20] quit
   # Configure IPv6 interface PBR by applying policy lab1
to GigabitEthernet 1/0/1.
   [RouterA] interface gigabitethernet 1/0/1
   [RouterA-GigabitEthernet1/0/1] ipv6 address 192::1 64
   [RouterA-GigabitEthernet1/0/1] undo ipv6 nd ra halt
   [RouterA-GigabitEthernet1/0/1] ripng 1 enable
   [RouterA-GigabitEthernet1/0/1] ipv6 policy-based-route lab1
   [RouterA-GigabitEthernet1/0/1] return

2. Configure RIPng on Router B.
   <RouterB> system-view
   [RouterB] ripng 1
   [RouterB-ripng-1] quit
Verifying the configuration

# Execute the `debugging ipv6 policy-based-route` command on Router A.

```
<RouterA> debugging ipv6 policy-based-route
<RouterA> terminal logging level 7
<RouterA> terminal monitor
```

# Ping Loopback 0 of Router B from Host A, and set the data length to 64 bytes.

```
C:\>ping -n 1 -l 64 10::1
```

Pinging 10::1 with 64 bytes of data:

Reply from 10::1: time=1ms

Ping statistics for 10::1:
   Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 1ms, Maximum = 1ms, Average = 1ms

The debugging information about IPv6 PBR displayed on Router A is as follows:

```
```

The output shows that Router A sets the next hop for the received packets to 150::2 according to IPv6 PBR. The packets are forwarded through GigabitEthernet 1/0/2.

# Ping Loopback 0 of Router B from Host A, and set the data length to 200 bytes.

```
C:\>ping -n 1 -l 200 10::1
```

Pinging 10::1 with 200 bytes of data:

Reply from 10::1: time=1ms

Ping statistics for 10::1:
   Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 1ms, Maximum = 1ms, Average = 1ms

The debugging information about IPv6 PBR displayed on Router A is as follows:
The output shows that Router A sets the next hop for the received packets to 151::2 according to IPv6 PBR. The packets are forwarded through GigabitEthernet 1/0/3.
Configuring routing policies

Overview

Routing policies control routing paths by filtering and modifying routing information. This chapter describes both IPv4 and IPv6 routing policies.

Routing policies can filter advertised, received, and redistributed routes, and modify attributes for specific routes.

To configure a routing policy:

1. Configure filters based on route attributes, such as destination address and the advertising router's address.
2. Create a routing policy and apply filters to the routing policy.

Filters

Routing policies can use the following filters to match routes.

ACL

ACLs include IPv4 ACLs and IPv6 ACLs. An ACL can match the destination or next hop of routes. For more information about ACLs, see ACL and QoS Configuration Guide.

IP prefix list

IP prefix lists include IPv4 prefix lists and IPv6 prefix lists.

An IP prefix list matches the destination address of routes. You can use the gateway option to receive routes only from specific routers. For more information about the gateway option, see "Configuring RIP" and "Configuring OSPF."

An IP prefix list can contain multiple items that specify prefix ranges. Each destination IP address prefix of a route is compared with these items in ascending order of their index numbers. A prefix matches the IP prefix list if it matches one item in the list.

AS path list

An AS path list matches the AS_PATH attribute of BGP routes. For more information about AS path lists, see "Configuring BGP."

Community list

A community list matches the COMMUNITY attribute of BGP routes. For more information about community lists, see "Configuring BGP."

Extended community list

An extended community list matches the extended community attribute (Route-Target for VPN and Site of Origin) of BGP routes.

For more information about extended community lists, see MPLS Configuration Guide.

MAC list

A MAC list matches MAC addresses contained in EVI IS-IS packets.

A MAC list can contain multiple items that specify MAC address ranges. Each MAC address entry in an EVI IS-IS packet is compared with these items in ascending order of their index numbers. A MAC address entry matches the MAC list if it matches one item in the list.
Routing policy

A routing policy can contain multiple nodes, which are in a logical OR relationship. A node with a smaller number is matched first. A route matches the routing policy if it matches one node (except the node configured with the continue clause) in the routing policy.

Each node has a match mode of permit or deny.

- **permit**—Specifies the permit match mode for a routing policy node. If a route meets all the if-match clauses of the node, it is handled by the apply clauses of the node. The route is not compared with the next node unless the continue clause is configured. If a route does not meet all the if-match clauses of the node, it is compared with the next node.

- **deny**—Specifies the deny match mode for a routing policy node. The apply and continue clauses of a deny node are never executed. If a route meets all the if-match clauses of the node, it is denied without being compared with the next node. If a route does not meet all the if-match clauses of the node, it is compared with the next node.

A node can contain a set of if-match, apply, and continue clauses.

- **if-match** clauses—Specify the match criteria that match the attributes of routes. The if-match clauses are in a logical AND relationship. A route must meet all the if-match clauses to match the node.

- **apply** clauses—Specify the actions to be taken on permitted routes, such as modifying a route attribute.

- **continue** clause—Specifies the next node. A route that matches the current node (permit node) must match the specified next node in the same routing policy. The continue clause combines the if-match and apply clauses of the two nodes to improve flexibility of the routing policy.

Follow these guidelines when you configure if-match, apply, and continue clauses:

- If you only want to filter routes, do not configure apply clauses.
- If you do not configure any if-match clauses for a permit node, the node will permit all routes.
- Configure a permit node containing no if-match or apply clauses following multiple deny nodes to allow unmatched routes to pass.

Configuring filters

Configuration prerequisites

Determine the IP prefix list name, matching address range, and community list number.

Configuring an IP prefix list

**Configuring an IPv4 prefix list**

If all the items are set to deny mode, no routes can pass the IPv4 prefix list. To permit unmatched IPv4 routes, you must configure the permit 0.0.0.0 0 less-equal 32 item following multiple deny items.

To configure an IPv4 prefix list:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure an IPv4 prefix list.</td>
<td>ip prefix-list prefix-list-name [ index index-number ] { deny</td>
</tr>
</tbody>
</table>
### Configuring an IPv6 prefix list

If all items are set to **deny** mode, no routes can pass the IPv6 prefix list. To permit unmatched IPv6 routes, you must configure the **permit :: 0 less-equal 128** item following multiple **deny** items.

To configure an IPv6 prefix list:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure an IPv6 prefix list.</td>
<td></td>
</tr>
</tbody>
</table>

```
ipv6 prefix-list prefix-list-name [ index index-number ] { deny | permit } ipv6-address { prefix-length | inverse inverse-prefix-length [ greater-equal min-prefix-length ] [ less-equal max-prefix-length ] }
```

By default, no IPv6 prefix lists exist.

### Configuring an AS path list

You can configure multiple items for an AS path list that is identified by a number. The relationship between the items is logical OR. A route matches the AS path list if it matches one item in the list.

To configure an AS path list:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure an AS path list.</td>
<td>ip as-path as-path-number { deny</td>
</tr>
</tbody>
</table>

By default, no AS path lists exist.

### Configuring a community list

You can configure multiple items for a community list that is identified by a number. The relationship between the items is logical OR. A route matches the community list if it matches one item in the list.

To configure a community list:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure a community list.</td>
<td></td>
</tr>
</tbody>
</table>

- Configure a basic community list:
  ```
ip community-list { basic-comm-list-num | basic basic-comm-list-name } { deny | permit | community-number<&1-32> | aa:nn<&1-32> | internet | no-advertise | no-export | no-export-subconfed }
```

- Configure an advanced community list:
  ```
ip community-list { adv-comm-list-num | advanced adv-comm-list-name } { deny | permit } regular-expression
```

By default, no community lists exist.
Configuring an extended community list

You can configure multiple items for an extended community list that is identified by a number. The relationship between the items is logical OR. A route matches the extended community list if it matches one item in the list.

To configure an extended community list:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure an extended community list.</td>
<td>ip extcommunity-list ext-comm-list-number { deny</td>
</tr>
</tbody>
</table>

Configuring a MAC list

If all the items are set to deny mode, no MAC address entries can pass the MAC list. To permit unmatched MAC address entries, you must configure the permit 0-0-0 0 item following multiple deny items.

To configure a MAC list:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure a MAC list.</td>
<td>mac-list mac-list-name [ index index-number ] { deny</td>
</tr>
</tbody>
</table>

Configuring a routing policy

Configuration prerequisites

Configure filters and routing protocols, and determine the routing policy name, node numbers, match criteria, and the attributes to be modified.

Creating a routing policy

For a routing policy that has more than one node, configure a minimum of one permit node. A route that does not match any node cannot pass the routing policy. If all the nodes are in deny mode, no routes can pass the routing policy.

To create a routing policy:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create a routing policy and a node, and enter routing policy node view.</td>
<td>route-policy route-policy-name { deny</td>
</tr>
</tbody>
</table>
Configuring if-match clauses

You can either specify no `if-match` clauses or multiple `if-match` clauses for a routing policy node. If no `if-match` clause is specified for a permit node, all routes can pass the node. If no `if-match` clause is specified for a deny node, no routes can pass the node.

The `if-match` clauses of a routing policy node have a logical AND relationship. A route must meet all `if-match` clauses before it can be executed by the `apply` clauses of the node. If an `if-match` command exceeds the maximum length, multiple `if-match` clauses of the same type are generated. These clauses have a logical OR relationship. A route only needs to meet one of them.

To configure `if-match` clauses:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter routing policy node view.</td>
<td><code>route-policy</code> route-policy-name { deny</td>
</tr>
<tr>
<td>3.</td>
<td>Match routes whose destination, next hop, or source address matches an ACL or prefix list.</td>
<td>• Match IPv4 routes whose destination, next hop, or source address matches an ACL or IPv4 prefix list: `if-match ip { address</td>
</tr>
<tr>
<td>4.</td>
<td>Match BGP routes whose AS_PATH attribute matches a specified AS path list.</td>
<td><code>if-match as-path as-path-number&lt;1-32&gt;</code></td>
</tr>
<tr>
<td>5.</td>
<td>Match BGP routes whose COMMUNITY attribute matches a specified community list.</td>
<td>`if-match community { { basic-community-list-number</td>
</tr>
<tr>
<td>6.</td>
<td>Match routes having the specified cost.</td>
<td><code>if-match cost cost-value</code></td>
</tr>
<tr>
<td>7.</td>
<td>Match BGP routes whose extended community attribute matches a specified extended community list.</td>
<td><code>if-match extcommunity ext-comm-list-number&lt;1-32&gt;</code></td>
</tr>
<tr>
<td>8.</td>
<td>Match routes having the specified output interface.</td>
<td><code>if-match interface { interface-type interface-number }&lt;1-16&gt;</code></td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>9.</td>
<td>if-match local-preference preference</td>
<td>This command is not supported by BGP.</td>
</tr>
<tr>
<td>10.</td>
<td>if-match mac-list mac-list-name</td>
<td>By default, no MAC list match criterion is configured.</td>
</tr>
<tr>
<td>11.</td>
<td>if-match mpls-label</td>
<td>By default, no MPLS label match criterion is configured.</td>
</tr>
<tr>
<td>12.</td>
<td>if-match route-type { external-type1</td>
<td>external-type1or2</td>
</tr>
<tr>
<td>13.</td>
<td>if-match tag tag-value</td>
<td>By default, no tag match criterion is configured.</td>
</tr>
<tr>
<td>14.</td>
<td>if-match vlan vlan-list</td>
<td>By default, no VLAN match criterion is configured.</td>
</tr>
</tbody>
</table>

Configuring apply clauses

Except for the **apply** commands used for setting the next hop for IPv4 and IPv6 routes, all **apply** commands are the same for IPv4 and IPv6 routing.

To configure **apply** clauses:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>route-policy route-policy-name { deny</td>
<td>permit } node node-number</td>
</tr>
<tr>
<td>3.</td>
<td>apply as-path as-number&amp;&lt;1-32&gt; [ replace ]</td>
<td>By default, no AS_PATH attribute is set for BGP routes.</td>
</tr>
<tr>
<td>4.</td>
<td>apply comm-list { comm-list-number</td>
<td>comm-list-name } delete</td>
</tr>
<tr>
<td>5.</td>
<td>apply community { none</td>
<td>additive</td>
</tr>
<tr>
<td>6.</td>
<td>apply cost [ +</td>
<td>- ] cost-value</td>
</tr>
<tr>
<td>7.</td>
<td>apply cost-type { external</td>
<td>internal</td>
</tr>
<tr>
<td>8.</td>
<td>apply extcommunity { rt route-target }&amp;&lt;1-32&gt;</td>
<td>By default, no extended community attribute is set for BGP routes.</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| 9.   | • Set the next hop for IPv4 routes: apply ip-address next-hop ip-address [ public | vpn-instance vpn-instance-name ]  
• Set the next hop for IPv6 routes: apply ipv6 next-hop ipv6-address | By default, no next hop is set for IPv4 or IPv6 routes. The apply ip-address next-hop and apply ipv6 next-hop commands do not apply to redistributed IPv4 and IPv6 routes. |
| 10.  | apply ip-precedence { value | clear } | By default, no IP precedence is set. |
| 11.  | apply isis { level-1 | level-1-2 | level-2 } | By default, routes are not redistributed into the specified IS-IS level. |
| 12.  | apply local-preference preference | By default, no local preference is set for BGP routes. |
| 13.  | apply mpls-label | By default, no MPLS label is set. |
| 14.  | apply origin { egp as-number | igp | incomplete } | By default, no ORIGIN attribute is set for BGP routes. |
| 15.  | apply preference preference | By default, no preference is set. |
| 16.  | apply preferred-value preferred-value | By default, no preferred value is set for BGP routes. |
| 17.  | apply prefix-priority { critical | high | medium } | By default, no prefix priority is set, which means the prefix priority is low. |
| 18.  | apply qos-local-id { local-id-value | clear } | By default, no local QoS ID is set. |
| 19.  | apply tag tag-value | By default, no tag value is set for IGP routes. |
| 20.  | apply traffic-index { value | clear } | By default, no traffic index is set for BGP routes. |
| 21.  | • Set an IPv4 backup link for FRR: apply fast-reroute { backup-interface interface-type interface-number [ backup-nexthop ip-address ] | backup-nexthop ip-address }  
• Set an IPv6 backup link for FRR: apply ipv6 fast-reroute backup-nexthop ipv6-address | By default, no backup link is set for FRR. |
Configuring the continue clause

Follow these guidelines when you configure the continue clause to combine multiple nodes:

- If you configure an apply clause that sets different attribute values on all the nodes, the apply clause of the node configured most recently takes effect.
- If you configure the following apply clauses on all the nodes, the apply clause of each node takes effect:
  - apply as-path without the replace keyword.
  - apply cost with the + or – keyword.
  - apply community with the additive keyword.
  - apply extcommunity with the additive keyword.
- The apply comm-list delete clause configured on the current node cannot delete the community attributes set by the apply community clauses of the preceding nodes.

To configure the continue clause:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter routing policy node view.</td>
<td>route-policy route-policy-name { deny</td>
</tr>
<tr>
<td>3.</td>
<td>Specify the next node to be matched.</td>
<td>continue [ node-number ]</td>
</tr>
</tbody>
</table>

Displaying and maintaining the routing policy

Execute display commands in any view and reset commands in user view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display BGP AS path list information.</td>
<td>display ip as-path [ as-path-number ]</td>
</tr>
<tr>
<td>Display BGP community list information.</td>
<td>display ip community-list [ basic-community-list-number</td>
</tr>
<tr>
<td>Display BGP extended community list information.</td>
<td>display ip extcommunity-list [ ext-comm-list-number ]</td>
</tr>
<tr>
<td>Display IPv4 prefix list statistics.</td>
<td>display ip prefix-list [ name prefix-list-name ]</td>
</tr>
<tr>
<td>Display IPv6 prefix list statistics.</td>
<td>display ipv6 prefix-list [ name prefix-list-name ]</td>
</tr>
<tr>
<td>Display MAC list statistics.</td>
<td>display mac-list [ name mac-list-name ]</td>
</tr>
<tr>
<td>Display routing policy information.</td>
<td>display route-policy [ name route-policy-name ]</td>
</tr>
<tr>
<td>Clear IPv4 prefix list statistics.</td>
<td>reset ip prefix-list [ prefix-list-name ]</td>
</tr>
<tr>
<td>Clear IPv6 prefix list statistics.</td>
<td>reset ipv6 prefix-list [ prefix-list-name ]</td>
</tr>
<tr>
<td>Clear MAC list statistics.</td>
<td>reset mac-list [ mac-list-name ]</td>
</tr>
</tbody>
</table>
Routing policy configuration examples

Routing policy configuration example for IPv4 route redistribution

Network requirements

As shown in Figure 120, Router B exchanges routing information with Router A by using OSPF and with Router C by using IS-IS.

On Router B, enable route redistribution from IS-IS to OSPF. Use a routing policy to set the cost of route 172.17.1.0/24 to 100 and the tag of route 172.17.2.0/24 to 20.

Figure 120 Network diagram

Configuration procedure

1. Configure IP addresses for interfaces. (Details not shown.)
2. Configure IS-IS:
   # Configure Router C.
   <RouterC> system-view
   [RouterC] isis
   [RouterC-isis-1] is-level level-2
   [RouterC-isis-1] network-entity 10.0000.0000.0001.00
   [RouterC-isis-1] quit
   [RouterC] interface gigabitethernet 1/0/1
   [RouterC-GigabitEthernet1/0/1] isis enable
   [RouterC-GigabitEthernet1/0/1] quit
   [RouterC] interface gigabitethernet 1/0/2
   [RouterC-GigabitEthernet1/0/2] isis enable
   [RouterC-GigabitEthernet1/0/2] quit
   [RouterC] interface gigabitethernet 1/0/3
   [RouterC-GigabitEthernet1/0/3] isis enable
   [RouterC-GigabitEthernet1/0/3] quit
   [RouterC] interface gigabitethernet 1/0/4
   [RouterC-GigabitEthernet1/0/4] isis enable
   [RouterC-GigabitEthernet1/0/4] quit
   # Configure Router B.
3. **Configure OSPF and route redistribution:**
   
   # Configure OSPF on Router A.
   ```
   <RouterA> system-view
   [RouterA] ospf
   [RouterA-ospf-1] area 0
   [RouterA-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
   [RouterA-ospf-1-area-0.0.0.0] quit
   [RouterA-ospf-1] quit
   ```
   
   # On Router B, configure OSPF and enable route redistribution from IS-IS to OSPF.
   ```
   [RouterB] ospf
   [RouterB-ospf-1] area 0
   [RouterB-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
   [RouterB-ospf-1-area-0.0.0.0] quit
   [RouterB-ospf-1] import-route isis 1
   [RouterB-ospf-1] quit
   ```
   
   # Display the OSPF routing table on Router A to view the redistributed routes.
   ```
   [RouterA] display ospf routing
   OSPF Process 1 with Router ID 192.168.1.1
   Routing Tables
   Routing for Network
   Destination         Cost     Type    NextHop        AdvRouter     Area
   192.168.1.0/24     1        Transit 192.168.1.1    192.168.1.1   0.0.0.0
   
   Routing for ASEs
   Destination         Cost     Type    Tag        NextHop        AdvRouter
   172.17.1.0/24      1        Type2   1          192.168.1.2    192.168.2.2
   172.17.2.0/24      1        Type2   1          192.168.1.2    192.168.2.2
   172.17.3.0/24      1        Type2   1          192.168.1.2    192.168.2.2
   
   Total Nets: 4
   Intra Area: 1  Inter Area: 0  ASE: 3  NSSA: 0
   ```
   
4. **Configure filtering lists on Router B:**
   
   # Configure IPv4 basic ACL 2002 to permit route 172.17.2.0/24.
   ```
   [RouterB] acl basic 2002
   [RouterB-acl-ipv4-basic-2002] rule permit source 172.17.2.0 0.0.0.255
   [RouterB-acl-ipv4-basic-2002] quit
   ```
   
   # Configure IP prefix list prefix-a to permit route 172.17.1.0/24.
   ```
   [RouterB] ip prefix-list prefix-a index 10 permit 172.17.1.0 24
   ```
5. Configure a routing policy on Router B:

```plaintext
[RouterB] route-policy isis2ospf permit node 10
[RouterB-route-policy-isis2ospf-10] if-match ip address prefix-list prefix-a
[RouterB-route-policy-isis2ospf-10] apply cost 100
[RouterB-route-policy-isis2ospf-10] quit
[RouterB] route-policy isis2ospf permit node 20
[RouterB-route-policy-isis2ospf-20] if-match ip address acl 2002
[RouterB-route-policy-isis2ospf-20] apply tag 20
[RouterB-route-policy-isis2ospf-20] quit
[RouterB] route-policy isis2ospf permit node 30
[RouterB-route-policy-isis2ospf-30] quit
```

6. Apply the routing policy to route redistribution on Router B:

```plaintext
# On Router B, enable route redistribution from IS-IS to OSPF and apply the routing policy.
[RouterB] ospf
[RouterB-ospf-1] import-route isis 1 route-policy isis2ospf
[RouterB-ospf-1] quit

# Display OSPF routing table information on Router A.
[RouterA] display ospf routing

OSPF Process 1 with Router ID 192.168.1.1
Routing Tables

Routing for Network
Destination        Cost     Type    NextHop         AdvRouter     Area
192.168.1.0/24     1        Transit 192.168.1.1     192.168.1.1   0.0.0.0

Routing for ASEs
Destination        Cost     Type    Tag         NextHop       AdvRouter
172.17.1.0/24      100      Type2   1           192.168.1.2   192.168.2.2
172.17.2.0/24      1        Type2   20          192.168.1.2   192.168.2.2
172.17.3.0/24      1        Type2   1           192.168.1.2   192.168.2.2

Total Nets: 4
Intra Area: 1  Inter Area: 0  ASE: 3  NSSA: 0

The output shows that the cost of route 172.17.1.0/24 is 100 and the tag of route 172.17.2.0/24 is 20.

Routing policy configuration example for IPv6 route redistribution

Network requirements

As shown in Figure 121:

- Run RIPng on Router A and Router B.
- Configure three static routes on Router A.
- On Router A, apply a routing policy to redistribute static routes 20::/32 and 40::/32 and deny route 30::/32.
Configuration procedure

1. Configure Router A:
   # Configure IPv6 addresses for interfaces GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.
   
   <RouterA> system-view
   [RouterA] interface gigabitethernet 1/0/1
   [RouterA-GigabitEthernet1/0/1] ipv6 address 10::1 32
   [RouterA-GigabitEthernet1/0/1] quit
   [RouterA] interface gigabitethernet 1/0/2
   [RouterA-GigabitEthernet1/0/2] ipv6 address 11::1 32
   [RouterA-GigabitEthernet1/0/2] quit
   
   # Enable RIPng on GigabitEthernet 1/0/1.
   [RouterA] interface gigabitethernet 1/0/1
   [RouterA-GigabitEthernet1/0/1] ripng 1 enable
   
   # Configure three static routes with next hop 11::2, and make sure the static routes are active.
   [RouterA] ipv6 route-static 20:: 32 11::2
   [RouterA] ipv6 route-static 30:: 32 11::2
   [RouterA] ipv6 route-static 40:: 32 11::2
   
   # Configure a routing policy.
   [RouterA] ipv6 prefix-list a index 10 permit 30:: 32
   [RouterA] route-policy static2ripng deny node 0
   [RouterA-route-policy-static2ripng-0] if-match ipv6 address prefix-list a
   [RouterA-route-policy-static2ripng-0] quit
   [RouterA] route-policy static2ripng permit node 10
   [RouterA-route-policy-static2ripng-10] quit
   
   # Enable RIPng and apply routing policy static2ripng to filter redistributed static routes on Router A.
   [RouterA] ripng
   [RouterA-ripng-1] import-route static route-policy static2ripng

2. Configure Router B:
   # Configure the IPv6 address of GigabitEthernet 1/0/1.
   
   <RouterB> system-view
   [RouterB] interface gigabitethernet 1/0/1
   [RouterB-GigabitEthernet1/0/1] ipv6 address 10::2 32
   
   # Enable RIPng.
   [RouterB] ripng
   [RouterB-ripng-1] quit
   
   # Enable RIPng on the interface.
   [RouterB] interface gigabitethernet 1/0/1
Verifying the configuration

# Display the RIPng routing table on Router B.

```plaintext
[RouterB] display ripng 1 route
Route Flags: A - Aging, S - Suppressed, G - Garbage-collect
```

Verifying the configuration

# Display the RIPng routing table on Router B.

```plaintext
[RouterB] display ripng 1 route
Route Flags: A - Aging, S - Suppressed, G - Garbage-collect

Peer FE80::7D58:0:CA03:1 on GigabitEthernet1/0/1
  Destination 10::/32,
    via FE80::7D58:0:CA03:1, cost 1, tag 0, A, 18 secs
  Destination 20::/32,
    via FE80::7D58:0:CA03:1, cost 1, tag 0, A, 8 secs
  Destination 40::/32,
    via FE80::7D58:0:CA03:1, cost 1, tag 0, A, 3 secs
```
Configuring MTR

Overview

Multi-Topology Routing (MTR) splits a base topology into multiple topologies, which intersect or overlap with one another. Route calculation is performed on a per-topology basis.

For example, IS-IS MTR enables IS-IS to perform separate route calculation for the IPv4 and IPv6 topologies in an IS-IS routing domain.

Work mechanism

As shown in Figure 122, the base topology is split into two topologies, topology A and topology B. You can forward voice traffic through topology A and video traffic through topology B.

Router B does not belong to topology A. In topology B, no direct link exists between Router A and Router D, and between Router B and Router C. Route calculation and traffic forwarding are performed in each topology independently.

Supported features

- IS-IS MTR. For more information, see "Configuring IS-IS" and "Configuring IPv6 IS-IS."
- Static routing MTR. For more information, see "Configuring static routing."

Configuring MTR

MTR classifies traffic by MTR policy. An MTR policy uses ACL, DSCP, and IP precedence as the match criteria.

An MTR policy can contain multiple nodes, which are in a logical OR relationship. A node with a smaller number is matched first. A packet that matches one node matches the MTR policy.

Each node contains a set of if-match and apply clauses.
- **if-match**—Defines a criterion to match packet attributes. The **if-match** clauses of a node are in an OR relationship. If a packet matches one of the **if-match** clauses, it matches the node.
- **apply**—Specifies a topology for packets matching the MTR policy node.

### IMPORTANT:
A node must contain both **if-match** and **apply** clauses. Otherwise, the topology configuration cannot take effect.

To configure MTR:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create the global address family and enter its view.</td>
<td>global-address-family ipv4 [ unicast ]</td>
</tr>
<tr>
<td>3.</td>
<td>Create a topology and enter its view.</td>
<td>topology topo-name</td>
</tr>
<tr>
<td>4.</td>
<td>(Optional.) Configure the maximum number of active routes supported by the topology.</td>
<td>routing-table limit number { warn-threshold</td>
</tr>
<tr>
<td>5.</td>
<td>Return to system view.</td>
<td>quit</td>
</tr>
<tr>
<td>6.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>7.</td>
<td>Associate the interface with a topology and enter IPv4 unicast topology view of the interface.</td>
<td>topology ipv4 [ unicast ] topo-name</td>
</tr>
<tr>
<td>8.</td>
<td>Return to system view.</td>
<td>quit</td>
</tr>
<tr>
<td>9.</td>
<td>Create an MTR policy node and enter its view.</td>
<td>mtr-policy policy-name node node-value</td>
</tr>
<tr>
<td>10.</td>
<td>Specify a topology for the MTR policy node.</td>
<td>apply topology topo-name</td>
</tr>
<tr>
<td>11.</td>
<td>Configure the match criteria.</td>
<td></td>
</tr>
</tbody>
</table>
|      | - Configure an ACL match criterion:  
      |  **if-match** ip acl acl-number | |
|      | - Configure a DSCP match criterion:  
      |  **if-match** ip dscp dscp-value | |
|      | - Configure an IP precedence match criterion:  
      |  **if-match** ip precedence ip-prec-value | |
| 12.  | Return to system view. | quit | N/A |
| 13.  | Enter global address family view. | global-address-family ipv4 [ unicast ] | N/A |
| 14.  | Enable the MTR policy. | topology-routing mtr-policy policy-name | By default, the MTR policy is disabled. |
## Displaying and maintaining MTR

Execute `display` commands in any view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display topology information.</td>
<td><code>display topology [ name topo-name ]</code></td>
</tr>
<tr>
<td>Display MTR policy information.</td>
<td><code>display mtr-policy [ name mtr-policy-name ]</code></td>
</tr>
</tbody>
</table>
Document conventions and icons

Conventions

This section describes the conventions used in the documentation.

Port numbering in examples

The port numbers in this document are for illustration only and might be unavailable on your device.

Command conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Boldface</strong></td>
<td>Bold text represents commands and keywords that you enter literally as shown.</td>
</tr>
<tr>
<td><em>Italic</em></td>
<td>Italic text represents arguments that you replace with actual values.</td>
</tr>
<tr>
<td>[]</td>
<td>Square brackets enclose syntax choices (keywords or arguments) that are optional.</td>
</tr>
<tr>
<td>{ x</td>
<td>y</td>
</tr>
<tr>
<td>[ x</td>
<td>y</td>
</tr>
<tr>
<td>{ x</td>
<td>y</td>
</tr>
<tr>
<td>[ x</td>
<td>y</td>
</tr>
<tr>
<td>&amp;&lt;1-n&gt;</td>
<td>The argument or keyword and argument combination before the ampersand (&amp;) sign can be entered 1 to n times.</td>
</tr>
<tr>
<td>#</td>
<td>A line that starts with a pound (#) sign is comments.</td>
</tr>
</tbody>
</table>

GUI conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Boldface</strong></td>
<td>Window names, button names, field names, and menu items are in Boldface. For example, the <em>New User</em> window appears; click <strong>OK</strong>.</td>
</tr>
<tr>
<td>&gt;</td>
<td>Multi-level menus are separated by angle brackets. For example, <em>File &gt; Create &gt; Folder</em>.</td>
</tr>
</tbody>
</table>

Symbols

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>▶️ <strong>WARNING!</strong></td>
<td>An alert that calls attention to important information that if not understood or followed can result in personal injury.</td>
</tr>
<tr>
<td>▶️ <strong>CAUTION:</strong></td>
<td>An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.</td>
</tr>
<tr>
<td>🔄 <strong>IMPORTANT:</strong></td>
<td>An alert that calls attention to essential information.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>An alert that contains additional or supplementary information.</td>
</tr>
<tr>
<td>💡 <strong>TIP:</strong></td>
<td>An alert that provides helpful information.</td>
</tr>
</tbody>
</table>
## Network topology icons

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Icon" /></td>
<td>Represents a generic network device, such as a router, switch, or firewall.</td>
</tr>
<tr>
<td><img src="image2.png" alt="Icon" /></td>
<td>Represents a routing-capable device, such as a router or Layer 3 switch.</td>
</tr>
<tr>
<td><img src="image3.png" alt="Icon" /></td>
<td>Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.</td>
</tr>
<tr>
<td><img src="image4.png" alt="Icon" /></td>
<td>Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.</td>
</tr>
<tr>
<td><img src="image5.png" alt="Icon" /></td>
<td>Represents an access point.</td>
</tr>
<tr>
<td><img src="image6.png" alt="Icon" /></td>
<td>Represents a wireless terminator unit.</td>
</tr>
<tr>
<td><img src="image7.png" alt="Icon" /></td>
<td>Represents a wireless terminator.</td>
</tr>
<tr>
<td><img src="image8.png" alt="Icon" /></td>
<td>Represents a mesh access point.</td>
</tr>
<tr>
<td><img src="image9.png" alt="Icon" /></td>
<td>Represents omnidirectional signals.</td>
</tr>
<tr>
<td><img src="image10.png" alt="Icon" /></td>
<td>Represents directional signals.</td>
</tr>
<tr>
<td><img src="image11.png" alt="Icon" /></td>
<td>Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.</td>
</tr>
<tr>
<td><img src="image12.png" alt="Icon" /></td>
<td>Represents a security card, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG card.</td>
</tr>
</tbody>
</table>
Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:
  www.hpe.com/assistance
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:
  www.hpe.com/support/hpesc

Information to collect
- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates, go to either of the following:
  - Hewlett Packard Enterprise Support Center Get connected with updates page:
    www.hpe.com/support/e-updates
  - Software Depot website:
    www.hpe.com/support/softwaredepot
- To view and update your entitlements, and to link your contracts, Care Packs, and warranties with your profile, go to the Hewlett Packard Enterprise Support Center More Information on Access to Support Materials page:
  www.hpe.com/support/AccessToSupportMaterials

⚠️ IMPORTANT:
Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HP Passport set up with relevant entitlements.
Websites

<table>
<thead>
<tr>
<th>Website</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Networking websites</td>
<td></td>
</tr>
<tr>
<td>Hewlett Packard Enterprise Information Library for Networking</td>
<td><a href="http://www.hpe.com/networking/resourcefinder">www.hpe.com/networking/resourcefinder</a></td>
</tr>
<tr>
<td>Hewlett Packard Enterprise Networking website</td>
<td><a href="http://www.hpe.com/info/networking">www.hpe.com/info/networking</a></td>
</tr>
<tr>
<td>Hewlett Packard Enterprise My Networking website</td>
<td><a href="http://www.hpe.com/networking/support">www.hpe.com/networking/support</a></td>
</tr>
<tr>
<td>Hewlett Packard Enterprise Networking Warranty</td>
<td><a href="http://www.hpe.com/networking/warranty">www.hpe.com/networking/warranty</a></td>
</tr>
<tr>
<td>General websites</td>
<td></td>
</tr>
<tr>
<td>Hewlett Packard Enterprise Information Library</td>
<td><a href="http://www.hpe.com/info/enterprise/docs">www.hpe.com/info/enterprise/docs</a></td>
</tr>
<tr>
<td>Hewlett Packard Enterprise Support Center</td>
<td><a href="http://www.hpe.com/support/hpesc">www.hpe.com/support/hpesc</a></td>
</tr>
<tr>
<td>Hewlett Packard Enterprise Support Services Central</td>
<td>ssc.hpe.com/portal/site/ssc/</td>
</tr>
<tr>
<td>Contact Hewlett Packard Enterprise Worldwide</td>
<td><a href="http://www.hpe.com/assistance">www.hpe.com/assistance</a></td>
</tr>
<tr>
<td>Subscription Service/Support Alerts</td>
<td><a href="http://www.hpe.com/support/e-updates">www.hpe.com/support/e-updates</a></td>
</tr>
<tr>
<td>Software Depot</td>
<td><a href="http://www.hpe.com/support/softwaredepot">www.hpe.com/support/softwaredepot</a></td>
</tr>
<tr>
<td>Customer Self Repair (not applicable to all devices)</td>
<td><a href="http://www.hpe.com/support/selfrepair">www.hpe.com/support/selfrepair</a></td>
</tr>
<tr>
<td>Insight Remote Support (not applicable to all devices)</td>
<td><a href="http://www.hpe.com/info/insightremotesupport/docs">www.hpe.com/info/insightremotesupport/docs</a></td>
</tr>
</tbody>
</table>

Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website: www.hpe.com/support/selfrepair

Remote support

Remote support is available with supported devices as part of your warranty, Care Pack Service, or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product’s service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

For more information and device support details, go to the following website: www.hpe.com/info/insightremotesupport/docs

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback@hpe.com). When submitting your feedback, include the document title,
part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.
Index

Numerics

4-byte
IPv4 BGP AS number suppression, 273
IPv6 BGP AS number suppression, 273

6PE
BGP 6PE, 301
BGP 6PE basics, 301
BGP 6PE optional capabilities, 302
IPv6 BGP 6PE configuration, 352

A

ABR
OSPF route summarization, 81
OSPF router type, 70
OSPF summary network discard route, 84
OSPFv3 route summarization, 428

accounting
BGP policy accounting, 300

ACL
rout ing policy, 507

action
IPv6 PBR node action, 497
PBR node, 375

address
IS-IS area, 136
IS-IS format, 135
IS-IS NSAP format, 135
IS-IS PPP interface hello packet source address check, 153
IS-IS routing method, 136
MP-BGP address family, 211

adjacency
OSPF BDR, 72
OSPF DR, 72
OSPFv3 BFD configuration, 464
OSPFv3 configuration, 422, 423, 445
OSPFv3 DR election configuration, 452
OSPFv3 GR configuration, 462
OSPFv3 IPsec profile configuration, 469
OSPFv3NSSA area configuration, 450
OSPFv3route redistribution, 455
OSPFv3 stub area configuration, 445

advertising
BGP COMMUNITY NO_ADVERTISE path attribute, 200
BGP configuration, 200, 213
BGP default route to peer/peer group, 241
BGP optimal route, 240
BGP optimal route advertisement, 240
BGP route advertisement rules, 205
BGP route generation, 233
IPv4 BGP basic configuration, 308
IPv4 BGP BFD configuration, 334
IPv4 BGP COMMUNITY, 287
IPv4 BGP COMMUNITY configuration, 321
IPv4 BGP confederation, 326
IPv4 BGP configuration, 308
IPv4 BGP fake AS number advertisement, 263
IPv4 BGP GR configuration, 333
IPv4 BGP load balancing configuration, 318
IPv4 BGP path selection configuration, 330
IPv4 BGP route reflector configuration, 324
IPv4 BGP route summarization, 315
IPv4 BGP+IGP route redistribution, 312
IPv6 BGP basic configuration, 347
IPv6 BGP COMMUNITY, 287
IPv6 BGP configuration, 347
IPv6 BGP fake AS number advertisement, 263
IS-IS default route, 148
multicast BGP configuration, 341, 367
OSPF basics configuration, 105
OSPF configuration, 67, 73, 105
OSPF host route advertisement, 86
OSPF route summarization configuration, 110
RIP default route, 31
RIP on interface, 28
RIP summary route advertisement configuration, 51
RIPng default route, 400
RIPv2 summary route, 31
applying
IPv6 PBR apply clause, 494
OSPFv3 IPsec profile, 443
PBR apply clause, 372
RIPng IPsec profile, 407
routing policy apply clause, 508, 512
area
IS-IS, 137
IS-IS area address, 136
IS-IS authentication (area), 165
OSPF area, 76
OSPF area configuration (NSSA), 77, 115
OSPF area configuration (stub), 77, 113
OSPF areas, 68
OSPF authentication (area), 90
OSPF backbone, 69
OSPF network type, 78
OSPF NSSA area, 70
OSPF stub area, 69
OSPF totally NSSA area, 70
OSPF totally stub area, 69
OSPF virtual link, 78
OSPFv3 area parameter, 425
OSPFv3 NSSA area, 425
OSPFv3 NSSA area configuration, 450
OSPFv3 stub area, 425
OSPFv3 stub area configuration, 445
OSPFv3 virtual link, 426
AS
BGP confederation, 292
BGP confederation compatibility, 292
BGP configuration, 200, 213
BGP first AS number of EBGP route updates, 267
BGP MED attribute, 256
BGP path AS_PATH attribute, 200
BGP path AS_SEQUENCE attribute, 200
BGP path AS_SET attribute, 200
IPv4 BGP 4-byte AS number suppression, 273
IPv4 BGP AS number substitution, 264
IPv4 BGP basic configuration, 308
IPv4 BGP BFD configuration, 334
IPv4 BGP COMMUNITY configuration, 321
IPv4 BGP confederation, 326
IPv4 BGP configuration, 308
IPv4 BGP fake AS number advertisement, 263
IPv4 BGP FRR configuration, 338
IPv4 BGP GR configuration, 333
IPv4 BGP load balancing configuration, 318
IPv4 BGP local AS number appearance, 262
IPv4 BGP MED AS route comparison (confederation peers), 259, 259
IPv4 BGP MED AS route comparison (diff ASs), 257, 257
IPv4 BGP MED AS route comparison (per-AS), 257, 257
IPv4 BGP MED default value, 256
IPv4 BGP path selection configuration, 330
IPv4 BGP private AS number removal, 266
IPv4 BGP route reflector configuration, 324
IPv4 BGP route summarization, 315
IPv4 BGP+IGP route redistribution, 312
IPv6 BGP 4-byte AS number suppression, 273
IPv6 BGP AS number substitution, 264
IPv6 BGP basic configuration, 347
IPv6 BGP BFD configuration, 355
IPv6 BGP configuration, 347
IPv6 BGP fake AS number advertisement, 263
IPv6 BGP FRR configuration, 364
IPv6 BGP local AS number appearance, 262
IPv6 BGP MED AS route comparison (confederation peers), 259, 259
IPv6 BGP MED AS route comparison (diff ASs), 257, 257
IPv6 BGP MED AS route comparison (per-AS), 257, 257
IPv6 BGP MED default value, 256
IPv6 BGP private AS number removal, 266
IPv6 BGP route reflector configuration, 350
IS-IS authentication configuration, 187
IS-IS basic configuration, 143
IS-IS basics configuration, 175
IS-IS configuration, 135, 142, 175
IS-IS DIS election configuration, 179
IS-IS route redistribution, 183
multicast BGP configuration, 341, 367
OSPF areas, 68
OSPF AS External LSA, 67
routing policy AS_PATH list, 507, 509
AS_PATH
BGP attribute, 262
IPv4 BGP optimal route selection, 263
ASBR
OSPF ASBR summary LSA, 67
OSPF redistributed route summarization, 81
OSPF router type, 70
OSPF summary network discard route, 84
OSPFv3 redistributed route summarization, 428
assigning
IPv6 IS-IS route convergence priority, 477
ATT
IS-IS ATT bit, 159
IS-IS ATT bit default route calculation, 159
IS-IS ATT bit Level-1 LSP, 160
attribute
BGP AS_PATH attribute, 262
BGP MED attribute, 256
BGP path AS_PATH, 200
authenticating
- IPv4 BGP peer MD5 authentication, 274
- IPv6 BGP IPsec, 277
- IPv6 BGP peer MD5 authentication, 274
- IS-IS authentication (area), 165
- IS-IS authentication (neighbor relationship), 165
- IS-IS authentication (routing domain), 166
- IS-IS authentication configuration, 187
- IS-IS network security enhancement, 164
- OSPF configuration, 90
- RIPng IPsec profile application, 407
- RIPv2 message authentication configuration, 36

auto
- IPv4 BGP route summarization (automatic), 237
- IPv6 IS-IS automatic link cost calculation, 476
- IPv6 IS-IS FRR automatic backup next hop
- LFA calculation, 481
- IS-IS automatic cost calculation, 146

automatic
- RIPv2 automatic route summarization enable, 30

B
backbone
- OSPF backbone area, 69
- OSPF router type, 70
backing up
- IP routing route backup, 3
bandwidth
- OSPF reference value, 83
BDR
- OSPF, 72
BFD
- IPv4 BGP BFD configuration, 296
- IPv4 BGP BFD configuration configuration, 334
- IPv6 BGP BFD configuration, 296
- IPv6 BGP BFD configuration configuration, 355
- IPv6 IS-IS BFD configuration, 479, 488
- IPv6 IS-IS FRR BFD, 482
- IPv6 static route BFD configuration, 386
- IPv6 static route BFD control mode (direct next hop), 387
- IPv6 static route BFD control mode (indirect next hop), 387
- IPv6 static route BFD echo mode (single hop), 387
- IPv6 static routing BFD (direct next hop), 390
- IPv6 static routing BFD (indirect next hop), 393
- IS-IS BFD, 168
- IS-IS BFD configuration, 194
- IS-IS FRR BFD enable (control packet mode), 171
- IS-IS FRR BFD enable (echo packet mode), 171
- OSPF BFD, 101
- OSPF configuration, 127
- OSPF detection configuration (bidirectional control), 101
- OSPF detection configuration (single-hop echo), 102
- OSPF FRR configuration, 103
- OSPF PIC BFD, 96
- OSPFv3 BFD configuration, 440, 464
- OSPFv3 FRR configuration, 442
- RIP BFD configuration, 41
- RIP BFD configuration (bidirectional control detection), 42, 60
- RIP BFD configuration (single-hop echo detection/neighbor), 41
- RIP BFD configuration (single-hop echo detection/specific destination), 41, 58
- RIP BFD single-hop echo detection, 56
- RIP FRR BFD enable, 43
- RIPng FRR BFD enable, 406
- static routing BFD bidirectional control mode (direct next hop), 10
static routing BFD bidirectional control mode (indirect next hop), 10
static routing BFD configuration, 10
static routing BFD single-hop echo mode, 11
BGP, 200, See also MP-BGP
  6PE configuration, 301
  6PE optional capabilities, 302
  AS_PATH attribute configuration, 262
  basic configuration, 216
  community, 207
  confederation, 207, 292
  confederation compatibility, 292
  configuration, 200, 213
  configuration views, 211
  default route advertisement to peer/peer group, 241
  dynamic peer configuration, 219
  dynamic peer configuration (IPv4 multicast address), 221
  dynamic peer configuration (IPv4 unicast address), 220
  dynamic peer configuration (IPv6 multicast address), 221
  dynamic peer configuration (IPv6 unicast address), 220
  enable, 216
  first AS number of EBGP route updates, 267
  flushing the suboptimal BGP route to the RIB, 286
  FRR configuration, 297
  GR configuration, 293
  GR helper, 293
  GR reater, 293
  GTSM configuration, 279
  IP routing EBGP direct connections after link failure, 273
  IPv4 EBGP peer protection (low memory exemption), 285
  IPv4 SoO attribute configuration, 268
IPv6 EBGP peer protection (low memory exemption), 285
IPv6 SoO attribute configuration, 268
large scale network management, 207
large-scale network, 287
load balancing, 206
MED attribute configuration, 256
message types, 200
MP-BGP, 210
MP-BGP address family, 211
MP-BGP extended attributes, 210
MPLS local label update delay, 286
multi-instance, 211
network optimization, 269
NSR configuration, 294
optimal route advertisement, 240
path attributes, 200
path selection control, 251
peer, 200
peer configuration, 217
peer configuration (IPv4 multicast address), 219
peer configuration (IPv4 unicast address), 217
peer configuration (IPv6 multicast address), 219
peer configuration (IPv6 unicast address), 218
peer group, 207
peer group configuration, 222
policy accounting configuration, 300
protocols and standards, 213
route advertisement, 205
route dampening, 207
route distribution control, 237
route filtering policies, 244
route generation, 233
route reception control, 237
route recursion, 206
route reflection, 289
route reflector, 207
route selection, 205, 206
route summarization, 207, 237
routing policy AS_PATH list, 507
routing policy COMMUNITY list, 507
session state change logging, 295
SNMP notification enable, 295
soft reset configuration, 280
speaker, 200
TCP connection source address, 232
troubleshoot peer connection state, 371
tuning network, 269

bidirectional
forwarding detection. Use BFD
IPv6 static route BFD control mode (direct next hop), 387
IPv6 static route BFD control mode (indirect next hop), 387
IPv6 static route BFD echo mode (single hop), 387
OSPF BFD detection configuration (bidirectional control), 101
RIP BFD configuration (bidirectional control detection), 42, 60
static routing BFD bidirectional control mode (direct next hop), 10
static routing BFD bidirectional control mode (indirect next hop), 10
Border Gateway Protocol. Use BGP
broadcast
IS-IS network type, 138
OSPF interface network type, 79
OSPF network type, 72, 78
OSPFv3 network type, 426
OSPFv3 network type (interface), 427

C

calculating
IPv6 IS-IS SPF calculation interval, 478
IS-IS ATT bit default route calculation, 159
IS-IS SPF calculation interval, 157
OSPF FRR backup next hop calculation (LFA algorithm), 103
OSPF interface cost, 83
OSPF route calculation, 71
OSPF SPF calculation interval, 88
OSPFv3 FRR backup next hop calculation (LFA algorithm), 441
OSPFv3 SPF calculation interval, 433

checking
OSPFv3 DD packet ignore MTU check, 434
circuit
IS-IS IS+ circuit level, 143
classless inter-domain routing. Use CIDR
clearing
IPv4 BGP information, 307
IPv6 BGP information, 307

CLNP
IS-IS configuration, 142
CLV (IS-IS PDU), 140
command and hardware compatibility
IP performance optimization, 374, 496

community
BGP, 207
BGP COMMUNITY path attribute, 200
IPv4 BGP COMMUNITY, 287
IPv4 BGP COMMUNITY configuration, 321
IPv4 BGP ORIGINATOR_ID attribute, 291
IPv4 BGP route reflector, 289
IPv6 BGP route reflector, 289
routing policy extended community list, 507
routing policy list, 507

COMMUNITY
routing policy COMMUNITY list, 509

community
IPv6 BGP COMMUNITY, 287
IPv6 BGP ORIGINATOR_ID attribute, 291
routing policy extended community list, 510

comparing
IPv4 BGP MED AS route comparison (confederation peers), 259
IPv4 BGP MED AS route comparison (diff ASs), 257
IPv4 BGP MED AS route comparison (per-AS), 257
IPv6 BGP MED AS route comparison (confederation peers), 259
IPv6 BGP MED AS route comparison (diff ASs), 257
IPv6 BGP MED AS route comparison (per-AS), 257

confederating
BGP confederation, 207, 292
BGP confederation compatibility, 292
IPv4 BGP confederation, 326
IPv4 BGP MED AS route comparison (confederation peers), 259
IPv6 BGP MED AS route comparison (confederation peers), 259

configuring
BGP, 200, 213
BGP 6PE, 301
BGP 6PE basics, 301
BGP 6PE optional capabilities, 302
BGP AS_PATH attribute, 262
BGP basics, 216
BGP confederation, 292
BGP confederation compatibility, 292
BGP dynamic peer, 219
BGP dynamic peer (IPv4 multicast address), 221
BGP dynamic peer (IPv4 unicast address), 220
BGP dynamic peer (IPv6 multicast address), 221
BGP dynamic peer (IPv6 unicast address), 220
BGP FRR, 297
BGP GR, 293
BGP GR helper, 293
BGP GR restarter, 293
BGP GTSM, 279
BGP large-scale network, 287
BGP MED attribute, 256
BGP MPLS local label update delay, 286
BGP NSR, 294
BGP peer, 217
BGP peer (IPv4 multicast address), 219
BGP peer (IPv4 unicast address), 217
BGP peer (IPv6 multicast address), 219
BGP peer (IPv6 unicast address), 218
BGP peer group, 222
BGP policy accounting, 300
BGP route filtering policies, 244
BGP route redistribution, 237
BGP route reflection, 289
BGP soft reset, 280

EBGP peer group (IPv4 multicast address), 224
EBGP peer group (IPv4 unicast address), 224
EBGP peer group (IPv6 multicast address), 224
EBGP peer group (IPv6 unicast address), 224
IBGP peer group (IPv4 multicast address), 222
IBGP peer group (IPv4 unicast address), 222
IBGP peer group (IPv6 multicast address), 222
IBGP peer group (IPv6 unicast address), 222
interface PBR, 377
interface PBR (packet length-based), 381
interface PBR (packet source-IP-based), 383
interface PBR (packet type-based), 380
IP routing, 1
IP routing inter-protocol FRR, 6
IP routing IPv4 RIB inter-protocol FRR, 7
IP routing IPv6 RIB inter-protocol FRR, 7
IP routing RIB NSR, 5
IP routing RIP route redistribution, 47
IPv4 BGP, 308
IPv4 BGP AS number substitution, 264
IPv4 BGP basics, 308
IPv4 BGP BFD, 296, 334
IPv4 BGP COMMUNITY, 287, 321
IPv4 BGP confederation, 326
IPv4 BGP default local preference, 254
IPv4 BGP dynamic peer, 345
IPv4 BGP FRR, 338
IPv4 BGP GR, 333
IPv4 BGP hold time, 269
IPv4 BGP keepalive interval, 269
IPv4 BGP load balancing, 275, 318
IPv4 BGP manual soft reset, 283
IPv4 BGP MED default value, 256
IPv4 BGP NEXT_HOP attribute, 259
IPv4 BGP path selection, 330
IPv4 BGP route dampening, 250
IPv4 BGP route distribution filtering policies, 244
IPv4 BGP route preference, 253
IPv4 BGP route reception filtering policies, 247
IPv4 BGP route reflector, 289, 324
IPv4 BGP route summarization, 315
IPv4 BGP route summarization (automatic), 237
IPv4 BGP route summarization (manual), 238
IPv4 BGP route update delay, 250
IPv4 BGP route update interval, 271
IPv4 BGP SoO attribute, 268
IPv4 BGP+IGP route redistribution, 312
IPv4 RIB NSR, 5
IPv6 BGP, 347
IPv6 BGP 6PE, 352
IPv6 BGP AS number substitution, 264
IPv6 BGP basics, 347
IPv6 BGP BFD, 296, 355
IPv6 BGP COMMUNITY, 287
IPv6 BGP default local preference, 254
IPv6 BGP FRR, 364
IPv6 BGP hold time, 269
IPv6 BGP IPsec, 277
IPv6 BGP keepalive interval, 269
IPv6 BGP load balancing, 275
IPv6 BGP manual soft reset, 283
IPv6 BGP MED default value, 256
IPv6 BGP NEXT_HOP attribute, 259
IPv6 BGP packet IPsec, 359
IPv6 BGP route dampening, 250
IPv6 BGP route distribution filtering policies, 244
IPv6 BGP route preference, 253
IPv6 BGP route reception filtering policies, 247
IPv6 BGP route reflector, 289, 350
IPv6 BGP route summarization (manual), 238
IPv6 BGP route update interval, 271
IPv6 BGP SoO attribute, 268
IPv6 default route, 396
IPv6 IS-IS, 474, 484
IPv6 IS-IS basics, 474, 484
IPv6 IS-IS BFD, 479, 488
IPv6 IS-IS FRR, 480, 491
IPv6 IS-IS FRR automatic backup next hop LFA calculation, 481
IPv6 IS-IS FRR using routing policy, 481
IPv6 IS-IS global cost, 476
IPv6 IS-IS interface cost, 476
IPv6 IS-IS interface tag value, 478
IPv6 IS-IS link cost, 476
IPv6 IS-IS route control, 475
IPv6 PBR, 494, 497, 499, 500
IPv6 PBR interface, 499
IPv6 PBR interface (packet length-based), 503
IPv6 PBR interface (packet type-based), 502
IPv6 PBR local, 499
IPv6 PBR local (packet type-based), 500
IPv6 PBR node action, 497
IPv6 PBR policy, 497
IPv6 RIB NSR, 6
IPv6 static route, 386
IPv6 static route BFD, 386
IPv6 static route BFD control mode (direct next hop), 387
OSPF GTSM, 97
OSPF host route advertisement, 86
OSPF interface cost, 83
OSPF interface network type (broadcast), 79
OSPF interface network type (NBMA), 79
OSPF interface network type (P2MP), 80
OSPF interface network type (P2P), 80
OSPF LSU transmit rate, 94
OSPF network management, 93
OSPF network type, 78
OSPF NSR, 100, 125
OSPF packet DSCP value, 91
OSPF PIC, 95
OSPF PIC BFD, 96
OSPF preference, 84
OSPF prefix priority, 95
OSPF prefix suppression (interface), 95
OSPF prefix suppression (OSPF process), 95
OSPF received route filtering, 82
OSPF redistributed route default parameters, 85
OSPF redistributed route summarization (ASBR), 81
OSPF route control, 81
OSPF route redistribution, 108
OSPF route redistribution (another routing protocol), 85
OSPF route redistribution (default route), 85
OSPF route summarization, 110
OSPF route summarization (ABR), 81
OSPF stub router, 89
OSPF summary network discard route, 84
OSPF Type-3 LSA filtering, 82
OSPF virtual link, 78, 121
OSPFv3, 422, 423, 445
OSPFv3 area parameter, 425
OSPFv3 BFD, 440, 464
OSPFv3 DR election, 452
OSPFv3 FRR, 441, 467
OSPFv3 FRR backup next hop (routing policy), 442
OSPFv3 FRR backup next hop calculation (LFA algorithm), 441
OSPFv3 FRR BFD, 442
OSPFv3 GR, 438
OSPFv3 GR configuration, 462
OSPFv3 GR helper, 439
OSPFv3 GR restarter, 438
OSPFv3 Inter-Area-Prefix LSA filtering, 429
OSPFv3 interface cost, 429
OSPFv3 interface DR priority, 434
OSPFv3 IPsec profile configuration, 469
OSPFv3 LSU transmit rate, 436
OSPFv3 NBMA neighbor, 427
OSPFv3 network management, 435
OSPFv3 network type, 426
OSPFv3 network type (interface), 427
OSPFv3 NSR, 439, 463
OSPFv3 NSSA area, 425, 450
OSPFv3 P2MP neighbor, 427
OSPFv3 preference, 430
OSPFv3 prefix suppression (interface), 438
OSPFv3 prefix suppression (OSPFv3 process), 437
OSPFv3 received route filtering, 428
OSPFv3 redistributed route tag, 431
OSPFv3 route control, 427
OSPFv3 route redistribution, 455
OSPFv3 route redistribution (another routing protocol), 431
OSPFv3 route redistribution (default route), 431
OSPFv3 route summarization, 458
OSPFv3 route summarization (ABR), 428
OSPFv3 route summarization (ASBR), 428
OSPFv3 stub area, 425, 445
OSPFv3 stub router, 436
OSPFv3 virtual link, 426
PBR, 372, 375, 377, 378
continue clause (routing policy), 508, 514
controlling
  BGP path selection, 251
  BGP route distribution, 237
  BGP route reception, 237
  IPv6 IS-IS route control, 475
  IPv6 IS-IS SPF calculation interval, 478
  IPv6 static route BFD control mode (direct next hop), 387
  IPv6 static route BFD control mode (indirect next hop), 387
  IS-IS route control, 144
  IS-IS SPF calculation interval, 157
  OSPF route control, 81
  OSPFv3 route control, 427
  RIP additional routing metric configuration, 30
  RIP interface advertisement, 28
  RIP interface reception, 28, 28
  RIP route control configuration, 30
  RIPng route control, 399
convergence priority (IPv6 IS-IS), 477
convergence priority (IS-IS), 158
cost
  IPv6 IS-IS automatic link cost calculation, 476
  IPv6 IS-IS global cost, 476
  IPv6 IS-IS interface cost, 476
  IPv6 IS-IS link cost, 476
  IS-IS automatic cost calculation, 146
  IS-IS global cost, 145
  IS-IS interface cost, 145
  IS-IS link cost, 144
  OSPF interface cost, 83
  OSPFv3 interface cost, 429
creating
  IPv6 PBR node, 497
  PBR node, 375
  routing policy, 510
CSNP
  IS-IS CSNP packet send interval, 153
D
dampening
  BGP route dampening, 207
  IPv4 BGP route dampening, 250
  IPv6 BGP route dampening, 250
database
  OSPF DD packet, 67
DD
  OSPFv3 DD packet ignore MTU check, 434
  OSPFv3 packet type, 422
dead packet timer (OSPF), 86
default
  BGP default route advertisement to peer/peer group, 241
  IPv4 BGP default local preference, 254
  IPv4 BGP MED default value, 256
  IPv6 BGP default local preference, 254
  IPv6 BGP MED default value, 256
  IPv6 default route configuration, 396
  IS-IS default route advertisement, 148
  OSPF redistributed route default parameters, 85
  OSPFv3 route redistribution (default route), 431
  RIP default route advertisement, 31
  RIPng default route advertisement, 400
static routing configuration. See under static routing
delaying
  BGP MPLS local label update delay, 286
  OSPFv3 LSA transmission delay, 432
detecting
  IPv4 BGP BFD, 296
  IPv6 BGP BFD, 296
  OSPF BFD, 101
  OSPF BFD detection configuration (bidirectional control), 101
  OSPF BFD detection configuration (single-hop echo), 102
  OSPF FRR BFD, 103
  OSPFv3 FRR BFD, 442
RIP BFD configuration (bidirectional control detection), 42, 60
RIP BFD configuration (single-hop echo detection/neighbor), 41
RIP BFD configuration (single-hop echo detection/specific destination), 41, 58
RIP BFD single-hop echo detection, 41, 56
device
interface PBR configuration (packet length-based), 381
interface PBR configuration (packet source-IP-based), 383
interface PBR configuration (packet type-based), 380
IP routing RIP route redistribution configuration, 47
IPv4 BGP basic configuration, 308
IPv4 BGP BFD configuration, 334
IPv4 BGP COMMUNITY configuration, 321
IPv4 BGP confederation, 326
IPv4 BGP configuration, 308
IPv4 BGP dynamic peer configuration, 345
IPv4 BGP GR configuration, 333
IPv4 BGP load balancing configuration, 318
IPv4 BGP path selection configuration, 330
IPv4 BGP route reflector configuration, 324
IPv4 BGP route summarization, 315
IPv4 BGP+IGP route redistribution, 312
IPv6 BGP 6PE configuration, 352
IPv6 BGP basic configuration, 347
IPv6 BGP BFD configuration, 355
IPv6 BGP configuration, 347
IPv6 BGP route reflector configuration, 350
IPv6 IS-IS basic configuration, 484
IPv6 IS-IS BFD configuration, 488
IPv6 IS-IS configuration, 484
IPv6 IS-IS FRR configuration, 491
IPv6 PBR configuration, 500
IPv6 PBR interface configuration (packet length-based), 503
IPv6 PBR interface configuration (packet type-based), 502
IPv6 PBR local configuration (packet type-based), 500
IPv6 static routing, 388
IPv6 static routing basics, 388
IPv6 static routing BFD (direct next hop), 390
IPv6 static routing BFD (indirect next hop), 393
IS-IS authentication configuration, 187
IS-IS basics configuration, 175
IS-IS BFD configuration, 194
IS-IS configuration, 175
IS-IS DIS election configuration, 179
IS-IS FRR configuration, 197
IS-IS GR configuration, 189
IS-IS NSR configuration, 190
IS-IS route redistribution, 183
local PBR configuration (packet type-based), 378
multicast BGP configuration, 341, 367
OSPF ABR router type, 70
OSPF area configuration (NSSA), 115
OSPF area configuration (stub), 113
OSPF ASBR router type, 70
OSPF backbone router type, 70
OSPF basics configuration, 105
OSPF BFD configuration, 127
OSPF configuration, 105
OSPF DR election configuration, 117
OSPF FRR configuration, 130
OSPF GR configuration, 123
OSPF internal router type, 70
OSPF route redistribution configuration, 108
OSPF route summarization configuration, 110
OSPF stub router, 89
OSPF virtual link configuration, 121
OSPFv3 BFD configuration, 464
OSPFv3 configuration, 445
OSPFv3 DR election configuration, 452
OSPFv3 FRR configuration, 467
OSPFv3 GR configuration, 462
OSPFv3 IPsec profile configuration, 469
OSPFv3 NSSA area configuration, 450
OSPFv3 route redistribution, 455
OSPFv3 route summarization, 458
OSPFv3 stub area configuration, 445
OSPFv3 stub router, 436
RIP basic configuration, 44
RIP BFD configuration (bidirectional control detection), 60
RIP BFD configuration (single-hop echo detection/specific destination), 58
RIP BFD single-hop echo detection, 56
RIP configuration, 44
RIP FRR configuration, 64
RIP GR configuration, 53
RIP interface additional metric configuration, 49
RIP NSR configuration, 54
RIP summary route advertisement configuration, 51
RIPng basic configuration, 408
RIPng configuration, 408
RIPng FRR configuration, 416
RIPng GR configuration, 413
RIPng IPsec profile configuration, 419
RIPng route redistribution, 411
routing policy configuration, 515
routing policy configuration (IPv4 route redistribution), 515
routing policy configuration (IPv6 route redistribution), 517
static routing basic configuration, 14
static routing BFD configuration (direct next hop), 16
static routing BFD configuration (indirect next hop), 18
static routing configuration, 14
static routing FRR configuration, 21
DIS
IS-IS DIS election, 138
IS-IS DIS election configuration, 179
IS-IS interface DIS priority, 153
disabling
IPv4 BGP session establishment disable, 278
IPv6 BGP session establishment disable, 278
IS-IS interface packet send/receive, 154
OSPF interface packet send/receive disable, 89
OSPFv3 interface packet send/receive, 434
RIP host route reception, 31
discard route (OSPF), 84
displaying
BGP, 303
IP routing table, 7
IPv4 BGP, 303, 303
IPv6 BGP, 303, 303
IPv6 IS-IS, 483
IPv6 PBR, 500
IPv6 static routing, 388
IS-IS, 173
MTR, 522
OSPF, 104
OSPFv3, 444
PBR, 378
RIP, 44
RIPng, 408
routing policy, 514
static routing, 14
distributing
BGP route distribution control, 237
IP routing extension attribute redistribution, 4
IP routing route redistribution, 3
IPv4 BGP+IGP route redistribution, 312
IS-IS route redistribution, 149
OSPF route redistribution configuration, 108
OSPFv3 route redistribution, 430, 455
RIPng received/redistributed route filtering, 400
RIPng route redistribution, 401, 411
domain
   IS-IS authentication (routing domain), 166
   IS-IS routing domain, 137
DR
   OSPF, 72
   OSPF DR election configuration, 117
   OSPFv3 DR election configuration, 452
   OSPFv3 interface DR priority, 434
DSCP
   OSPF packet DSCP value, 91
DSP (IS-IS area address), 136
dynamic
   BGP dynamic peer, 219
   IP routing dynamic routing protocols, 2
   IS-IS system ID > host name mapping, 161
E
EBGP
   BGP first AS number of route updates, 267
direct connections after link failure, 273
IPv4 BGP multiple hop EBGP session establishment, 272
IPv4 BGP private AS number removal from EBGP peer/peer group update, 266
IPv6 BGP multiple hop EBGP session establishment, 272
IPv6 BGP private AS number removal from EBGP peer/peer group update, 266
peer, 200
ter group configuration (IPv4 multicast address), 224
peer group configuration (IPv4 unicast address), 224
peer group configuration (IPv6 multicast address), 224
peer group configuration (IPv6 unicast address), 224
   IPv6 static route BFD echo mode (single hop), 387
   RIP BFD configuration (bidirectional control detection), 60
   RIP BFD configuration (single-hop echo detection/specific destination), 58
   RIP BFD single-hop echo detection, 41, 56
   static routing BFD single-hop echo mode, 11
ECMP, 275, See also load balancing
   IPv4 BGP load balancing, 275
   IPv6 BGP load balancing, 275
   ISIS ECMP routes max, 147
   OSPF ECMP routes max, 83
   OSPFv3 ECMP route max, 430
   RIP ECMP route max number, 35
   RIPng ECMP route max, 403
electing
   OSPF DR election configuration, 117
   OSPFv3 DR election configuration, 452
enabling
   BGP, 216
   BGP session state change logging, 295
   BGP SNMP notification, 295
   IP routing EBGP direct connections after link failure, 273
   IPv4 BGP 4-byte AS number suppression, 273
   IPv4 BGP MED AS route comparison (confederation peers), 259
   IPv4 BGP MED AS route comparison (diff ASs), 257
   IPv4 BGP MED AS route comparison (per-AS), 257
   IPv4 BGP multiple hop EBGP session establishment, 272
   IPv4 BGP peer MD5 authentication, 274
   IPv4 BGP route refresh, 280
   IPv6 BGP 4-byte AS number suppression, 273
   IPv6 BGP MED AS route comparison (confederation peers), 259
IPv6 BGP MED AS route comparison (diff ASs), 257
IPv6 BGP MED AS route comparison (per-AS), 257
IPv6 BGP multiple hop EBGP session establishment, 272
IPv6 BGP peer MD5 authentication, 274
IPv6 BGP route refresh, 280
IPv6 IS-IS automatic link cost calculation, 476
IPv6 IS-IS FRR BFD, 482
IPv6 IS-IS ISPF, 479
IPv6 IS-IS MTR, 482
IPv6 IS-IS prefix suppression, 479
IS-IS, 143
IS-IS automatic cost calculation, 146
IS-IS FRR BFD (control packet mode), 171
IS-IS FRR BFD (echo packet mode), 171
IS-IS interface hello packet send, 154
IS-IS ISPF, 162
IS-IS LSP flash flooding, 156
IS-IS LSP fragment extension, 156
IS-IS neighbor state change logging, 161
IS-IS PIC, 164
IS-IS PIC BFD, 164
IS-IS PPP interface hello packet source address check, 153
IS-IS prefix suppression, 162
OSPF (on interface), 76
OSPF (on network), 75
OSPF ISPF, 94
OSPF neighbor state change logging, 92
OSPF PIC, 96
OSPF RFC 1583 compatibility, 92
OSPFv3, 424
OSPFv3 neighbor state change logging, 435
RIP, 28
RIP FRR BFD, 43
RIP NSR, 40
RIP poison reverse, 34
RIP split horizon, 34
RIP update source IP address check, 35
RIPv1 incoming message zero field check, 35
RIPv2 automatic route summarization, 30
triggered RIP (TRIP), 37
enhancing
   IS-IS network security, 164
establishing
   IPv4 BGP multiple hop EBGP session establishment, 272
   IPv4 BGP session establishment disable, 278
   IPv6 BGP multiple hop EBGP session establishment, 272
   IPv6 BGP session establishment disable, 278
exit overflow interval (OSPF), 92
extending
   IS-IS LSP fragment extension, 156
   MP-BGP MP_REACH_NLRI extended attribute, 210
   MP-BGP MP_UNREACH_NLRI extended attribute, 210
Exterior Gateway Protocol. Use EGP external
   OSPF LSDB external LSAs max, 91
external BGP. Use EGP
F
fast reroute. Use FRR
FIB
   IP routing table, 1
filtering
   BGP configuration, 200, 213
   BGP route filtering policies, 244
   IPv4 BGP basic configuration, 308
   IPv4 BGP BFD configuration, 334
   IPv4 BGP COMMUNITY configuration, 321
   IPv4 BGP confederation, 326
   IPv4 BGP configuration, 308
   IPv4 BGP FRR configuration, 338
IPv4 BGP GR configuration, 333
IPv4 BGP load balancing configuration, 318
IPv4 BGP path selection configuration, 330
IPv4 BGP route distribution filtering policies, 244
IPv4 BGP route reception filtering policies, 247
IPv4 BGP route reflector configuration, 324
IPv4 BGP route summarization, 315
IPv4 BGP+IGP route redistribution, 312
IPv6 BGP basic configuration, 347
IPv6 BGP BFD configuration, 355
IPv6 BGP configuration, 347
IPv6 BGP FRR configuration, 364
IPv6 BGP route distribution filtering policies, 244
IPv6 BGP route reception filtering policies, 247
IS-IS LSP-calculated routes, 150
IS-IS redistributed routes, 150
IS-IS routes, 150
OSPF outbound LSA (interface), 97
OSPF outbound LSAs (specified neighbor), 97
OSPF received route filtering, 82
OSPF Type-3 LSA filtering, 82
OSPFv3 Inter-Area-Prefix LSA filtering, 429
OSPFv3 received route filtering, 428
RIP received/redistributed route filtering, 32
RIPng received/redistributed route filtering, 400
routing policy ACLs, 507
routing policy apply clause, 512
routing policy AS_PATH list, 507, 509
routing policy COMMUNITY list, 507, 509
routing policy configuration, 507, 510, 515
routing policy configuration (IPv4 route redistribution), 515
routing policy configuration (IPv6 route redistribution), 517
routing policy continue clause, 514
routing policy creation, 510
routing policy extended community list, 507, 510
routing policy filter configuration, 508
routing policy filters, 507
routing policy if-match clause, 511
routing policy IP prefix list, 508
routing policy MAC list, 507, 510
routing policy prefix list, 507
flooding
IS-IS LSP flash flooding, 156
IS-IS LSP flooding, 157
flushing
suboptimal BGP route, 286
format
IS-IS address format, 135
IS-IS NSAP address format, 135
forwarding
interface PBR configuration, 377
interface PBR configuration (packet length-based), 381
interface PBR configuration (packet source-IP-based), 383
interface PBR configuration (packet type-based), 380
IP routing inter-protocol FRR, 6
IP routing IPv4 RIB inter-protocol FRR, 7
IP routing IPv6 RIB inter-protocol FRR, 7
IP routing RIB NSR, 5
IPv4 RIB NSR configuration, 5
IPv6 IS-IS BFD configuration, 479, 488
IPv6 PBR configuration, 494, 497, 499, 500
IPv6 PBR interface configuration, 499
IPv6 PBR interface configuration (packet length-based), 503
IPv6 PBR interface configuration (packet type-based), 502
IPv6 PBR local configuration, 499
IPv6 PBR local configuration (packet type-based), 500
IPv6 PBR policy configuration, 497
IPv6 RIB NSR configuration, 6
local PBR configuration, 377
local PBR configuration (packet type-based), 378
OSPF GR, 98
OSPF GR helper, 99
OSPF GR restart, 99
OSPF NSR, 100
OSPF NSR configuration, 125
OSPFv3 BFD, 440
OSPFv3 NSR, 439
OSPFv3 NSR configuration, 463
PBR configuration, 372, 375, 377, 378
PBR policy configuration, 375
RIPng NSR, 405
RIPng NSR configuration, 414
fragment
IS-IS LSP fragment extension, 156
FRR
BFD enable, 43, 406
BGP FRR configuration, 297
IPv4 BGP FRR configuration, 338
IPv6 BGP FRR configuration, 364
IPv6 IS-IS FRR, 480
IPv6 IS-IS FRR automatic backup next hop
LFA calculation, 481
IPv6 IS-IS FRR BFD, 482
IPv6 IS-IS FRR configuration, 491
IPv6 IS-IS FRR using routing policy, 481
IS-IS FRR, 169
IS-IS FRR backup next hop configuration (LFA calculation), 169
IS-IS FRR BFD enable (control packet mode), 171
IS-IS FRR BFD enable (echo packet mode), 171
IS-IS FRR configuration, 197
IS-IS FRR configuration (routing policy), 170
OSPF backup next hop (routing policy), 103
OSPF backup next hop calculation (LFA algorithm), 103
OSPF FRR BFD, 103
OSPF FRR configuration, 102, 130
OSPFv3 backup next hop (routing policy), 442
OSPFv3 backup next hop calculation (LFA algorithm), 441
OSPFv3 FRR BFD, 442
OSPFv3 FRR configuration, 441, 467
RIP configuration, 42, 64, 406
RIPng configuration, 416
static routing FRR configuration, 12, 21

G

garbage-collect timer (RIP), 33
Generalized TTL Security Mechanism. See GTSM

generating

BGP route, 233
OSPFv3 LSA generation interval, 433
Graceful Restart (GR)

BGP configuration, 293
IPv4 BGP GR configuration, 333
IS-IS GR configuration, 166, 189
IS-IS GR helper, 166
IS-IS GR restart, 166
IS-IS NSR, 167
IS-IS NSR configuration, 190
OSPF configuration, 123
OSPF GR configuration, 98
OSPF GR helper configuration, 99
OSPF GR restart configuration, 99
OSPF NSR, 100
OSPF trigger, 100
OSPFv3 GR configuration, 438, 462
OSPFv3 GR helper configuration, 439

545
OSPFv3 GR restarter configuration, 438
OSPFv3 trigger, 439
RIP configuration, 39, 53
RIP GR helper configuration, 39
RIP GR restarter configuration, 39
RIPv2 configuration, 404, 413
group
BGP peer group, 222
GTSM
BGP configuration, 279
OSPF configuration, 97

H
hello
IS-IS hello multiplier, 152
IS-IS hello packet send interval, 152
IS-IS interface hello packet send, 154
IS-IS PDU type, 140
IS-IS PPP interface hello packet source address check, 153
OSPF hello packet, 67
OSPF hello packet timer, 86
OSPFv2 packet type, 422
HO-DSP (IS-IS area address), 136
hold time
IPv4 BGP, 269
IPv6 BGP, 269
hop
OSPF BFD detection configuration
(single-hop echo), 102
RIP BFD configuration (bidirectional control detection), 42
RIP BFD configuration (single-hop echo detection/neighbor), 41
RIP BFD configuration (single-hop echo detection/specific destination), 41
host
IS-IS system ID > host name mapping, 160
OSPF host route advertisement, 86
host route reception, 31

I
IBGP
BGP configuration, 292
IPv4 BGP ORIGINATOR_ID attribute, 291
IPv4 BGP route reflector, 289
IPv6 BGP ORIGINATOR_ID attribute, 291
IPv6 BGP route reflector, 289
peer, 200
peer group configuration (IPv4 multicast address), 222
peer group configuration (IPv4 unicast address), 222
peer group configuration (IPv6 multicast address), 222
peer group configuration (IPv6 unicast address), 222
ICMP
OSPF area configuration (NSSA), 115
OSPF area configuration (stub), 113
OSPF basics configuration, 105
OSPF BFD configuration, 127
OSPF configuration, 67, 73, 105
OSPF DR election configuration, 117
OSPF FRR configuration, 130
OSPF GR configuration, 123
OSPF route redistribution configuration, 108
OSPF route summarization configuration, 110
OSPF virtual link configuration, 121
OSPFv3 FRR configuration, 467
OSPFv3 route summarization, 458
ID
IS-IS system ID, 136
IDP (IS-IS area address), 136
IETF
OSPF GR, 98
OSPF GR helper, 99
OSPF GR restarter, 99
ignoring
BGP first AS number of EBGP route updates, 267
IPv4 BGP AS_PATH optimal route selection, 263
IPv4 BGP IGP metrics optimal route selection, 267
IPv4 BGP ORIGINATOR_ID attribute, 291
IPv6 BGP ORIGINATOR_ID attribute, 291
OSPFv3 DD packet MTU check, 434

IGP
BGP ORIGIN path attribute, 200
IPv4 BGP+IGP route redistribution, 312
IS-IS authentication configuration, 187
IS-IS basic configuration, 143
IS-IS basics configuration, 175
IS-IS configuration, 135, 142, 175
IS-IS DIS election configuration, 179
IS-IS route redistribution, 183
RIP BFD configuration (bidirectional control detection), 42
RIP BFD configuration (single-hop echo detection/neighbor), 41
RIP BFD configuration (single-hop echo detection/specific destination), 41
RIP configuration, 25, 27, 44
RIP neighbor specification, 37

IGP metrics
IPv4 BGP optimal route selection, 267

INCOMPLETE
BGP ORIGIN path attribute, 200

Incremental Shortest Path First. Use ISPF injecting
IPv4 BGP local network, 234
IPv6 BGP local network, 234

instance
BGP multi-instance, 211

inter-area
OSPF route type, 71

interface
interface PBR configuration (packet length-based), 381
interface PBR configuration (packet source-IP-based), 383
interface PBR configuration (packet type-based), 380
IPv6 PBR interface configuration, 499
IPv6 PBR interface configuration (packet length-based), 503
IPv6 PBR interface configuration (packet type-based), 502
PBR configuration, 377


Use IS-IS internal
  BGP. Use IBGP
  OSPF router type, 70

INTERNET
BGP COMMUNITY path attribute, 200

interval
BGP soft reset, 280
IPv4 BGP keepalive interval, 269
IPv4 BGP route update interval, 271
IPv6 BGP keepalive interval, 269
IPv6 BGP route update interval, 271
IPv6 IS-IS SPF calculation interval, 478
IS-IS CSNP packet send interval, 153
IS-IS hello multiplier, 152
IS-IS hello packet send interval, 152
IS-IS SPF calculation interval, 152
OSPF exit overflow interval, 92
OSPF LSA arrival interval, 88
OSPF LSA generation interval, 88
OSPF LSU transit rate, 94
OSPF SPF calculation interval, 88
OSPFv3 LSA generation interval, 433
OSPFv3 LSU transit rate, 436
OSPFv3 SPF calculation interval, 433
RIP triggered update interval, 36
RIPvng triggered update send interval, 403

intra-area
OSPF route type, 71
IP addressing
   RIP configuration, 25, 27, 44
   RIP update source IP address check, 35
IP performance optimization
   command and hardware compatibility, 374, 496
IP routing
   BGP 6PE basics, 301
   BGP 6PE optional capabilities, 302
   BGP AS_PATH attribute, 262
   BGP community, 207
   BGP confederation, 207, 292
   BGP confederation compatibility, 292
   BGP configuration, 200, 213
   BGP default route advertisement to peer/peer group, 241
   BGP display, 303
   BGP dynamic peer, 219
   BGP dynamic peer (IPv4 multicast address), 221
   BGP dynamic peer (IPv4 unicast address), 220
   BGP dynamic peer (IPv6 multicast address), 221
   BGP dynamic peer (IPv6 unicast address), 220
   BGP first AS number of EBGP route updates, 267
   BGP FRR, 297
   BGP GR, 293
   BGP GR helper, 293
   BGP GR restarter, 293
   BGP GTSM configuration, 279
   BGP large scale network management, 207
   BGP large-scale network, 287
   BGP load balancing, 206
   BGP maintain, 303
   BGP MED attribute, 256
BGP MPLS local label update delay, 286
BGP multi-instance, 211
BGP network optimization, 269
BGP NSR, 294
BGP optimal route advertisement, 240
BGP path selection, 251
BGP peer, 217
BGP peer (IPv4 multicast address), 219
BGP peer (IPv4 unicast address), 217
BGP peer (IPv6 multicast address), 219
BGP peer (IPv6 unicast address), 218
BGP peer group, 207, 222
BGP policy accounting, 300
BGP protocols and standards, 213
BGP route dampening, 207
BGP route distribution, 237
BGP route filtering policies, 244
BGP route generation, 233
BGP route reception, 237
BGP route recursion, 206
BGP route reflection, 289
BGP route selection, 205, 206
BGP route summarization, 207, 237
BGP session state change logging, 295
BGP SNMP notification enable, 295
BGP soft reset, 280
BGP TCP connection source address, 232
configuration, 1
displaying IPv6 static routing, 388
displaying routing table, 7
displaying static routes, 14
dynamic routing protocols, 2
EBGP peer group (IPv4 multicast address), 224
EBGP peer group (IPv4 unicast address), 224
EBGP peer group (IPv6 multicast address), 224
EBGP peer group (IPv6 unicast address), 224
extension attribute redistribution, 4
FIB route max lifetime, 4
IBGP peer group (IPv4 multicast address), 222
IBGP peer group (IPv4 unicast address), 222
IBGP peer group (IPv6 multicast address), 222
IBGP peer group (IPv6 unicast address), 222
interface PBR configuration, 377
inter-protocol FRR configuration, 6
IPv4, 234, See also IPv4
IPv4 BGP SoO attribute, 268
IPv4 RIB inter-protocol FRR configuration, 7
IPv6, 234, See also IPv6
IPv6 BGP IPsec, 277
IPv6 BGP SoO attribute, 268
IPv6 default route. See under IPv6 static routing
IPv6 IS-IS, 474, See also IPv6 IS-IS
IPv6 IS-IS display, 483
IPv6 IS-IS FRR, 480
IPv6 IS-IS FRR configuration, 491
IPv6 policy-based routing. See IPv6 PBR
IPv6 RIB inter-protocol FRR configuration, 7
IPv6 static routing. See IPv6 static routing
IS-IS ATT bit, 159
IS-IS authentication (area), 165
IS-IS authentication (neighbor relationship), 165
IS-IS authentication (routing domain), 166
IS-IS authentication configuration, 187
IS-IS automatic cost calculation, 146
IS-IS basic configuration, 143
IS-IS basics configuration, 175
IS-IS BFD, 168
IS-IS BFD configuration, 194
IS-IS configuration, 135, 142, 175
IS-IS CSNP packet send interval, 153
IS-IS default route advertisement, 148
IS-IS DIS election configuration, 179
IS-IS display, 173
IS-IS ECMP routes max, 147
IS-IS FRR, 169
IS-IS FRR configuration, 197
IS-IS global cost, 145
IS-IS GR, 166
IS-IS GR configuration, 189
IS-IS hello multiplier, 152
IS-IS hello packet send interval, 152
IS-IS interface cost, 145
IS-IS interface DIS priority, 153
IS-IS interface hello packet send, 154
IS-IS interface packet send/receive, 154
IS-IS interface tag value, 160
IS-IS ISPF, 162
IS-IS link cost, 144
IS-IS LSDB overload bit, 159
IS-IS LSP flash flooding, 156
IS-IS LSP flooding, 157
IS-IS LSP fragment extension, 156
IS-IS LSP length, 155
IS-IS LSP parameters, 154
IS-IS LSP timer, 154
IS-IS LSP-calculated route filtering, 150
IS-IS maintain, 173
IS-IS MTR, 172
IS-IS network management, 163
IS-IS network optimization, 152
IS-IS network security enhancement, 164
IS-IS network tuning, 152
IS-IS NSR, 167
IS-IS NSR configuration, 190
IS-IS PDU CLVs, 140
IS-IS PDU hello type, 140
IS-IS PDU LSP type, 140
IS-IS PDU SNP type, 140
IS-IS PDU types, 139
IS-IS PIC BF D, 164
IS-IS PIC configuration, 163
IS-IS preference, 146
IS-IS prefix suppression, 162
IS-IS protocols and standards, 141
IS-IS redistributed route filtering, 150
IS-IS route control, 144
IS-IS route convergence priority, 158
IS-IS route filtering, 150
IS-IS route leaking, 138, 151
IS-IS route redistribution, 149, 183
IS-IS route summarization, 148
IS-IS routing domain, 137
IS-IS SPF calculation interval, 157
IS-IS system ID > host name mapping, 160
load sharing, 3
local PBR configuration, 377
maintaining routing table, 7
MP-BGP, 210
MP-BGP protocols and standards, 213
MTR configuration, 520, 520
MTR display, 522
OSPF area, 76
OSPF area configuration (NSSA), 77, 115
OSPF area configuration (stub), 77, 113
OSPF authentication, 90
OSPF basics configuration, 105
OSPF BDR, 72
OSPF BFD, 101, 101
OSPF BFD configuration, 127
OSPF BFD detection configuration (bidirectional control), 101
OSPF BFD detection configuration (single-hop echo), 102
OSPF configuration, 67, 73, 105
OSPF DD packet interface MTU, 91
OSPF display, 104
OSPF DR, 72
OSPF DR election configuration, 117
OSPF ECMP routes max, 83
OSPF exit overflow interval, 92
OSPF FRR, 102
OSPF FRR BFD, 103
OSPF FRR configuration, 130
OSPF GR, 98
OSPF GR configuration, 123
OSPF GR helper, 99
OSPF GR restarter, 99
OSPF GTSM configuration, 97
OSPF host route advertisement, 86
OSPF interface cost, 83
OSPF interface network type (broadcast), 79
OSPF interface network type (NBMA), 79
OSPF interface network type (P2MP), 80
OSPF interface network type (P2P), 80
OSPF interface packet send/receive disable, 89
OSPF ISPF, 94
OSPF log count, 96
OSPF LSA arrival interval, 88
OSPF LSA generation interval, 88
OSPF LSA transmission delay, 87
OSPF LSDB external LSAs max, 91
OSPF LSU transmit rate, 94
OSPF maintain, 104
OSPF neighbor state change, 92
OSPF network management, 93
OSPF network optimization, 86
OSPF network tuning, 86
OSPF network type, 78
OSPF NSR, 100
OSPF NSR configuration, 125
OSPF outbound LSA filtering (interface), 97
OSPF outbound LSA filtering (specified neighbor), 97
OSPF packet DSCP value, 91
OSPF PIC configuration, 95
OSPF preference, 84
OSPF prefix priority, 95
OSPF prefix suppression, 94
OSPF protocols and standards, 73
OSPF received route filtering, 82
OSPF RFC 1583 compatibility, 92
OSPF route control, 81
OSPF route redistribution, 84
OSPF route redistribution configuration, 108
OSPF route summarization, 81
OSPF route summarization configuration, 110
OSPF SPF calculation interval, 88
OSPF stub router, 89
OSPF summary network discard route, 84
OSPF timer set, 86
OSPF Type-3 LSA filtering, 82
OSPF virtual link, 78
OSPF virtual link configuration, 121
OSPFv3 area parameter, 425
OSPFv3 BFD, 440
OSPFv3 BFD configuration, 464
OSPFv3 configuration, 422, 423, 445
OSPFv3 DD packet ignore MTU check, 434
OSPFv3 display, 444
OSPFv3 DR election configuration, 452
OSPFv3 ECMP route max, 430
OSPFv3 enable, 424
OSPFv3 FRR, 441
OSPFv3 FRR BFD, 442
OSPFv3 FRR configuration, 467
OSPFv3 GR, 438
OSPFv3 GR configuration, 462
OSPFv3 GR helper, 439
OSPFv3 GR restart, 438
OSPFv3 Inter-Area-Prefix LSA filtering, 429
OSPFv3 interface cost, 429
OSPFv3 interface DR priority, 434
OSPFv3 interface packet send/receive disable, 434
OSPFv3 IPsec profile application, 443
OSPFv3 IPsec profile configuration, 469
OSPFv3 LSA generation interval, 433
OSPFv3 LSA transmission delay, 432
OSPFv3 LSU transmit rate, 436
OSPFv3 maintain, 444
OSPFv3 NBMA neighbor, 427
OSPFv3 neighbor state change logging, 435
OSPFv3 network management traps, 435
OSPFv3 network optimization, 432
OSPFv3 network tuning, 432
OSPFv3 network type, 426
OSPFv3 network type (interface), 427
OSPFv3 NSR, 439
OSPFv3 NSR configuration, 463
OSPFv3 NSSA area, 425
OSPFv3 NSSA area configuration, 450
OSPFv3 P2MP neighbor, 427
OSPFv3 preference, 430
OSPFv3 prefix suppression, 437
OSPFv3 protocols and standards, 423
OSPFv3 received route filtering, 428
OSPFv3 route control, 427
OSPFv3 route redistribution, 430, 455
OSPFv3 route summarization, 428, 458
OSPFv3 SPF calculation interval, 433
OSPFv3 stub area, 425
OSPFv3 stub area configuration, 445
OSPFv3 stub router, 436
OSPFv3 timer, 432
OSPFv3 virtual link, 426
PBR configuration, 375, 377, 378
PBR display, 378
PBR maintain, 378
PBR node action, 375
PBR node creation, 375
PBR node match criteria, 375
PBR policy, 372
PBR policy configuration, 375
PBR+Track collaboration, 374
policy apply clause, 512
policy AS_PATH list, 509
policy COMMUNITY list, 509
policy configuration, 507, 510, 515
policy configuration (IPv4 route redistribution), 515
RIP network optimization, 33
RIP network tuning, 33
RIP NSR configuration, 54
RIP NSR enable, 40
RIP operation, 25
RIP packet max length, 39
RIP packet send rate configuration, 38
RIP poison reverse configuration, 34
RIP preference configuration, 32
RIP received/redistributed route filtering, 32
RIP route control configuration, 30
RIP route entries, 25
RIP route redistribution configuration, 33, 47
RIP routing loop prevention, 25
RIP split horizon configuration, 34
RIP summary route advertisement configuration, 51
RIP timer configuration, 33
RIP triggered update interval configuration, 36
RIP update source IP address check, 35
RIP version configuration, 29
RIP versions, 26
RIPng basic configuration, 398, 408
RIPng configuration, 397, 398, 408
RIPng default route advertisement, 400
RIPng display, 408
RIPng ECMP route max, 403
RIPng FRR configuration, 406, 416
RIPng GR configuration, 404, 413
RIPng IPsec profile application, 407
RIPng IPsec profile configuration, 419
RIPng maintain, 408
RIPng network optimization, 401
RIPng network tuning, 401
RIPng NSR, 405
RIPng NSR configuration, 414
RIPng packet, 397
RIPng packet send rate, 403
RIPng packet zero field check configuration, 402

policy configuration (IPv6 route redistribution), 517
policy continue clause, 514
policy creation, 510
policy display, 514
policy extended community list, 510
policy filter configuration, 508
policy filtering, 508
policy filters, 507
policy if-match clause, 511
policy IP prefix list, 508
policy MAC list, 510
policy maintain, 514
policy-based routing. See PBR
RIB label max lifetime, 4
RIB NSR configuration, 5
RIB route max lifetime, 4
RIP additional routing metric configuration, 30
RIP basic configuration, 27, 44
RIP BFD configuration, 41
RIP BFD configuration (bidirectional control detection), 42, 60
RIP BFD configuration (single-hop echo detection/neighbor), 41
RIP BFD configuration (single-hop echo detection/specific destination), 41, 58
RIP BFD single-hop echo detection, 56
RIP configuration, 25, 27, 44
RIP default route advertisement, 31
RIP ECMP route max number, 35
RIP FRR configuration, 42, 64
RIP GR configuration, 39, 53
RIP host route reception disable, 31
RIP interface additional metric configuration, 49
RIP interface advertisement control, 28
RIP interface reception control, 28
RIP neighbor specification, 37
RIP network management configuration, 38
RIPng poison reverse configuration, 402
RIPng preference, 400
RIPng protocols and standards, 398
RIPng received/redistributed route filtering, 400
RIPng route control, 399
RIPng route entry, 397
RIPng route redistribution, 401, 411
RIPng route summarization, 399
RIPng routing metric configuration, 399
RIPng split horizon configuration, 402
RIPng timer configuration, 401
RIPng triggered update send interval, 403
RIPv1 message zero field check, 35
RIPv2 message authentication configuration, 36
RIPv2 route summarization configuration, 30
route backup, 3
route preference, 2
route recursion, 3
route redistribution, 3
routing table, 1
static routing basic configuration, 14
static routing BFD bidirectional control mode (direct next hop), 10
static routing BFD bidirectional control mode (indirect next hop), 10
static routing BFD configuration, 10
static routing BFD configuration (direct next hop), 16
static routing BFD configuration (indirect next hop), 18
static routing BFD single-hop echo mode, 11
static routing configuration, 9, 9, 14
static routing default route configuration, 24
static routing DR configuration, 12, 21
triggered RIP (TRIP), 26
triggered RIP (TRIP) configuration, 37
troubleshooting BGP, 371
troubleshooting OSPF configuration, 133
troubleshooting OSPF incorrect routing information, 133
troubleshooting OSPF no neighbor relationship established, 133
IPsec
IPv6 BGP packet IPsec configuration, 359
OSPFv3 IPsec profile application, 443
OSPFv3 IPsec profile configuration, 469
RIPng IPsec profile application, 407
RIPng IPsec profile configuration, 419
IPv4
IP routing FIB route max lifetime, 4
IP routing RIB label max lifetime, 4
IP routing RIB route max lifetime, 4
IPv6 BGP 6PE configuration, 352
IS-IS authentication configuration, 187
IS-IS basic configuration, 143
IS-IS basics configuration, 175
IS-IS configuration, 135, 175
IS-IS DIS election configuration, 179
IS-IS route redistribution, 183
MTR configuration, 520, 520
OSPF area configuration (NSSA), 115
OSPF area configuration (stub), 113
OSPF basics configuration, 105
OSPF BFD configuration, 127
OSPF configuration, 67, 73, 105
OSPF DR election configuration, 117
OSPF FRR configuration, 130
OSPF GR configuration, 123
OSPF route redistribution configuration, 108
OSPF route summarization configuration, 110
OSPF virtual link configuration, 121
OSPFv3 FRR configuration, 467
RIB NSR, 5
routing policy ACLs, 507
routing policy configuration, 507, 515
routing policy configuration (IPv4 route redistribution), 515
routing policy IP prefix list, 508
routing policy prefix list, 507

IPv4 BGP
4-byte AS number suppression, 273
6PE, 301
6PE optional capabilities, 302
AS number substitution, 264
AS_PATH optimal route selection, 263
basic configuration, 308
BFD configuration, 296, 334
BGP route update delay, 250
BGP+IGP route redistribution, 312
COMMUNITY configuration, 287
COMMUNITY configuration configuration, 321
confederation configuration, 326
configuration, 308
default local preference, 254
default route advertisement to peer/peer group, 241
display, 303, 303
dynamic peer configuration, 345
fake AS number advertisement, 263
FRR configuration, 338
GR configuration, 333
hold time, 269
IGP metrics optimal route selection, 267
IGP route redistribution, 235
information clearance, 307
keepalive interval, 269
load balancing, 275
load balancing configuration, 318
local AS number appearance, 262
local network injection, 234
maintain, 303
manual soft reset configuration, 283
MED AS route comparison (confederation peers), 259
MED AS route comparison (diff ASs), 257
MED AS route comparison (per-AS), 257
MED default value, 256
multicast BGP configuration, 341, 367
multiple hop EBGP session establishment, 272
NEXT_HOP attribute, 259
ORIGINATOR_ID attribute, 291
path selection configuration, 330
peer MD5 authentication, 274
private AS number removal, 266
received route preferred value, 251
route dampening, 250
route distribution filtering policies, 244
route preference configuration, 253
route reception filtering policies, 247
route reflector, 289
route reflector configuration, 324
route refresh, 280
route summarization, 315
route summarization (automatic), 237
route summarization (manual), 238
route update interval, 271
route update save, 282
routes received from peer/peer group, 242
session establishment disable, 278
session reset, 307

IPv4 EBGP
peer protection (low memory exemption), 285

IPv6
IP routing FIB route max lifetime, 4
IP routing RIB label max lifetime, 4
IP routing RIB route max lifetime, 4
IS-IS. See IPv6 IS-IS
MTR configuration, 520, 520
OSPFv3 area parameter, 425
OSPFv3 BFD, 440
OSPFv3 BFD configuration, 464
OSPFv3 configuration, 422, 423, 445
OSPFv3 DD packet ignore MTU check, 434
OSPFv3 DR election configuration, 452
OSPFv3 ECMP route max, 430
OSPFv3 GR, 438
OSPFv3 GR configuration, 462
OSPFv3 GR helper, 439
OSPFv3 GR rearter, 438
OSPFv3 Inter-Area-Prefix LSA filtering, 429
OSPFv3 interface cost, 429
OSPFv3 interface DR priority, 434
OSPFv3 interface packet send/receive disable, 434
OSPFv3 IPsec profile application, 443
OSPFv3 IPsec profile configuration, 469
OSPFv3 LSA generation interval, 433
OSPFv3 LSA transmission delay, 432
OSPFv3 NBMA neighbor, 427
OSPFv3 neighbor state change logging, 435
OSPFv3 network optimization, 432
OSPFv3 network tuning, 432
OSPFv3 network type, 426
OSPFv3 network type (interface), 427
OSPFv3 NSSA area, 425
OSPFv3 NSSA area configuration, 450
OSPFv3 P2MP neighbor, 427
OSPFv3 preference, 430
OSPFv3 received route filtering, 428
OSPFv3 route control, 427
OSPFv3 route redistribution, 430, 455
OSPFv3 route summarization, 428, 458
OSPFv3 SPF calculation interval, 433
OSPFv3 stub area, 425
OSPFv3 stub area configuration, 445
OSPFv3 timer, 432
OSPFv3 virtual link, 426
policy-based routing. See IPv6 PBR
provider edge. See 6PE
RIB NSR, 6
RIP, 397, See also RIPng
RIPng GR configuration, 413

routing policy ACLs, 507
routing policy configuration, 507, 515
routing policy configuration (IPv6 route redistribution), 517
routing policy IP prefix list, 508
routing policy prefix list, 507

IPv6 BGP
4-byte AS number suppression, 273
6PE configuration, 352
AS number substitution, 264
basic configuration, 347
BFD configuration, 296
BFD configuration configuration, 355
COMMUNITY configuration, 287
configuration, 347
default local preference, 254
default route advertisement to peer/peer group, 241
display, 303, 303
fake AS number advertisement, 263
FRR configuration, 364
hold time, 269
IGP route redistribution, 235
information clearance, 307
IPsec configuration, 277
keepalive interval, 269
local AS number appearance, 262
local network injection, 234
maintain, 303
manual soft reset, 283
MED AS route comparison (confederation peers), 259
MED AS route comparison (diff ASs), 257
MED AS route comparison (per-AS), 257
MED default value, 256
multiple hop EBGP session establishment, 272
NEXT_HOP attribute, 259
ORIGINATOR_ID attribute, 291

IPv6 BGP
4-byte AS number suppression, 273
6PE configuration, 352
AS number substitution, 264
basic configuration, 347
BFD configuration, 296
BFD configuration configuration, 355
COMMUNITY configuration, 287
configuration, 347
default local preference, 254
default route advertisement to peer/peer group, 241
display, 303, 303
fake AS number advertisement, 263
FRR configuration, 364
hold time, 269
IGP route redistribution, 235
information clearance, 307
IPsec configuration, 277
keepalive interval, 269
local AS number appearance, 262
local network injection, 234
maintain, 303
manual soft reset, 283
MED AS route comparison (confederation peers), 259
MED AS route comparison (diff ASs), 257
MED AS route comparison (per-AS), 257
MED default value, 256
multiple hop EBGP session establishment, 272
NEXT_HOP attribute, 259
ORIGINATOR_ID attribute, 291
packet IPsec configuration, 359
peer MD5 authentication, 274
private AS number removal, 266
received route preferred value, 251
route dampening, 250
route distribution filtering policies, 244
route preference, 253
route reception filtering policies, 247
route reflector, 289
route reflector configuration, 350
route refresh, 280
route summarization (manual), 238
route update interval, 271
route update save, 282
routes received from peer/peer group, 242
session establishment disable, 278
session reset, 307
IPv6 EBGP
peer protection (low memory exemption), 285
IPv6 IS-IS
basic configuration, 474, 484
BFD configuration, 479, 488
configuration, 474, 484
display, 483
FRR automatic backup next hop LFA calculation, 481
FRR BFD enabling, 482
FRR configuration, 480, 491
FRR using routing policy, 481
global cost configuration, 476
interface cost configuration, 476
interface tag value configuration, 478
ISPF enable, 479
link cost configuration, 476
LSDB overload bit, 478
MTR enable, 482
network optimization, 477
network tuning, 477
prefix suppression, 479
route control configuration, 475
route convergence priority assignment, 477
SPF calculation interval, 478
IPv6 PBR
apply clause, 494
configuration, 494, 497, 499, 500
display, 500
if-match clause, 494
interface configuration, 499
interface configuration (packet length-based), 503
interface configuration (packet type-based), 502
interface PBR, 494
local configuration, 499
local configuration (packet type-based), 500
local PBR, 494
maintain, 500
match mode/node clause relationship, 495
node action, 497
node creation, 497
node match criteria, 497
policy, 494
policy configuration, 497
Track collaboration, 496
IPv6 static routing
basic configuration, 388
BFD configuration, 386
BFD configuration (direct next hop), 390
BFD configuration (indirect next hop), 393
BFD control mode (direct next hop), 387
BFD control mode (indirect next hop), 387
BFD echo mode (single hop), 387
configuration, 386, 388
default route configuration, 396
displaying, 388
route configuration, 386
IS-IS
address format, 135
area, 137
area address, 136
ATT bit, 159
ATT bit default route calculation, 159
ATT bit Level-1 LSP, 160
authentication (area), 165
authentication (neighbor relationship), 165
authentication (routing domain), 166
authentication configuration, 187
basic configuration, 143, 175
BFD configuration, 168, 194
broadcast network type, 138
configuration, 135, 142, 175
CSNP packet send interval, 153
default route advertisement, 148
DIS election, 138, 179
display, 173
ECMP routes max, 147
enable, 143
enabling automatic cost calculation, 146
FRR backup next hop configuration (LFA calculation), 169
FRR BFD enable (control packet mode), 171
FRR BFD enable (echo packet mode), 171
FRR configuration, 169, 177
FRR configuration (routing policy), 170
global cost configuration, 145
GR configuration, 166, 189
hello multiplier, 152
hello packet send interval, 152
interface cost configuration, 145
interface DIS priority, 153
interface hello packet send enable, 154
interface P2P network type configuration, 144
interface packet send/receive disable, 154
interface tag value, 160
IPv6 IS-IS. See IPv6 IS-IS
IS+circuit level set, 143
ISPF enable, 162
Level-1 router, 137
Level-1-2 router, 137
Level-2 router, 137
link cost configuration, 144
LSDB overload bit, 159
LSP flash flooding, 156
LSP flooding, 157
LSP fragment extension, 156
LSP length specification, 155
LSP parameter configuration, 154
LSP timer configuration, 154
LSP-calculated route filtering, 150
maintain, 173
MTR configuration, 172
neighbor state change logging, 161
NET, 136
network management, 163
network optimization, 152
network security enhancement, 164
network tuning, 152
nonstop routing (NSR) configuration, 167, 190
NSAP address format, 135
N-SEL, 136
PDU CLVs, 140
PDU hello type, 140
PDU LSP type, 140
PDU SNP type, 140
PDU types, 139
PIC BFD enabling, 164
PIC configuration, 163
point-to-point network type, 138
PPP interface hello packet source address check, 153
preference specification, 146
prefix suppression enable, 162
protocols and standards, 141
pseudonode, 138
redistributed route filtering, 150
route control configuration, 144
route convergence priority, 158
route filtering, 150
route leaking, 138
route leaking configuration, 151
route redistribution, 149, 183
route summarization, 148
routing method, 136
SPF calculation interval, 157
system ID, 136
system ID > host name mapping, 160
terminology, 135

ISPF
IPv6 IS-IS enable, 479
OSPF ISPF, 94

K
keepalive
IPv4 BGP keepalive interval, 269
IPv4 BGP route update interval, 271
IPv6 BGP keepalive interval, 269
IPv6 BGP route update interval, 271

L
label
BGP MPLS local label update delay, 286
IP routing RIB label max lifetime, 4
leaking
IS-IS routes, 151
level
IPv4 EBGP peer protection (level 2 threshold exemption), 285
IPv6 EBGP peer protection (level 2 threshold exemption), 285
Level-1
IS-IS ATT bit Level-1 LSP, 160
limiting
IPv4 BGP routes received from peer/peer group, 242
IPv6 BGP routes received from peer/peer group, 242
IS-IS LSP flooding, 157
list
routing policy AS_PATH list, 507, 509
routing policy COMMUNITY list, 507, 509
routinig policy extended community list, 507, 510
routing policy IP prefix list, 508
routing policy MAC list, 507, 510
routiing policy prefix list, 507
load balancing, 206, See also ECMP
BGP, 206
IP routing RIB NSR, 5
IPv4 BGP, 275
IPv4 BGP load balancing configuration, 318
IPv6 BGP, 275
OSPF ECMP routes max, 83
OSPFv3 ECMP route max, 430
RIPv3 ECMP route max, 403
load sharing
IP routing load sharing, 3
IS-IS ECMP routes max, 147
RIP ECMP route max number, 35
local
BGP LOCAL_PREF path attribute, 200
IPv4 BGP default local preference, 254
IPv6 BGP default local preference, 254
IPv6 PBR local configuration, 499
IPv6 PBR local configuration (packet type-based), 500
local PBR configuration (packet type-based), 378
PBR configuration, 377
logging
BGP session state change logging, 295
IS-IS neighbor state change, 161
OSPF log count, 96
OSPF neighbor state change, 92
OSPFv3 neighbor state change logging, 435
loop
BGP FRR, 297
RIP routing loop prevention, 25
LSA
OSPF AS External LSA, 67
OSPF ASBR summary LSA, 67
OSPF exit overflow interval, 92
OSPF LSA arrival interval, 88
OSPF LSA generation interval, 88
OSPF LSA retransmission packet timer, 86
OSPF LSA transmission delay, 87
OSPF LSDB external LSAs max, 91
OSPF network LSA, 67
OSPF network summary LSA, 67
OSPF NSSA LSA, 67
OSPF opaque LSA, 67
OSPF outbound LSA filtering (specified neighbor), 97
OSPF router LSA, 67
OSPF Type-3 LSA filtering, 82
OSPFv3 AS external LSA, 422
OSPFv3 grace LSA, 422
OSPFv3 inter-area-prefix LSA, 422
OSPFv3 Inter-Area-Prefix LSA filtering, 429
OSPFv3 inter-area-router LSA, 422
OSPFv3 intra-area-prefix LSA, 422
OSPFv3 link LSA, 422
OSPFv3 LSA generation interval, 433
OSPFv3 LSA transmission delay, 432
OSPFv3 network LSA, 422
OSPFv3 NSSA LSA, 422
OSPFv3 router LSA, 422
LSAck
OSPF LSAck packet, 67
OSPFv3 packet type, 422
LSDB
IPv6 IS-IS LSDB overload bit, 478
IS-IS LSDB overload bit, 159
OSPF LSDB external LSAs max, 91
LSP
IS-IS ATT bit Level-1 LSP, 160
IS-IS LSP flash flooding, 156
IS-IS LSP flooding, 157
IS-IS LSP fragment extension, 156
IS-IS LSP length, 155
IS-IS LSP parameters, 154
IS-IS LSP timers, 154
IS-IS PDU type, 140
IS-IS route summarization, 148
LSR
OSPF LSR packet, 67
OSPFv3 packet type, 422
LSU
OSPF LSU packet, 67
OSPF LSU transmit rate, 94
OSPFv3 LSU transmit rate, 436
OSPFv3 packet type, 422
M
MAC addressing
routing policy MAC list, 507, 510
maintaining
BGP, 303
IP routing table, 7
IPv4 BGP, 303
IPv6 BGP, 303
IPv6 PBR, 500
IS-IS, 173
OSPF, 104
OSPFv3, 444
PBR, 378
RIP, 44
RIPng, 408
routing policy, 514
managing
BGP large scale network management, 207
manual
IPv4 BGP route summarization (manual), 238
IPv6 BGP route summarization (manual), 238
mapping
IS-IS system ID > host name mapping, 160
IS-IS system ID > host name mapping (dynamic), 161
IS-IS system ID > host name mapping (static), 160
matching
IPv6 PBR if-match clause, 494
IPv6 PBR node match criteria, 497
PBR deny match mode, 372
PBR if-match clause, 372
PBR node match criteria, 375
PBR permit match mode, 372
routing policy if-match clause, 508, 511
MD5
IPv4 BGP peer MD5 authentication, 274
IPv6 BGP peer MD5 authentication, 274
MED
BGP MED attribute, 256
BGP path attribute, 200
IPv4 BGP MED AS route comparison (confederation peers), 259
IPv4 BGP MED AS route comparison (diff ASs), 257
IPv4 BGP MED AS route comparison (per-AS), 257
IPv4 BGP MED default value, 256
IPv6 BGP MED AS route comparison (confederation peers), 259
IPv6 BGP MED AS route comparison (diff ASs), 257
IPv6 BGP MED AS route comparison (per-AS), 257
IPv6 BGP MED default value, 256
memory
IPv4 EBGP peer protection (low memory exemption), 285
IPv6 EBGP peer protection (low memory exemption), 285
message
BGP notification, 200
BGP open, 200
BGP route-refresh, 200
BGP update, 200
RIPv1 message zero field check enable, 35
RIPv2 message authentication configuration, 36
metric
RIP additional routing metric configuration, 30
RIP interface additional metric configuration, 49
RIPng routing metric configuration, 399
MIB
OSPF network management, 93
mode
IPv6 static route BFD control (direct next hop), 387
IPv6 static route BFD control (indirect next hop), 387
IPv6 static route BFD echo (single hop), 387
PBR deny match, 372
PBR permit match, 372
static routing BFD bidirectional control mode (direct next hop), 10
static routing BFD bidirectional control mode (indirect next hop), 10
static routing BFD single-hop echo mode, 11
MP_REACH_NLRI (MP-BGP), 210
MP_UNREACH_NLRI (MP-BGP), 210
MP-BGP, 200, See also BGP
  address family, 211
  BGP configuration, 200, 213
  extended attributes, 210
  IPv4 BGP basic configuration, 308
  IPv4 BGP BFD configuration, 334
  IPv4 BGP COMMUNITY configuration, 321
  IPv4 BGP confederation, 326
  IPv4 BGP configuration, 308
  IPv4 BGP FRR configuration, 338
  IPv4 BGP GR configuration, 333
  IPv4 BGP load balancing configuration, 318
  IPv4 BGP path selection configuration, 330
  IPv4 BGP route reflector configuration, 324
  IPv4 BGP route summarization, 315
  IPv4 BGP+IGP route redistribution, 312
  IPv6 BGP basic configuration, 347
  IPv6 BGP BFD configuration, 355
  IPv6 BGP configuration, 347
  IPv6 BGP FRR configuration, 364
  IPv6 BGP route reflector configuration, 350
  overview, 210
  protocols and standards, 213
MPLS
  BGP 6PE, 301
  BGP 6PE basics, 301
  BGP 6PE optional capabilities, 302
  IPv6 BGP 6PE configuration, 352
  routing policy extended community list, 507
MPU
  OSPF NSR, 100
  OSPFv3 NSR, 439
  OSPFv3 NSR configuration, 463
MTR
  configuration, 520, 520
display, 522
feature support, 520
how it works, 520
IPv6 IS-IS MTR enable, 482
IS-IS configuration, 172
MTU
  OSPF DD packet interface MTU, 91
  OSPFv3 DD packet ignore MTU check, 434
multicast
  BGP dynamic peer, 219
  BGP peer, 217
  OSPF network type, 72
  RIPng basic configuration, 398
  RIPng configuration, 397, 398
multicast BGP
  IPv4 BGP configuration, 341, 367
  IPv4 BGP dynamic peer configuration, 345
Multiprotocol Extensions for BGP-4. See MP-BGP
Multi-Topology Routing. Use MTR
N
naming
  IS-IS system ID > host name mapping, 160
NBMA
  OSPF interface network type, 79
  OSPF network type, 72, 78
  OSPFv3 NBMA neighbor, 427
  OSPFv3 network type, 426
  OSPFv3 network type (interface), 427
ND
  OSPFv3 BFD configuration, 464
  OSPFv3 configuration, 422, 423, 445
  OSPFv3 DR election configuration, 452
  OSPFv3 GR configuration, 462
  OSPFv3 IPsec profile configuration, 469
  OSPFv3 NBMA neighbor, 427
  OSPFv3 neighbor state change logging, 435
  OSPFv3 NSSA area configuration, 450

561
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPFv3 P2MP neighbor</td>
<td>427</td>
</tr>
<tr>
<td>OSPFv3 route control</td>
<td>427</td>
</tr>
<tr>
<td>OSPFv3 route redistribution</td>
<td>455</td>
</tr>
<tr>
<td>OSPFv3 stub area configuration</td>
<td>445</td>
</tr>
<tr>
<td>IPv4 BGP BFD</td>
<td>296</td>
</tr>
<tr>
<td>IPv6 BGP BFD</td>
<td>296</td>
</tr>
<tr>
<td>IS-IS authentication (neighbor relationship)</td>
<td>165</td>
</tr>
<tr>
<td>IS-IS neighbor state change logging</td>
<td>161</td>
</tr>
<tr>
<td>OSPF neighbor state change logging</td>
<td>92</td>
</tr>
<tr>
<td>OSPF outbound LSAs (specified neighbor)</td>
<td>97</td>
</tr>
<tr>
<td>RIP neighbor specification</td>
<td>37</td>
</tr>
<tr>
<td>IS-IS</td>
<td>136</td>
</tr>
<tr>
<td>network</td>
<td></td>
</tr>
<tr>
<td>BGP 6PE</td>
<td>301</td>
</tr>
<tr>
<td>BGP 6PE basics</td>
<td>301</td>
</tr>
<tr>
<td>BGP 6PE optional capabilities</td>
<td>302</td>
</tr>
<tr>
<td>BGP AS_PATH attribute</td>
<td>262</td>
</tr>
<tr>
<td>BGP basic configuration</td>
<td>216</td>
</tr>
<tr>
<td>BGP community</td>
<td>207</td>
</tr>
<tr>
<td>BGP confederation</td>
<td>207</td>
</tr>
<tr>
<td>BGP route reflection</td>
<td>289</td>
</tr>
<tr>
<td>BGP route reflector</td>
<td>207</td>
</tr>
<tr>
<td>BGP route selection</td>
<td>205</td>
</tr>
<tr>
<td>BGP route summarization</td>
<td>207</td>
</tr>
<tr>
<td>BGP session state change logging</td>
<td>295</td>
</tr>
<tr>
<td>BGP SNMP notification enable</td>
<td>295</td>
</tr>
<tr>
<td>BGP soft reset</td>
<td>280</td>
</tr>
<tr>
<td>BGP TCP connection source address</td>
<td>232</td>
</tr>
<tr>
<td>entity title. Use NET</td>
<td></td>
</tr>
<tr>
<td>interface PBR configuration (packet length-based)</td>
<td>381</td>
</tr>
<tr>
<td>interface PBR configuration (packet source-IP-based)</td>
<td>383</td>
</tr>
<tr>
<td>interface PBR configuration (packet type-based)</td>
<td>380</td>
</tr>
<tr>
<td>IP routing dynamic routing protocols</td>
<td>2</td>
</tr>
<tr>
<td>IP routing extension attribute redistribution</td>
<td>4</td>
</tr>
<tr>
<td>IP routing FIB route max lifetime</td>
<td>4</td>
</tr>
<tr>
<td>IP routing inter-protocol FRR</td>
<td>6</td>
</tr>
<tr>
<td>IP routing IPv4 RIB inter-protocol FRR</td>
<td>7</td>
</tr>
<tr>
<td>IP routing IPv6 RIB inter-protocol FRR</td>
<td>7</td>
</tr>
<tr>
<td>IP routing load sharing</td>
<td>3</td>
</tr>
<tr>
<td>IP routing RIB label max lifetime</td>
<td>4</td>
</tr>
<tr>
<td>IP routing RIB NSR</td>
<td>5</td>
</tr>
<tr>
<td>IP routing RIB route max lifetime</td>
<td>4</td>
</tr>
<tr>
<td>IP routing RIP route redistribution configuration</td>
<td>47</td>
</tr>
<tr>
<td>IP routing route backup</td>
<td>3</td>
</tr>
</tbody>
</table>
IP routing route preference, 2
IP routing route recursion, 3
IP routing route redistribution, 3
IPv4 BGP 4-byte AS number suppression, 273
IPv4 BGP AS number substitution, 264
IPv4 BGP AS_PATH optimal route selection, 263
IPv4 BGP basics, 308
IPv4 BGP BFD configuration, 296, 334
IPv4 BGP community, 287
IPv4 BGP COMMUNITY configuration, 321
IPv4 BGP confederation, 326
IPv4 BGP default local preference, 254
IPv4 BGP dynamic peer configuration, 345
IPv4 BGP fake AS number advertisement, 263
IPv4 BGP FRR configuration, 338
IPv4 BGP GR configuration, 333
IPv4 BGP hold time, 269
IPv4 BGP IGP metrics optimal route selection, 267
IPv4 BGP IGP route redistribution, 235
IPv4 BGP keepalive interval, 269
IPv4 BGP load balancing, 275, 318
IPv4 BGP local network injection, 234
IPv4 BGP multiple hop EBGP session establishment, 272
IPv4 BGP NEXT_HOP attribute, 259
IPv4 BGP path selection, 330
IPv4 BGP peer MD5 authentication, 274
IPv4 BGP private AS number removal, 266
IPv4 BGP received route preferred value, 251
IPv4 BGP route dampening, 250
IPv4 BGP route preference, 253
IPv4 BGP route reflector configuration, 324
IPv4 BGP route summarization, 315
IPv4 BGP route update interval, 271
IPv4 BGP routes received from peer/peer group, 242
IPv4 BGP session establishment disable, 278
IPv4 BGP SoO attribute, 268
IPv4 BGP+IGP route redistribution, 312
IPv4 RIB NSR configuration, 5
IPv6 BGP 4-byte AS number suppression, 273
IPv6 BGP 6PE configuration, 352
IPv6 BGP AS number substitution, 264
IPv6 BGP basic configuration, 347
IPv6 BGP BFD, 296
IPv6 BGP BFD configuration, 355
IPv6 BGP COMMUNITY, 287
IPv6 BGP default local preference, 254
IPv6 BGP fake AS number advertisement, 263
IPv6 BGP FRR configuration, 364
IPv6 BGP hold time, 269
IPv6 BGP IGP route redistribution, 235
IPv6 BGP IPsec, 277
IPv6 BGP keepalive interval, 269
IPv6 BGP load balancing, 275
IPv6 BGP local network injection, 234
IPv6 BGP multiple hop EBGP session establishment, 272
IPv6 BGP NEXT_HOP attribute, 259
IPv6 BGP packet IPsec configuration, 359
IPv6 BGP peer MD5 authentication, 274
IPv6 BGP private AS number removal, 266
IPv6 BGP received route preferred value, 251
IPv6 BGP route dampening, 250
IPv6 BGP route preference, 253
IPv6 BGP route reflector configuration, 350
IPv6 BGP route update interval, 271
IPv6 BGP routes received from peer/peer group, 242
IPv6 BGP session establishment disable, 278
IPv6 BGP SoO attribute, 268
IPv6 IS-IS automatic link cost calculation, 476
IPv6 IS-IS basic configuration, 474, 484
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 IS-IS BFD configuration</td>
<td>479, 488</td>
</tr>
<tr>
<td>IPv6 IS-IS FRR</td>
<td>480</td>
</tr>
<tr>
<td>IPv6 IS-IS FRR configuration</td>
<td>491</td>
</tr>
<tr>
<td>IPv6 IS-IS global cost</td>
<td>476</td>
</tr>
<tr>
<td>IPv6 IS-IS interface cost</td>
<td>476</td>
</tr>
<tr>
<td>IPv6 IS-IS interface tag value</td>
<td>478</td>
</tr>
<tr>
<td>IPv6 IS-IS ISPF enable</td>
<td>479</td>
</tr>
<tr>
<td>IPv6 IS-IS link cost</td>
<td>476</td>
</tr>
<tr>
<td>IPv6 IS-IS LSDB overload bit</td>
<td>478</td>
</tr>
<tr>
<td>IPv6 IS-IS network optimization</td>
<td>477</td>
</tr>
<tr>
<td>IPv6 IS-IS network tuning</td>
<td>477</td>
</tr>
<tr>
<td>IPv6 IS-IS prefix suppression</td>
<td>479</td>
</tr>
<tr>
<td>IPv6 IS-IS route control</td>
<td>475</td>
</tr>
<tr>
<td>IPv6 IS-IS route convergence priority</td>
<td>477</td>
</tr>
<tr>
<td>IPv6 IS-IS SPF calculation interval</td>
<td>478</td>
</tr>
<tr>
<td>IPv6 PBR configuration</td>
<td>499</td>
</tr>
<tr>
<td>IPv6 PBR interface configuration</td>
<td>499</td>
</tr>
<tr>
<td>IPv6 PBR local configuration</td>
<td>499</td>
</tr>
<tr>
<td>IPv6 PBR node action</td>
<td>497</td>
</tr>
<tr>
<td>IPv6 PBR node creation</td>
<td>497</td>
</tr>
<tr>
<td>IPv6 PBR node match criteria</td>
<td>497</td>
</tr>
<tr>
<td>IPv6 PBR policy configuration</td>
<td>497</td>
</tr>
<tr>
<td>IPv6 PBR+Track collaboration</td>
<td>496</td>
</tr>
<tr>
<td>IPv6 RIB NSR configuration</td>
<td>6</td>
</tr>
<tr>
<td>IPv6 static route BFD configuration</td>
<td>386</td>
</tr>
<tr>
<td>IPv6 static route BFD control mode (direct next hop)</td>
<td>387</td>
</tr>
<tr>
<td>IPv6 static route BFD control mode (indirect next hop)</td>
<td>387</td>
</tr>
<tr>
<td>IPv6 static route BFD echo mode (single hop)</td>
<td>387</td>
</tr>
<tr>
<td>IPv6 static route configuration</td>
<td>386</td>
</tr>
<tr>
<td>IS-IS area</td>
<td>137</td>
</tr>
<tr>
<td>IS-IS ATT bit</td>
<td>159, 159</td>
</tr>
<tr>
<td>IS-IS authentication (area)</td>
<td>165</td>
</tr>
<tr>
<td>IS-IS authentication (neighbor relationship)</td>
<td>165</td>
</tr>
<tr>
<td>IS-IS authentication (routing domain)</td>
<td>166</td>
</tr>
<tr>
<td>IS-IS authentication configuration</td>
<td>187</td>
</tr>
<tr>
<td>IS-IS automatic cost calculation</td>
<td>146</td>
</tr>
<tr>
<td>IS-IS basic configuration</td>
<td>143</td>
</tr>
<tr>
<td>IS-IS basics configuration</td>
<td>175</td>
</tr>
<tr>
<td>IS-IS BFD</td>
<td>168</td>
</tr>
<tr>
<td>IS-IS BFD configuration</td>
<td>194</td>
</tr>
<tr>
<td>IS-IS broadcast type</td>
<td>138</td>
</tr>
<tr>
<td>IS-IS DIS election</td>
<td>138</td>
</tr>
<tr>
<td>IS-IS DIS election configuration</td>
<td>179</td>
</tr>
<tr>
<td>IS-IS enable</td>
<td>143</td>
</tr>
<tr>
<td>IS-IS FRR</td>
<td>169</td>
</tr>
<tr>
<td>IS-IS FRR configuration</td>
<td>197</td>
</tr>
<tr>
<td>IS-IS global cost</td>
<td>145</td>
</tr>
<tr>
<td>IS-IS GR</td>
<td>166</td>
</tr>
<tr>
<td>IS-IS GR configuration</td>
<td>189</td>
</tr>
<tr>
<td>IS-IS hello multiplier</td>
<td>152</td>
</tr>
<tr>
<td>IS-IS hello packet send interval</td>
<td>152</td>
</tr>
<tr>
<td>IS-IS interface cost</td>
<td>145</td>
</tr>
<tr>
<td>IS-IS interface DIS priority</td>
<td>153</td>
</tr>
<tr>
<td>IS-IS interface hello packet send</td>
<td>154</td>
</tr>
<tr>
<td>IS-IS interface P2P network type</td>
<td>144</td>
</tr>
<tr>
<td>IS-IS interface packet send/receive</td>
<td>154</td>
</tr>
<tr>
<td>IS-IS interface tag value</td>
<td>160</td>
</tr>
<tr>
<td>IS-IS IS+ circuit level</td>
<td>143</td>
</tr>
<tr>
<td>IS-IS ISPF</td>
<td>162</td>
</tr>
<tr>
<td>IS-IS link cost</td>
<td>144</td>
</tr>
<tr>
<td>IS-IS LSDB overload bit</td>
<td>159</td>
</tr>
<tr>
<td>IS-IS LSP flash flooding</td>
<td>156</td>
</tr>
<tr>
<td>IS-IS LSP flooding</td>
<td>157</td>
</tr>
<tr>
<td>IS-IS LSP fragment extension</td>
<td>156</td>
</tr>
<tr>
<td>IS-IS LSP length</td>
<td>155</td>
</tr>
<tr>
<td>IS-IS LSP parameters</td>
<td>154</td>
</tr>
<tr>
<td>IS-IS LSP timer</td>
<td>154</td>
</tr>
<tr>
<td>IS-IS MTR</td>
<td>172</td>
</tr>
<tr>
<td>IS-IS neighbor state change logging</td>
<td>161</td>
</tr>
<tr>
<td>IS-IS network management</td>
<td>163</td>
</tr>
<tr>
<td>IS-IS network optimization</td>
<td>152</td>
</tr>
<tr>
<td>IS-IS network tuning</td>
<td>152</td>
</tr>
<tr>
<td>IS-IS NSR</td>
<td>167</td>
</tr>
<tr>
<td>IS-IS NSR configuration</td>
<td>190</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>IS-IS PIC BFD</td>
<td>164</td>
</tr>
<tr>
<td>IS-IS PIC configuration</td>
<td>163</td>
</tr>
<tr>
<td>IS-IS point-to-point type</td>
<td>138</td>
</tr>
<tr>
<td>IS-IS preference</td>
<td>146</td>
</tr>
<tr>
<td>IS-IS prefix suppression</td>
<td>162</td>
</tr>
<tr>
<td>IS-IS pseudonode</td>
<td>138</td>
</tr>
<tr>
<td>IS-IS route control</td>
<td>144</td>
</tr>
<tr>
<td>IS-IS route convergence priority</td>
<td>158</td>
</tr>
<tr>
<td>IS-IS route leaking</td>
<td>138</td>
</tr>
<tr>
<td>IS-IS route redistribution</td>
<td>183</td>
</tr>
<tr>
<td>IS-IS routing domain</td>
<td>137</td>
</tr>
<tr>
<td>IS-IS security enhancement</td>
<td>164</td>
</tr>
<tr>
<td>IS-IS SPF calculation interval</td>
<td>157</td>
</tr>
<tr>
<td>IS-IS system ID &gt; host name mapping</td>
<td>160</td>
</tr>
<tr>
<td>local PBR configuration (packet type-based)</td>
<td>378</td>
</tr>
<tr>
<td>MP-BGP</td>
<td>210</td>
</tr>
<tr>
<td>MTR configuration</td>
<td>520</td>
</tr>
<tr>
<td>multicast BGP configuration</td>
<td>341</td>
</tr>
<tr>
<td>OSPF area</td>
<td>76</td>
</tr>
<tr>
<td>OSPF area configuration (NSSA)</td>
<td>77, 115</td>
</tr>
<tr>
<td>OSPF area configuration (stub)</td>
<td>77, 113</td>
</tr>
<tr>
<td>OSPF basics configuration</td>
<td>105</td>
</tr>
<tr>
<td>OSPF BFD</td>
<td>101</td>
</tr>
<tr>
<td>OSPF BFD configuration</td>
<td>127</td>
</tr>
<tr>
<td>OSPF BFD detection configuration (bidirectional control)</td>
<td>101</td>
</tr>
<tr>
<td>OSPF BFD detection configuration (single-hop echo)</td>
<td>102</td>
</tr>
<tr>
<td>OSPF DD packet interface MTU</td>
<td>91</td>
</tr>
<tr>
<td>OSPF DR election configuration</td>
<td>117</td>
</tr>
<tr>
<td>OSPF ECMP routes max</td>
<td>83</td>
</tr>
<tr>
<td>OSPF enable</td>
<td>75</td>
</tr>
<tr>
<td>OSPF exit overflow interval</td>
<td>92</td>
</tr>
<tr>
<td>OSPF FRR</td>
<td>102</td>
</tr>
<tr>
<td>OSPF FRR configuration</td>
<td>130</td>
</tr>
<tr>
<td>OSPF GR</td>
<td>98</td>
</tr>
<tr>
<td>OSPF GR configuration</td>
<td>123</td>
</tr>
<tr>
<td>OSPF GR helper</td>
<td>99</td>
</tr>
<tr>
<td>OSPF GR restarters</td>
<td>99</td>
</tr>
<tr>
<td>OSPF GTSM configuration</td>
<td>97</td>
</tr>
<tr>
<td>OSPF host route advertisement</td>
<td>86</td>
</tr>
<tr>
<td>OSPF interface cost</td>
<td>83</td>
</tr>
<tr>
<td>OSPF interface network type (broadcast)</td>
<td>79</td>
</tr>
<tr>
<td>OSPF interface network type (NBMA)</td>
<td>79</td>
</tr>
<tr>
<td>OSPF interface network type (P2MP)</td>
<td>80</td>
</tr>
<tr>
<td>OSPF interface network type (P2P)</td>
<td>80</td>
</tr>
<tr>
<td>OSPF interface packet send/receive disable</td>
<td>89</td>
</tr>
<tr>
<td>OSPF ISPF</td>
<td>94</td>
</tr>
<tr>
<td>OSPF log count</td>
<td>96</td>
</tr>
<tr>
<td>OSPF LSA arrival interval</td>
<td>88</td>
</tr>
<tr>
<td>OSPF LSA generation interval</td>
<td>88</td>
</tr>
<tr>
<td>OSPF LSA transmission delay</td>
<td>87</td>
</tr>
<tr>
<td>OSPF LSDB external LSAs max</td>
<td>91</td>
</tr>
<tr>
<td>OSPF LSU transmit rate</td>
<td>94</td>
</tr>
<tr>
<td>OSPF neighbor state change logging</td>
<td>92</td>
</tr>
<tr>
<td>OSPF network LSA</td>
<td>67</td>
</tr>
<tr>
<td>OSPF network management</td>
<td>93</td>
</tr>
<tr>
<td>OSPF network summary LSA</td>
<td>67</td>
</tr>
<tr>
<td>OSPF network type</td>
<td>78</td>
</tr>
<tr>
<td>OSPF NSR</td>
<td>100</td>
</tr>
<tr>
<td>OSPF NSR configuration</td>
<td>125</td>
</tr>
<tr>
<td>OSPF optimization</td>
<td>86</td>
</tr>
<tr>
<td>OSPF outbound LSA filtering (interface)</td>
<td>97</td>
</tr>
<tr>
<td>OSPF outbound LSA filtering (specified neighbor)</td>
<td>97</td>
</tr>
<tr>
<td>OSPF packet DSCP value</td>
<td>91</td>
</tr>
<tr>
<td>OSPF PIC configuration</td>
<td>95</td>
</tr>
<tr>
<td>OSPF preference</td>
<td>84</td>
</tr>
<tr>
<td>OSPF prefix priority</td>
<td>95</td>
</tr>
<tr>
<td>OSPF prefix suppression</td>
<td>94</td>
</tr>
<tr>
<td>OSPF received route filtering</td>
<td>82</td>
</tr>
<tr>
<td>OSPF RFC 1583 compatibility</td>
<td>92</td>
</tr>
<tr>
<td>OSPF route calculation</td>
<td>71</td>
</tr>
<tr>
<td>OSPF route control</td>
<td>81</td>
</tr>
<tr>
<td>OSPF route redistribution</td>
<td>84</td>
</tr>
<tr>
<td>OSPF route redistribution configuration</td>
<td>108</td>
</tr>
<tr>
<td>OSPF route summarization</td>
<td>81</td>
</tr>
</tbody>
</table>
RIP network optimization, 33
RIP network tuning, 33
RIP NSR configuration, 54
RIP NSR enable, 40
RIP operation, 25
RIP packet max length, 39
RIP packet send rate configuration, 38
RIP poison reverse configuration, 34
RIP preference configuration, 32
RIP received/redistributed route filtering, 32
RIP route control configuration, 30
RIP route entries, 25
RIP route redistribution configuration, 33
RIP routing loop prevention, 25
RIP split horizon configuration, 34
RIP summary route advertisement configuration, 51
RIP timer configuration, 33
RIP triggered update interval configuration, 36
RIP update source IP address check, 35
RIP version configuration, 29
RIP versions, 26
RIPv1 message zero field check, 35
RIPv2 message authentication configuration, 36
RIPv2 route summarization configuration, 30
routing policy apply clause, 512
routing policy AS_PATH list, 509
routing policy COMMUNITY list, 509
routing policy configuration, 510
routing policy configuration (IPv4 route redistribution), 515
routing policy configuration (IPv6 route redistribution), 517
routing policy continue clause, 514
routing policy creation, 510
routing policy extended community list, 510
routing policy filter configuration, 508
routing policy if-match clause, 511
routing policy IP prefix list, 508
routing policy MAC list, 510
static routing BFD bidirectional control mode (direct next hop), 10
static routing BFD bidirectional control mode (indirect next hop), 10
static routing BFD configuration, 10
static routing BFD single-hop echo mode, 11
static routing configuration, 9
static routing FRR configuration, 12
triggered RIP (TRIP), 26
triggered RIP (TRIP) configuration, 37
tuning BGP, 269

network management
BGP configuration, 200, 213
BGP large scale networks, 207
IP routing configuration, 1
IPv4 BGP configuration, 308
IPv6 BGP configuration, 347
IPv6 default route configuration, 396
IPv6 IS-IS configuration, 474, 484
IPv6 PBR configuration, 494, 497, 500
IPv6 PBR interface configuration (packet length-based), 503
IPv6 PBR interface configuration (packet type-based), 502
IPv6 PBR local configuration (packet type-based), 500
IPv6 static routing basic configuration, 388
IPv6 static routing BFD (direct next hop), 390
IPv6 static routing BFD (indirect next hop), 393
IPv6 static routing configuration, 386, 388
IS-IS configuration, 135, 142, 175
MTR configuration, 520
OSPF configuration, 67, 73, 105
OSPFv3 configuration, 422, 423, 445
OSPFv3 network optimization, 432
OSPFv3 network tuning, 432
PBR configuration, 372, 375, 377, 378
RIP configuration, 25, 27, 44
RIPng configuration, 397, 398, 408
routing policy configuration, 507, 515
static routing basic configuration, 14
static routing BFD configuration (direct next hop), 16
static routing BFD configuration (indirect next hop), 18
static routing configuration, 9, 14
static routing default route configuration, 24
static routing FRR configuration, 21

**NEXT_HOP**

BGP path attribute, 200

**IPV4 BGP NEXT_HOP attribute configuration, 259**

**IPV6 BGP NEXT_HOP attribute configuration, 259**

**NO_ADVERTISE**

BGP COMMUNITY path attribute, 200

**NO_EXPORT**

BGP COMMUNITY path attribute, 200

**NO_EXPORT_SUBCONFED**

BGP COMMUNITY path attribute, 200

node

IPv6 PBR node action, 497
IPv6 PBR node creation, 497
IPv6 PBR node match criteria, 497
IPv6 PBR policy, 494
IPv6 PBR+Track collaboration, 496
IS-IS pseudonode, 138
IS-IS route control, 144
PBR apply clause, 372
PBR creation, 375
PBR if-match clause, 372
PBR match criteria, 375
PBR node action, 375
PBR policy, 372
PBR-Track collaboration, 374
routing policy apply clause, 508, 512
routing policy continue clause, 508, 514
routing policy deny match, 508
routing policy if-match clause, 508, 511
routing policy permit match, 508

**non-IETF**

OSPF GR, 98
OSPF GR helper, 99
OSPF GR restarter, 99

**nonstop routing. Use NSR**

notifying

BGP notification message, 200
BGP SNMP notification enable, 295
OSPF network management, 93
NSAP
- IS-IS address format, 135
- NET, 136
N-SEL (IS-IS), 136
NSR
- BGP NSR configuration, 294
- IP routing RIB NSR, 5
- IPv4 RIB NSR configuration, 5
- IPv6 RIB NSR configuration, 6
- IS-IS NSR, 167
- IS-IS NSR configuration, 190
 OSPF configuration, 100
- OSPF NSR configuration, 125
- OSPFv3 NSR, 439
- OSPFv3 NSR configuration, 463
- RIP configuration, 54
- RIPng NSR configuration, 405, 414
NSSA
- OSPF area configuration, 77, 115
- OSPF NSSA area, 70
- OSPF NSSA LSA, 67
- OSPF totally NSSA area, 70
- OSPFv3 NSSA area, 425
- OSPFv3 NSSA area configuration, 450
number
- BGP first AS number of EBGP route updates, 267
- IPv4 BGP 4-byte AS number suppression, 273
- IPv4 BGP AS number substitution, 264
- IPv4 BGP fake AS number advertisement, 263
- IPv4 BGP local AS number appearance, 262
- IPv4 BGP private AS number removal, 266
- IPv6 BGP 4-byte AS number suppression, 273
- IPv6 BGP AS number substitution, 264
- IPv6 BGP fake AS number advertisement, 263
- IPv6 BGP local AS number appearance, 262
- IPv6 BGP private AS number removal, 266
O
open
- BGP message, 200
- Open Shortest Path First. Use OSPF
- Open Shortest Path First version 3. Use OSPFv3 optimal
  - BGP route, 240
  - IP routing FIB table optimal routes, 1
optimizing
  - BGP network, 269
  - IPv6 IS-IS networks, 477
  - IS-IS networks, 152
  - OSPF network, 86
  - OSPFv3 network, 432
  - RIP networks, 33
  - RIPng network, 401
ORIGIN
- BGP path attribute, 200
OSPF, 422, See also OSPFv3
  - area configuration, 76
  - area configuration (NSSA), 77, 115
  - area configuration (stub), 77, 113
  - areas, 68
  - authentication configuration, 90
  - backbone area, 69
  - basic configuration, 105
  - BDR, 72
  - BFD configuration, 101, 127
  - BFD detection configuration (bidirectional control), 101
  - BFD detection configuration (single-hop echo), 102
  - BFD FRR configuration, 103
  - configuration, 67, 73, 105
  - DD packet interface MTU add, 91
display, 104
DR, 72
DR election configuration, 117
ECMP routes max, 83
enable, 75
exit overflow interval, 92
FRR backup next hop calculation (LFA algorithm), 103
FRR backup next hop specification (routing policy), 103
FRR configuration, 102, 130
GR configuration, 98, 123
GR helper, 99
GR reOF28ga, 99
GR trigger, 100
GTSM configuration, 97
host route advertisement, 86
interface cost, 83
interface network type (broadcast), 79
interface network type (NBMA), 79
interface network type (P2MP), 80
interface network type (P2P), 80
interface packet send/receive disable, 89
IS-IS BFD, 168
IS-IS DIS election, 138
ISPF enable, 94
log count configuration, 96
LSA arrival interval, 88
LSA generation interval, 88
LSA transmission delay, 87
LSA types, 67
LSDB external LSAs max, 91
LSU transmit rate configuration, 94
maintain, 104
neighbor state change logging, 92
network management configuration, 93
network optimization, 86
network tuning, 86
network type configuration, 78
network types, 72
nonstop routing (NSR) configuration, 100, 125
NSSA area, 70
outbound LSA filtering (interface), 97
outbound LSA filtering (specified neighbor), 97
packet DSCP value configuration, 91
packet types, 67
PIC configuration, 95
PIC enable, 96
preference configuration, 84
prefix priority configuration, 95
prefix suppression, 94
protocols and standards, 73
received route filtering, 82
redistributed route default parameters, 85
redistributed route summarization (ASBR), 81
RFC 1583 compatibility, 92
route calculation, 71
route control configuration, 81
route redistribution, 84
route redistribution configuration, 108
route summarization, 81
route summarization (ABR), 81
route summarization configuration, 110
route types, 71
router types, 70
SPF calculation interval, 88
stub area, 69
stub router configuration, 89
summary network discard route, 84
timer set, 86
totally NSSA area, 70
totally stub area, 69
troubleshoot configuration, 133
troubleshoot incorrect routing information, 133
troubleshoot no neighbor relationship established, 133
Type-3 LSA filtering, 82
virtual link configuration, 78, 121
virtual links, 69
OSPFv3, 422, See also OSPF
area parameter configuration, 425
BFD configuration, 440, 464
BFD FRR configuration, 442
configuration, 422, 423, 445
DD packet ignore MTU check, 434
display, 444
DR election configuration, 452
ECMP route max, 430
enable, 424
FRR backup next hop calculation (LFA algorithm), 441
FRR backup next hop specification (routing policy), 442
FRR configuration, 441, 467
GR configuration, 438, 462
GR helper configuration, 439
GR replacer configuration, 438
GR trigger, 439
Inter-Area-Prefix LSA filtering, 429
interface cost configuration, 429
interface DR priority, 434
interface packet send/receive disable, 434
IPsec profile application, 443
IPsec profile configuration, 469
LSA generation interval, 433
LSA transmission delay, 432
LSA types, 422
LSU transmit rate, 436
maintain, 444
NBMA neighbor configuration, 427
neighbor state change logging, 435
network management configuration, 435
network optimization, 432
network tuning, 432
network type configuration, 426
network type configuration (interface), 427
nonstop routing (NSR) configuration, 439
NSR configuration, 463
NSSA area configuration, 425, 450
P2MP neighbor configuration, 427
packet types, 422
preference configuration, 430
prefix suppression, 437
protocols and standards, 423
received route filtering, 428
redistributed route tag, 431
route control configuration, 427
route redistribution, 430, 455
route redistribution (another routing protocol), 431
route redistribution (default route), 431
route summarization, 428, 458
route summarization (ABR), 428
route summarization (ASBR), 428
SPF calculation interval, 433
stub area configuration, 425, 445
stub router configuration, 436
timer configuration, 432
virtual link configuration, 426

P

P2MP
OSPF interface network type, 80
OSPF network type, 72
OSPFv3 P2MP neighbor, 427

P2P
IS-IS network type, 144
OSPF interface network type, 80
OSPF network type, 72, 78
OSPFv3 network type, 426
OSPFv3 network type (interface), 427

packet
interface PBR configuration, 377
interface PBR configuration (packet length-based), 381
interface PBR configuration (packet source-IP-based), 383
interface PBR configuration (packet type-based), 380
IP routing configuration, 1
IP routing dynamic routing protocols, 2
IP routing extension attribute redistribution, 4
IP routing load sharing, 3
IP routing route backup, 3
IP routing route preference, 2
IP routing route recursion, 3
IP routing route redistribution, 3
IPv6 BGP IPsec, 277
IPv6 BGP packet IPsec configuration, 359
IPv6 PBR configuration, 494, 497, 499, 500
IPv6 PBR interface configuration, 499
IPv6 PBR interface configuration (packet length-based), 503
IPv6 PBR interface configuration (packet type-based), 502
IPv6 PBR local configuration, 499
IPv6 PBR local configuration (packet type-based), 500
IPv6 PBR policy, 494
IPv6 PBR policy configuration, 497
IS-IS CSNP packet send interval, 153
IS-IS hello multiplier, 152
IS-IS hello packet send interval, 152
IS-IS interface hello packet send, 154
IS-IS interface packet send/receive, 154
IS-IS PDU CLVs, 140
IS-IS PDU hello type, 140
IS-IS PDU LSP type, 140
IS-IS PDU SNP type, 140
IS-IS PDU types, 139
IS-IS PPP interface hello packet source address check, 153
local PBR configuration, 377
local PBR configuration (packet type-based), 378
OSPF basics configuration, 105
OSPF BFD, 101
OSPF configuration, 67, 73, 105
OSPF DD, 67
OSPF DD packet interface MTU, 91
OSPF exit overflow interval, 92
OSPF FRR, 102
OSPF GR, 98
OSPF GR helper, 99
OSPF GR restart, 99
OSPF hello, 67
OSPF interface packet send/receive disable, 89
OSPF ISPF, 94
OSPF LSAck, 67
OSPF LSDB external LSAs max, 91
OSPF LSR, 67
OSPF LSU, 67
OSPF LSU transmit rate, 94
OSPF packet DSCP value, 91
OSPF RFC 1583 compatibility, 92
OSPF route redistribution configuration, 108
OSPF stub router, 89
OSPFv3 BFD configuration, 464
OSPFv3 configuration, 422, 423, 445
OSPFv3 DD, 422
OSPFv3 DD packet ignore MTU check, 434
OSPFv3 DR election configuration, 452
OSPFv3 FRR, 441
OSPFv3 GR configuration, 462
OSPFv3 hello, 422
OSPFv3 interface packet send/receive disable, 434
OSPFv3 IPsec profile configuration, 469
OSPFv3 LSAck, 422
OSPFv3 LSR, 422
OSPFv3 LSU, 422
OSPFv3 LSU transmit rate, 436
OSPFv3 NSSA area configuration, 450
OSPFv3 route redistribution, 455
OSPFv3 stub area configuration, 445
OSPFv3 stub router, 436
PBR configuration, 372, 375, 377, 378
PBR policy configuration, 375
RIP BFD configuration (bidirectional control detection), 42
RIP BFD configuration (single-hop echo detection/neighbor), 41
RIP BFD configuration (single-hop echo detection/specific destination), 41
RIP network management configuration, 38
RIP packet max length, 39
RIP packet send rate configuration, 38
RIPvng, 397
RIPvng packet send rate, 403
RIPvng packet zero field check, 402
RIPvng triggered update send interval, 403
IPv6 IS-IS LSDB overload bit, 478
IPv6 IS-IS SPF calculation interval, 478
IS-IS LSDB overload bit, 159
IS-IS LSP parameters, 154
IS-IS route convergence priority, 158
IS-IS SPF calculation interval, 157
OSPF redistributed route default parameters, 85
OSPFv3 area parameter, 425
triggered RIP (TRIP) retransmission parameters, 37
BGP MED attribute, 256
BGP path attributes, 200
BGP path selection, 251
IPv4 BGP COMMUNITY configuration, 321
IPv4 BGP MED AS route comparison (confederation peers), 259
IPv4 BGP MED AS route comparison (diff ASs), 257
IPv4 BGP MED AS route comparison (per-AS), 257
IPv4 BGP MED default value, 256
IPv4 BGP NEXT_HOP attribute, 259
IPv4 BGP path selection configuration, 330
IPv6 BGP MED AS route comparison (confederation peers), 259
IPv6 BGP MED AS route comparison (diff ASs), 257
IPv6 BGP MED AS route comparison (per-AS), 257
IPv6 BGP MED default value, 256
IPv6 BGP NEXT_HOP attribute, 259
multicast BGP configuration, 341, 367
OSPF configuration, 67
PBR configuration, 372, 375, 377, 378
display, 378
interface configuration, 377
interface configuration (packet length-based), 381
interface configuration (packet source-IP-based), 383
interface configuration (packet type-based), 380
interface PBR, 372
local configuration, 377
local configuration (packet type-based), 378
local PBR, 372
maintain, 378
node action configuration, 375
node creation, 375
node match criteria, 375
policy, 372
policy configuration, 375
relationship between match mode/clauses, 373
Track collaboration, 374
PDU
IS-IS CLVs, 140
IS-IS hello type, 140
IS-IS LSP type, 140
IS-IS SNP type, 140
IS-IS types, 139
routing policy apply clause, 512
routing policy AS_PATH list, 509
routing policy COMMUNITY list, 509
routing policy configuration, 507, 510, 515
routing policy configuration (IPv4 route redistribution), 515
routing policy configuration (IPv6 route redistribution), 517
routing policy continue clause, 514
routing policy creation, 510
routing policy extended community list, 510
routing policy filter configuration, 508
routing policy filtering, 508
routing policy if-match clause, 511
routing policy IP prefix list, 508
routing policy MAC list, 510
policy-based routing. Use PBR
poll packet timer (OSPF), 86
PPP
  interface hello packet source address check, 153
preference
  IP routing route preference, 2
  OSPF route redistribution, 84
  RIP configuration, 32
preferring
  BGP received route preferred value, 251
  IPv4 BGP default local preference, 254
  IPv4 BGP route preference, 253
  IPv6 BGP default local preference, 254
  IPv6 BGP route preference, 253
  IS-IS preference specification, 146
  OSPF protocol preference, 84
  OSPFv3 preference, 430
  RIPng preference, 400
prefix
  IPv6 IS-IS prefix suppression, 479
  IS-IS prefix suppression, 162
  OSPF PIC configuration, 95
OSPF prefix priority, 95
OSPF prefix suppression, 94
OSPFv3 prefix suppression, 437
routing policy IP prefix list, 508
routing policy prefix list, 507
Prefix Independent Convergence. Use PIC
  priority
  IPv6 IS-IS route convergence priority, 477
  IS-IS interface DIS priority, 153
  IS-IS route convergence priority, 158
  OSPF prefix priority configuration, 95
  OSPF route level priority, 71
  OSPFv3 interface DR priority, 434
procedure
  advertising BGP default route to peer/peer group, 241
  advertising BGP optimal route, 240
  advertising IPv4 BGP fake AS number, 263
  advertising IPv6 BGP fake AS number, 263
  advertising IS-IS default route, 148
  advertising RIP default route, 31
  advertising RIPng default route, 400
  advertising RIPv2 summary route, 31
  applying OSPFv3 IPsec profile, 443
  applying RIPng IPsec profile, 407
  assigning IPv6 IS-IS route convergence priority, 477
  clearing IPv4 BGP information, 307
  clearing IPv6 BGP information, 307
  configuring BGP, 213
  configuring BGP 6PE, 301
  configuring BGP 6PE basics, 301
  configuring BGP 6PE optional capabilities, 302
  configuring BGP AS_PATH attribute, 262
  configuring BGP basics, 216
  configuring BGP confederation, 292
  configuring BGP configuration compatability, 292
  configuring BGP dynamic peer, 219
configuring BGP dynamic peer (IPv4 multicast address), 221
configuring BGP dynamic peer (IPv4 unicast address), 220
configuring BGP dynamic peer (IPv6 multicast address), 221
configuring BGP dynamic peer (IPv6 unicast address), 220
configuring BGP FRR, 297
configuring BGP GR, 293
configuring BGP GR helper, 293
configuring BGP GR restarter, 293
configuring BGP GTSM, 279
configuring BGP large-scale network, 287
configuring BGP MED attribute, 256
configuring BGP MPLS local label update delay, 286
configuring BGP NSR, 294
configuring BGP peer, 217
configuring BGP peer (IPv4 multicast address), 219
configuring BGP peer (IPv4 unicast address), 217
configuring BGP peer (IPv6 multicast address), 219
configuring BGP peer (IPv6 unicast address), 218
configuring BGP peer group, 222
configuring BGP policy accounting, 300
configuring BGP route filtering policies, 244
configuring BGP route reflection, 289
configuring BGP route summarization, 237
configuring BGP soft reset, 280
configuring EBGP peer group (IPv4 multicast address), 224
configuring EBGP peer group (IPv4 unicast address), 224
configuring EBGP peer group (IPv6 multicast address), 224
configuring EBGP peer group (IPv6 unicast address), 224
configuring IBGP peer group (IPv4 multicast address), 222
configuring IBGP peer group (IPv4 unicast address), 222
configuring IBGP peer group (IPv6 multicast address), 222
configuring IBGP peer group (IPv6 unicast address), 222
configuring interface PBR, 377
configuring interface PBR (packet length-based), 381
configuring interface PBR (packet source-IP-based), 383
configuring interface PBR (packet type-based), 380
configuring inter-protocol FRR, 6
configuring IP routing IPv6 IS-IS route control, 475
configuring IP routing RIB NSR, 5
configuring IP routing RIP GR, 53
configuring IP routing RIP NSR, 54
configuring IP routing RIP route redistribution, 47
configuring IPv4 BGP AS number substitution, 264
configuring IPv4 BGP basics, 308
configuring IPv4 BGP BFD, 296, 334
configuring IPv4 BGP COMMUNITY, 287, 321
configuring IPv4 BGP confederation, 326
configuring IPv4 BGP default local preference, 254
configuring IPv4 BGP dynamic peer, 345
configuring IPv4 BGP FRR, 338
configuring IPv4 BGP GR, 333
configuring IPv4 BGP hold time, 269
configuring IPv4 BGP keepalive interval, 269
configuring IPv4 BGP load balancing, 318
configuring IPv4 BGP MED default value, 256
configuring IPv4 BGP NEXT_HOP attribute, 259
configuring IPv4 BGP path selection, 330
configuring IPv4 BGP route dampening, 250
configuring IPv4 BGP route distribution filtering policies, 244
configuring IPv4 BGP route preference, 253
configuring IPv4 BGP route reception filtering policies, 247
configuring IPv4 BGP route reflector, 289, 324
configuring IPv4 BGP route summarization, 315
configuring IPv4 BGP route summarization (automatic), 237
configuring IPv4 BGP route summarization (manual), 238
configuring IPv4 BGP route update delay, 250
configuring IPv4 BGP route update interval, 271
configuring IPv4 BGP soft reset manually, 283
configuring IPv4 BGP SoO attribute, 268
configuring IPv4 BGP to ignore IGP metrics during optimal route selection, 267
configuring IPv4 BGP to ignore the AS_PATH attributes during optimal route selection, 263
configuring IPv4 BGP+IGP route redistribution, 312
configuring IPv4 RIB inter-protocol FRR, 7
configuring IPv4 RIB NSR, 5
configuring IPv6 BGP 6PE, 352
configuring IPv6 BGP AS number substitution, 264
configuring IPv6 BGP basics, 347
configuring IPv6 BGP BFD, 296, 355
configuring IPv6 BGP COMMUNITY, 287
configuring IPv6 BGP default local preference, 254
configuring IPv6 BGP FRR, 364
configuring IPv6 BGP hold time, 269
configuring IPv6 BGP IPsec, 277
configuring IPv6 BGP keepalive interval, 269
configuring IPv6 BGP load balancing, 275
configuring IPv6 BGP MED default value, 256
configuring IPv6 BGP NEXT_HOP attribute, 259
configuring IPv6 BGP packet IPsec, 359
configuring IPv6 BGP route dampening, 250
configuring IPv6 BGP route distribution filtering policies, 244
configuring IPv6 BGP route preference, 253
configuring IPv6 BGP route reception filtering policies, 247
configuring IPv6 BGP route reflector, 289, 350
configuring IPv6 BGP route summarization (manual), 238
configuring IPv6 BGP route update interval, 271
configuring IPv6 BGP soft reset manually, 283
configuring IPv6 BGP SoO attribute, 268
configuring IPv6 IS-IS basics, 474, 484
configuring IPv6 IS-IS BFD, 479, 488
configuring IPv6 IS-IS FRR, 480, 491
configuring IPv6 IS-IS FRR automatic backup next hop LFA calculation, 481
configuring IPv6 IS-IS FRR using routing policy, 481
configuring IPv6 IS-IS global cost, 476
configuring IPv6 IS-IS interface cost, 476
configuring IPv6 IS-IS interface tag value, 478
configuring IPv6 IS-IS link cost, 476
configuring IPv6 PBR, 497, 499
configuring IPv6 PBR interface, 499
configuring IPv6 PBR interface (packet length-based), 503
configuring IPv6 PBR interface (packet type-based), 502
configuring IPv6 PBR local, 499
configuring IPv6 PBR local (packet type-based), 500
configuring IPv6 PBR node action, 497
configuring IPv6 PBR policy, 497
configuring IPv6 RIB inter-protocol FRR, 7
configuring IPv6 RIB NSR, 6
configuring IPv6 static route, 386
configuring IPv6 static route BFD, 386
configuring IPv6 static route BFD control mode (direct next hop), 387
configuring IPv6 static route BFD control mode (indirect next hop), 387
configuring IPv6 static route BFD echo mode (single hop), 387
configuring IPv6 static routing, 388
configuring IPv6 static routing basics, 388
configuring IPv6 static routing BFD (direct next hop), 390
configuring IPv6 static routing BFD (indirect next hop), 393
configuring IS-IS, 142
configuring IS-IS ATT bit, 159
configuring IS-IS ATT bit default route calculation, 159
configuring IS-IS authentication, 187
configuring IS-IS authentication (area), 165
configuring IS-IS authentication (neighbor relationship), 165
configuring IS-IS authentication (routing domain), 166
configuring IS-IS basics, 143, 175
configuring IS-IS BFD, 168, 194
configuring IS-IS DIS election, 179
configuring IS-IS ECMP routes max, 147
configuring IS-IS FRR, 169, 197
configuring IS-IS FRR (routing policy), 170
configuring IS-IS FRR backup next hop (LFA calculation), 169
configuring IS-IS global cost, 145
configuring IS-IS GR, 166, 189
configuring IS-IS interface cost, 145
configuring IS-IS interface DIS priority, 153
configuring IS-IS interface P2P network type, 144
configuring IS-IS interface tag value, 160
configuring IS-IS link cost, 144
configuring IS-IS LSP parameters, 154
configuring IS-IS LSP timer, 154
configuring IS-IS LSP-calculated route filtering, 150
configuring IS-IS MTR, 172
configuring IS-IS network management, 163
configuring IS-IS NSR, 167, 190
configuring IS-IS PIC, 163
configuring IS-IS redistributed route filtering, 150
configuring IS-IS route control, 144
configuring IS-IS route convergence priority, 158
configuring IS-IS route filtering, 150
configuring IS-IS route leaking, 151
configuring IS-IS route redistribution, 149, 183
configuring IS-IS route summarization, 148
configuring IS-IS system ID > host name mapping, 160
configuring IS-IS system ID > host name mapping (dynamic), 161
configuring IS-IS system ID > host name mapping (static), 160
configuring local PBR, 377
configuring local PBR (packet type-based), 378
configuring MTR, 520
configuring multicast BGP, 341, 367
configuring OSPF, 73
configuring OSPF area, 76
configuring OSPF area (NNSA), 77, 115
configuring OSPF area (stub), 77, 113
configuring OSPF authentication (area), 90
configuring OSPF authentication (interface), 90
configuring OSPF basics, 105
configuring OSPF BFD, 101, 127
configuring OSPF BFD detection (bidirectional control), 101
configuring OSPF BFD detection (single-hop echo), 102
configuring OSPF DD packet interface MTU, 91
configuring OSPF DR election, 117
configuring OSPF FRR, 102, 130
configuring OSPF FRR backup next hop (routing policy), 103
configuring OSPF FRR backup next hop calculation (LFA algorithm), 103
configuring OSPF FRR BFD, 103
configuring OSPF GR, 98, 123
configuring OSPF GR helper (IETF), 99
configuring OSPF GR helper (non-IETF), 100
configuring OSPF GR restarter, 99
configuring OSPF GR restarter (IETF), 99
configuring OSPF GR restarter (non-IETF), 99
configuring OSPF GTSM, 97
configuring OSPF host route advertisement, 86
configuring OSPF interface cost, 83
configuring OSPF interface network type (broadcast), 79
configuring OSPF interface network type (NBMA), 79
configuring OSPF interface network type (P2MP), 80
configuring OSPF interface network type (P2P), 80
configuring OSPF LSU transmit rate, 94
configuring OSPF network management, 93
configuring OSPF network type, 78
configuring OSPF NSR, 100, 125
configuring OSPF packet DSCP value, 91
configuring OSPF PIC, 95
configuring OSPF PIC BFD, 96
configuring OSPF preference, 84
configuring OSPF prefix priority, 95
configuring OSPF prefix suppression (interface), 95
configuring OSPF prefix suppression (OSPF process), 95
configuring OSPF received route filtering, 82
configuring OSPF redistributed route default parameters, 85
configuring OSPF redistributed route summarization (ASBR), 81
configuring OSPF route control, 81
configuring OSPF route redistribution, 108
configuring OSPF route redistribution (another routing protocol), 85
configuring OSPF route redistribution (default route), 85
configuring OSPF route summarization, 110
configuring OSPF route summarization (ABR), 81
configuring OSPF stub router, 89
configuring OSPF summary network discard route, 84
configuring OSPF Type-3 LSA filtering, 82
configuring OSPF virtual link, 78, 121
configuring OSPFv3, 423
configuring OSPFv3 area parameter, 425
configuring OSPFv3 BFD, 440, 464
configuring OSPFv3 DR election, 452
configuring OSPFv3 FRR, 441, 467
configuring OSPFv3 FRR backup next hop (routing policy), 442
configuring OSPFv3 FRR backup next hop calculation (LFA algorithm), 441
configuring OSPFv3 FRR BFD, 442
configuring OSPFv3 GR, 438, 462
configuring OSPFv3 GR helper, 439
configuring OSPFv3 GR restarter, 438
configuring OSPFv3 Inter-Area-Prefix LSA filtering, 429
configuring OSPFv3 interface cost, 429
configuring OSPFv3 interface DR priority, 434
configuring OSPFv3 IPsec profile, 469
configuring OSPFv3 LSU transmit rate, 436
configuring OSPFv3 NBMA neighbor, 427
configuring OSPFv3 network management, 435
configuring OSPFv3 network type, 426
configuring OSPFv3 network type (interface), 427
configuring OSPFv3 NSR, 439, 463
configuring OSPFv3 NSSA area, 425, 450
configuring OSPFv3 P2MP neighbor, 427
configuring OSPFv3 preference, 430
configuring OSPFv3 prefix suppression (interface), 438
configuring OSPFv3 prefix suppression (OSPFv3 process), 437
configuring OSPFv3 received route filtering, 428
configuring OSPFv3 redistributed route tag, 431
configuring OSPFv3 route control, 427
configuring OSPFv3 route redistribution, 455
configuring OSPFv3 route redistribution (another routing protocol), 431
configuring OSPFv3 route redistribution (default route), 431
configuring OSPFv3 route summarization, 458
configuring OSPFv3 route summarization (ABR), 428
configuring OSPFv3 route summarization (ASBR), 428
configuring OSPFv3 stub area, 425, 445
configuring OSPFv3 stub router, 436
configuring OSPFv3 virtual link, 426
configuring PBR, 375, 377
configuring PBR node action, 375
configuring PBR policy, 375
configuring RIP, 27, 44
configuring RIP additional routing metric, 30
configuring RIP basics, 27, 44
configuring RIP BFD, 41
configuring RIP BFD (bidirectional control detection), 42, 60
configuring RIP BFD (single-hop echo detection/neighbor), 41
configuring RIP BFD (single-hop echo detection/specific destination), 41, 58
configuring RIP BFD single-hop echo detection, 56
configuring RIP FRR, 42, 64
configuring RIP GR, 39
configuring RIP interface additional metric, 49
configuring RIP network management, 38
configuring RIP packet send rate, 38
configuring RIP poison reverse, 34
configuring RIP received/redistributed route filtering, 32
configuring RIP route control, 30
configuring RIP route redistribution, 33
configuring RIP split horizon, 34
configuring RIP summary route advertisement, 51
configuring RIP timers, 33
configuring RIP version, 29
configuring RIPng, 398
configuring RIPng basics, 398, 408
configuring RIPng FRR, 406, 416
configuring RIPng GR, 404, 413
configuring RIPng IPsec profile configuration, 419
configuring RIPng NSR, 405, 414
configuring RIPng packet send rate, 403
configuring RIPng packet zero field check, 402
configuring RIPng poison reverse, 402
configuring RIPng received/redistributed route filtering, 400
configuring RIPng route control, 399
configuring RIPng route redistribution, 401, 411
configuring RIPng route summarization, 399
configuring RIPng routing metric, 399
configuring RIPng split horizon, 402
configuring RIPv2 message authentication, 36
configuring RIPv2 route summarization, 30
configuring routing policy, 510
configuring routing policy (IPv4 route redistribution), 515
configuring routing policy (IPv6 route redistribution), 517
configuring routing policy apply clause, 512
configuring routing policy AS_PATH list, 509
configuring routing policy COMMUNITY list, 509
configuring routing policy continue clause, 514
configuring routing policy extended community list, 510
configuring routing policy filter, 508
configuring routing policy if-match clause, 511
configuring routing policy IPv4 prefix list, 508
configuring routing policy IPv6 prefix list, 509
configuring routing policy MAC list, 510
configuring static route, 9
configuring static route BFD, 10
configuring static route FRR (auto backup next hop), 13
configuring static routing, 14
configuring static routing basics, 14
configuring static routing BFD (direct next hop), 16
configuring static routing BFD (indirect next hop), 18
configuring static routing BFD bidirectional control mode (direct next hop), 10
configuring static routing BFD bidirectional control mode (indirect next hop), 10
configuring static routing BFD single-hop echo mode, 11
configuring static routing default route, 24
configuring static routing FRR, 12, 21
configuring static routing FRR (backup next hop), 13
configuring triggered RIP (TRIP), 37
controlling BGP path selection, 251
controlling BGP route distribution, 237
controlling BGP route reception, 237
controlling IPv6 IS-IS SPF calculation interval, 478
controlling IS-IS SPF calculation interval, 157
controlling RIP interface advertisement, 28
controlling RIP interface reception, 28
creating IPv6 PBR node, 497
creating PBR node, 375
creating routing policy, 510
disabling IPv4 BGP session establishment, 278
disabling IPv6 BGP session establishment, 278
disabling IS-IS interface packet send/receive, 154
disabling OSPF interface packet send/receive, 89
disabling OSPFv3 interface packet send/receive, 434
disabling RIP host route reception, 31
displaying BGP, 303
displaying IP routing table, 7
displaying IPv4 BGP, 303, 303
displaying IPv6 BGP, 303, 303
displaying IPv6 IS-IS, 483
displaying IPv6 PBR, 500
displaying IPv6 static routing, 388
displaying IS-IS, 173
displaying MTR, 522
displaying OSPF, 104
displaying OSPFv3, 444
displaying PBR, 378
displaying RIP, 44
displaying RIPng, 408
displaying routing policy, 514
displaying static routing, 14
enabling BGP, 216
enabling BGP session state change logging, 295
enabling BGP SNMP notification, 295
enabling IP routing EBGP direct connections upon link failure, 273
enabling IPv4 BGP 4-byte AS number suppression, 273
enabling IPv4 BGP load balancing, 275
enabling IPv4 BGP MED AS route comparison (confederation peers), 259
enabling IPv4 BGP MED AS route comparison (diff ASs), 257
enabling IPv4 BGP MED AS route comparison (per-AS), 257
enabling IPv4 BGP multiple hop EBGP session establishment, 272
enabling IPv4 BGP peer MD5 authentication, 274
enabling IPv4 BGP route-refresh, 280
enabling IPv6 BGP 4-byte AS number suppression, 273
enabling IPv6 BGP MED AS route comparison (confederation peers), 259
enabling IPv6 BGP MED AS route comparison (diff ASs), 257
enabling IPv6 BGP MED AS route comparison (per-AS), 257
enabling IPv6 BGP multiple hop EBGP session establishment, 272
enabling IPv6 BGP peer MD5 authentication, 274
enabling IPv6 BGP route-refresh, 280
enabling IPv6 IS-IS automatic link cost calculation, 476
enabling IPv6 IS-IS FRR BFD, 482
enabling IPv6 IS-IS ISPF, 479
enabling IPv6 IS-IS MTR, 482
enabling IPv6 IS-IS prefix suppression, 479
enabling IS-IS, 143
enabling IS-IS automatic cost calculation, 146
enabling IS-IS FRR BFD (control packet mode), 171
enabling IS-IS FRR BFD (echo packet mode), 171
enabling IS-IS interface hello packet send, 154
enabling IS-IS ISPF, 162
enabling IS-IS LSP flash flooding, 156
enabling IS-IS LSP fragment extension, 156
enabling IS-IS neighbor state change logging, 161
enabling IS-IS PIC, 164
enabling IS-IS PIC BFD, 164
enabling IS-IS PPP interface hello packet source address check, 153
enabling IS-IS prefix suppression, 162
enabling OSPF (on interface), 76
enabling OSPF (on network), 75
enabling OSPF ISPF, 94
enabling OSPF neighbor state change logging, 92
enabling OSPF PIC, 96
enabling OSPF RFC 1583 compatibility, 92
enabling OSPFv3, 424
enabling OSPFv3 neighbor state change logging, 435
enabling RIP, 28
enabling RIP FRR BFD, 43
enabling RIP NSR, 40
enabling RIP poison reverse, 34
enabling RIP split horizon, 34
enabling RIP update source IP address check, 35
enabling RIPng FRR BFD, 406
enabling RIPv1 message zero field check, 35
enabling RIPv2 automatic route summarization, 30
enabling static routing FRR BFD echo packet mode, 13
enabling triggered RIP (TRIP), 37
enhancing IS-IS network security, 164
filtering OSPF outbound LSA (interface), 97
filtering OSPF outbound LSAs (specified neighbor), 97
flushing the suboptimal BGP route to the RIB, 286
generating BGP route, 233
ignoring BGP first AS number of EBGP route updates, 267
ignoring IPv4 BGP ORIGINATOR_ID attribute, 291
ignoring IPv6 BGP ORIGINATOR_ID attribute, 291
ignoring OSPFv3 DD packet MTU check, 434
injecting IPv4 BGP local network, 234
injecting IPv6 BGP local network, 234
limiting IPv4 BGP routes received from peer/peer group, 242
limiting IPv6 BGP routes received from peer/peer group, 242
limiting IS-IS LSP flooding, 157
maintaining BGP, 303
maintaining IP routing table, 7
maintaining IPv4 BGP, 303
maintaining IPv6 BGP, 303
maintaining IPv6 PBR, 500
maintaining IS-IS, 173
maintaining OSPF, 104
maintaining OSPFv3, 444
maintaining PBR, 378
maintaining RIP, 44
maintaining RIPng, 408
maintaining routing policy, 514
optimizing BGP network, 269
optimizing IPv6 IS-IS networks, 477
optimizing IS-IS networks, 152
optimizing OSPF network, 86
optimizing OSPFv3 network, 432
optimizing RIP networks, 33
optimizing RIPng network, 401
permitting IPv4 BGP local AS number appearance, 262
permitting IPv6 BGP local AS number appearance, 262
protecting IPv4 EBGP peer (low memory exemption), 285
protecting IPv6 EBGP peer (low memory exemption), 285
redistributing IPv4 BGP IGP routes, 235
redistributing IPv6 BGP IGP routes, 235
removing IPv4 BGP private AS number from EBGP peer/peer group update, 266
removing IPv6 BGP private AS number from EBGP peer/peer group update, 266
resetting IPv4 BGP sessions, 307
resetting IPv6 BGP sessions, 307
saving IPv4 BGP route update, 282
saving IPv6 BGP route update, 282
setting IP routing FIB route max lifetime, 4
setting IP routing RIB label max lifetime, 4
setting IP routing RIB route max lifetime, 4
setting IPv4 BGP received route preferred value, 251
setting IPv6 BGP received route preferred value, 251
setting IPv6 IS-IS LSDB overload bit, 478
setting IPv6 PBR node match criteria, 497
setting IS-IS ATT bit Level-1 LSP, 160
setting IS-IS IS+circuit level, 143
setting IS-IS LSDB overload bit, 159
setting OSPF ECMP routes max, 83
setting OSPF exit overflow interval, 92
setting OSPF log count, 96
setting OSPF LSA transmission delay, 87
setting OSPF LSDB external LSAs max, 91
setting OSPF timer, 86
setting OSPFv3 ECMP route max, 430
setting OSPFv3 LSA generation interval, 433
setting OSPFv3 LSA transmission delay, 432
setting OSPFv3 SPF calculation interval, 433
setting OSPFv3 timer, 432
setting PBR node match criteria, 375
setting RIP ECMP route max number, 35
setting RIP packet max length, 39
setting RIP preference, 32
setting RIP triggered update interval, 36
setting RIPng ECMP route max, 403
setting RIPng preference, 400
setting RIPng timer, 401
setting RIPng triggered update send interval, 403
setting triggered RIP (TRIP) retransmission parameters, 37
specifying BGP TCP connection source address, 232
specifying IS-IS CSNP packet send interval, 153
specifying IS-IS hello multiplier, 152
specifying IS-IS hello packet send interval, 152
specifying IS-IS LSP length, 155
specifying IS-IS preference, 146
specifying OSPF LSA arrival interval, 88
specifying OSPF LSA generation interval, 88
specifying OSPF SPF calculation interval, 88
specifying RIP neighbor, 37
triggering OSPF GR, 100
triggering OSPFv3 GR, 439
doubleooting BGP peer connection state, 371
doubleooting OSPF incorrect routing information, 133
doubleooting OSPF no neighbor relationship established, 133
tuning BGP network, 269
tuning IP routing OSPF network, 86
tuning IP routing RIP networks, 33
tuning IPv6 IS-IS network, 477
tuning IS-IS network, 152
tuning OSPFv3 network, 432
tuning RIPng network, 401
profile
OSPFv3 IPsec profile application, 443
OSPFv3 IPsec profile configuration, 469
protecting
IPv4 EBGP peer (low memory exemption), 285
IPv6 EBGP peer (low memory exemption), 285
protocols and standards
BGP, 213
IP routing dynamic routing protocols, 2
IS-IS, 141
MP-BGP, 213
OSPF, 73
OSPF preference, 84
OSPF RFC 1583 compatibility, 92
OSPFv3, 423
RIP, 26
RIPng, 398
triggered RIP (TRIP), 26
R
rate
OSPFv3 LSU transmit rate, 436
receiving
IPv4 BGP routes received from peer/peer group, 242
IPv6 BGP routes received from peer/peer group, 242
IS-IS interface packet send/receive, 154
OSPF interface packet send/receive disable, 89
OSPF received route filtering, 82
OSPFv3 interface packet send/receive disable, 434
RIPng received/redistributed route filtering, 400
recursion
BGP route recursion, 206, 206
IP routing route recursion, 3
redistributing
BGP route generation, 233
BGP route summarization, 237
IP routing extension attribute redistribution, 4
IP routing RIP route redistribution, 47
IP routing route redistribution, 3
IPv4 BGP IGP routes, 235
IPv4 BGP+IGP route redistribution, 312
IPv6 BGP IGP routes, 235
IS-IS redistributed route filtering, 150
IS-IS route redistribution, 149, 183
OSPF redistributed route default parameters, 85
OSPF route redistribution, 84
OSPF route redistribution configuration, 108
OSPFv3 redistributed route tag, 431
OSPFv3 route redistribution, 430, 455
OSPFv3 route redistribution (another routing protocol), 431
OSPFv3 route redistribution (default route), 431
RIP received/redistributed route filtering, 32
RIP routes, 33
RIPng received/redistributed route filtering, 400
RIPng route redistribution, 401, 411
reflected
BGP route reflector, 207
removing
IPv4 BGP private AS number removal, 266
IPv6 BGP private AS number, 266
resetting
IPv4 BGP sessions, 307
IPv6 BGP sessions, 307
restrictions
RIP FRR configuration, 43, 406
retransmitting
triggered RIP (TRIP) retransmission parameters, 37
RFC 1583 compatibility (OSPF), 92
RIB
flushing the suboptimal BGP route to the RIB, 286
IP routing FIB route max lifetime, 4
IP routing RIB label max lifetime, 4
IP routing RIB route max lifetime, 4
IPv4 NSR configuration, 5
IPv6 NSR configuration, 6
RIP, 397, See also RIPng
additional routing metric configuration, 30
basic configuration, 27, 44
BFD configuration, 41
BFD configuration (bidirectional control detection), 42, 60
BFD configuration (single-hop echo detection/neighbor), 41
BFD configuration (single-hop echo detection/specific destination), 41, 58
BFD single-hop echo detection, 56
configuration, 25, 27, 44
default route advertisement, 31
displaying, 44
ECMP route max number, 35
enabling, 28
FRR BFD enable, 43
FRR configuration, 42, 64
FRR configuration restrictions, 43, 406
GR configuration, 39, 53
GR helper configuration, 39
GR retractor configuration, 39
host route reception disable, 31
interface additional metric configuration, 49
interface advertisement control, 28
interface reception control, 28
IPv6. See RIPng
maintaining, 44
neighbor specification, 37
network management configuration, 38
network optimization, 33
network tuning, 33
NSR configuration, 54
NSR enable, 40
operation, 25
packet max length, 39
packet send rate configuration, 38
poison reverse configuration, 34
poison reverse enable, 34
preference configuration, 32
protocols and standards, 26
received/redistributed route filtering, 32
RIPv1 message zero field check enable, 35
RIPv2 message authentication configuration, 36
RIPv2 route summarization configuration, 30
route control configuration, 30
route entries, 25
route redistribution configuration, 33, 47
routing loop prevention, 25
split horizon configuration, 34
split horizon enable, 34
summary route advertisement configuration, 51
timer configuration, 33
triggered RIP (TRIP), 26
triggered RIP (TRIP) configuration, 37
triggered RIP (TRIP) setting, 37
triggered update interval configuration, 36
update source IP address check, 35
version configuration, 29
versions, 26
RIPng, 397, See also RIP
  basic configuration, 398, 408
  configuration, 397, 398, 408
default route advertisement, 400
display, 408
ECMP route max, 403
FRR BFD enable, 406
FRR configuration, 406, 406, 416
GR configuration, 404, 413
IPsec profile application, 407
IPsec profile configuration, 419
maintain, 408
network optimization, 401
network tuning, 401
NSR configuration, 405, 414
packet, 397
packet send rate configuration, 403
packet zero field check, 402
poison reverse configuration, 402
preference configuration, 400
protocols and standards, 398
received/redistributed route filtering, 400
route control, 399
route entry, 397
route redistribution, 411
route redistribution configuration, 401
route summarization, 399
routing metric configuration, 399
split horizon configuration, 402
timer configuration, 401
triggered update send interval configuration, 403
RIPv1
  message zero field check enable, 35
  protocols and standards, 26
  RIP basic configuration, 27
  RIP configuration, 25, 27, 44
  RIP versions, 26
  version configuration, 29
RIPv2
  automatic route summarization enable, 30
  message authentication configuration, 36
  protocols and standards, 26
  RIP basic configuration, 27
  RIP configuration, 25, 27, 44
  RIP versions, 26
  route summarization configuration, 30
  summary route advertisement, 31
  version configuration, 29
route
BGP default route advertisement to peer/peer group, 241
BGP optimal route advertisement rules, 240
BGP route advertisement rules, 205
BGP route dampening, 207
BGP route filtering policies, 244
BGP route generation, 233
BGP route recursion, 206
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP route reflection,</td>
<td>289</td>
</tr>
<tr>
<td>BGP route reflector,</td>
<td>207</td>
</tr>
<tr>
<td>BGP route selection,</td>
<td>205, 206</td>
</tr>
<tr>
<td>BGP route summarization,</td>
<td>207</td>
</tr>
<tr>
<td>BGP route-refresh message,</td>
<td>200</td>
</tr>
<tr>
<td>IP routing FIB route max lifetime,</td>
<td>4</td>
</tr>
<tr>
<td>IP routing FIB table optimal routes,</td>
<td>1</td>
</tr>
<tr>
<td>IP routing inter-protocol FRR,</td>
<td>6</td>
</tr>
<tr>
<td>IP routing IPv4 RIB inter-protocol FRR,</td>
<td>7</td>
</tr>
<tr>
<td>IP routing IPv6 RIB inter-protocol FRR,</td>
<td>7</td>
</tr>
<tr>
<td>IP routing load sharing,</td>
<td>3</td>
</tr>
<tr>
<td>IP routing RIB label max lifetime,</td>
<td>4</td>
</tr>
<tr>
<td>IP routing RIB NSR,</td>
<td>5</td>
</tr>
<tr>
<td>IP routing RIB max lifetime,</td>
<td>4</td>
</tr>
<tr>
<td>IP routing RIP route redistribution configuration,</td>
<td>47</td>
</tr>
<tr>
<td>IP routing route backup,</td>
<td>3</td>
</tr>
<tr>
<td>IP routing route preference,</td>
<td>2</td>
</tr>
<tr>
<td>IP routing route recursion,</td>
<td>3</td>
</tr>
<tr>
<td>IP routing route redistribution,</td>
<td>3</td>
</tr>
<tr>
<td>IPv4 BGP IGP route redistribution,</td>
<td>235</td>
</tr>
<tr>
<td>IPv4 BGP MED AS route comparison (confederation peers),</td>
<td>259</td>
</tr>
<tr>
<td>IPv4 BGP MED AS route comparison (diff ASs),</td>
<td>257</td>
</tr>
<tr>
<td>IPv4 BGP MED AS route comparison (per-AS),</td>
<td>257</td>
</tr>
<tr>
<td>IPv4 BGP ORIGINATOR_ID attribute,</td>
<td>291</td>
</tr>
<tr>
<td>IPv4 BGP route dampening,</td>
<td>250</td>
</tr>
<tr>
<td>IPv4 BGP route distribution filtering policies,</td>
<td>244</td>
</tr>
<tr>
<td>IPv4 BGP route reception filtering policies,</td>
<td>247</td>
</tr>
<tr>
<td>IPv4 BGP route reflector,</td>
<td>289</td>
</tr>
<tr>
<td>IPv4 BGP route reflector configuration,</td>
<td>324</td>
</tr>
<tr>
<td>IPv4 BGP route refresh,</td>
<td>280</td>
</tr>
<tr>
<td>IPv4 BGP route summarization,</td>
<td>315</td>
</tr>
<tr>
<td>IPv4 BGP route update delay,</td>
<td>250</td>
</tr>
<tr>
<td>IPv4 BGP route update interval,</td>
<td>271</td>
</tr>
<tr>
<td>IPv4 BGP route update save,</td>
<td>282</td>
</tr>
<tr>
<td>IPv4 BGP routes received from peer/peer group,</td>
<td>242</td>
</tr>
<tr>
<td>IPv4 BGP+IGP route redistribution,</td>
<td>312</td>
</tr>
<tr>
<td>IPv6 BGP IGP route redistribution,</td>
<td>235</td>
</tr>
<tr>
<td>IPv6 BGP MED AS route comparison (confederation peers),</td>
<td>259</td>
</tr>
<tr>
<td>IPv6 BGP MED AS route comparison (diff ASs),</td>
<td>257</td>
</tr>
<tr>
<td>IPv6 BGP MED AS route comparison (per-AS),</td>
<td>257</td>
</tr>
<tr>
<td>IPv6 BGP route reflector,</td>
<td>289</td>
</tr>
<tr>
<td>IPv6 BGP route reflector configuration,</td>
<td>350</td>
</tr>
<tr>
<td>IPv6 BGP route refresh,</td>
<td>280</td>
</tr>
<tr>
<td>IPv6 BGP route refresh interval,</td>
<td>271</td>
</tr>
<tr>
<td>IPv6 BGP route update save,</td>
<td>282</td>
</tr>
<tr>
<td>IPv6 BGP routes received from peer/peer group,</td>
<td>242</td>
</tr>
<tr>
<td>IPv6 default route configuration,</td>
<td>396</td>
</tr>
<tr>
<td>IPv6 IS-IS route control,</td>
<td>475</td>
</tr>
<tr>
<td>IPv6 IS-IS route convergence priority,</td>
<td>477</td>
</tr>
<tr>
<td>IPv6 static route BFD configuration,</td>
<td>386</td>
</tr>
<tr>
<td>IPv6 static route BFD control mode (direct next hop),</td>
<td>387</td>
</tr>
<tr>
<td>IPv6 static route BFD control mode (indirect next hop),</td>
<td>387</td>
</tr>
<tr>
<td>IPv6 static route BFD echo mode (single hop),</td>
<td>387</td>
</tr>
<tr>
<td>IPv6 static route configuration,</td>
<td>386</td>
</tr>
<tr>
<td>IPv6 static routing basic configuration,</td>
<td>388</td>
</tr>
<tr>
<td>IPv6 static routing BFD (direct next hop),</td>
<td>390</td>
</tr>
<tr>
<td>IPv6 static routing BFD (indirect next hop),</td>
<td>393</td>
</tr>
<tr>
<td>IPv6 static routing configuration,</td>
<td>386, 388</td>
</tr>
<tr>
<td>IS-IS default route advertisement,</td>
<td>148</td>
</tr>
<tr>
<td>IS-IS ECMP routes max,</td>
<td>147</td>
</tr>
</tbody>
</table>
IS-IS LSP-calculated route filtering, 150
IS-IS redistributed route filtering, 150
IS-IS route control, 144
IS-IS route filtering, 150
IS-IS route leaking, 151, 151
IS-IS route redistribution, 149, 183
IS-IS route summarization, 148
OSPF area configuration (NSSA), 115
OSPF area configuration (stub), 113
OSPF ECMP routes max, 83
OSPF host route advertisement, 86
OSPF preference, 84
OSPF received route filtering, 82
OSPF redistributed route default parameters, 85
OSPF redistributed route summarization (ASBR), 81
OSPF route calculation, 71
OSPF route control, 81
OSPF route level priority, 71
OSPF route redistribution, 84
OSPF route redistribution configuration, 108
OSPF route summarization, 81
OSPF route summarization (ABR), 81
OSPF route summarization configuration, 110
OSPF summary network discard route, 84
OSPFv3 ECMP route max, 430
OSPFv3 received route filtering, 428
OSPFv3 redistributed route tag, 431
OSPFv3 route control, 427
OSPFv3 route redistribution, 430, 455
OSPFv3 route redistribution (another routing protocol), 431
OSPFv3 route redistribution (default route), 431
OSPFv3 route summarization, 428, 458
OSPFv3 route summarization (ASBR), 428
RIP default route advertisement, 31
RIP ECMP route max number, 35
RIP host route reception disable, 31
RIP poison reverse configuration, 34
RIP preference configuration, 32
RIP received/redistributed route filtering, 32
RIP route control configuration, 30
RIP route entries, 25
RIP route redistribution configuration, 33
RIP split horizon configuration, 34
RIP update source IP address check, 35
RIPng default route advertisement, 400
RIPng ECMP route max, 403
RIPng preference, 400
RIPng received/redistributed route filtering, 400
RIPng route control, 399
RIPng route entry, 397
RIPng route redistribution, 401, 411
RIPng route summarization, 399
RIPv1 message zero field check, 35
RIPv2 summary route advertisement, 31
routing policy filters, 507
static routing basic configuration, 14
static routing BFD configuration, 10
static routing BFD configuration (direct next hop), 16
static routing BFD configuration (indirect next hop), 18
static routing configuration, 9, 9, 14
static routing default route configuration, 24
static routing FRR configuration, 12, 21
triggered RIP (TRIP), 26

router
IS-IS interface P2P network type, 144
IS-IS IS+circuit level, 143
IS-IS Level-1 router, 137
IS-IS Level-1-2 router, 137
IS-IS Level-2 router, 137
IS-IS route leaking, 138
IS-IS routing method, 136
IS-IS system ID, 136
OSPF ABR type, 70
OSPF ASBR type, 70
OSPF backbone type, 70
OSPF internal type, 70
OSPF router LSA, 67
OSPF stub router, 89
OSPFv3 stub router, 436
RIPng FRR configuration, 416

Routing
IPv4 BGP load balancing, 275
IPv4 RIB NSR configuration, 5
IPv6 BGP load balancing, 275
IPv6 BGP packet IPsec configuration, 359
IPv6 default route. See under IPv6 static routing
IPv6 IS-IS. See IPv6 IS-IS
IPv6 policy-based routing. See IPv6 PBR
IPv6 RIB NSR configuration, 6
IPv6 static routing. See IPv6 static routing
policy-based routing. Use PBR
tuning BGP network, 269

Routing Information Protocol. Use RIP
rout policy
display, 514
maintain, 514

rule
BGP route advertisement rules, 205

S
saving
IPv4 BGP route update, 282
IPv6 BGP route update, 282

security
BGP GTSM configuration, 279
IPv6 BGP IPsec, 277
IPv6 BGP packet IPsec configuration, 359
IPv6 IS-IS prefix suppression, 479
IS-IS authentication (area), 165

IS-IS authentication (neighbor relationship), 165
IS-IS authentication (routing domain), 166
IS-IS network security enhancement, 164
OSPF authentication (area), 90
OSPF authentication (interface), 90
OSPF prefix priority, 95
OSPF prefix suppression, 94
OSPFv3 IPsec profile configuration, 443
OSPFv3 prefix suppression, 469
OSPFv3 prefix suppression, 437
RIPng IPsec profile configuration, 407
RIPng packet rate, 403

SEL
IS-IS N-SEL, 136
NET, 136

selecting
BGP path selection, 251
BGP route, 205
BGP route selection, 206
IPv4 BGP path selection configuration, 330
multicast BGP configuration, 341, 367

sending
IS-IS CSNP packet send interval, 153
IS-IS hello packet send interval, 152
IS-IS interface hello packet send, 154
IS-IS interface packet send/receive, 154
OSPF interface packet send/receive disable, 89
OSPFv3 interface packet send/receive disable, 434
RIPng packet rate, 403
RIPng triggered update send interval, 403

session
BGP session state change logging, 295
IPv4 BGP multiple hop EBGP session establishment, 272
IPv4 BGP session establishment disable, 278
IPv6 BGP multiple hop EBGP session establishment, 272
IPv6 BGP session establishment disable, 278
setting

- IP routing FIB route max lifetime, 4
- IP routing RIB label max lifetime, 4
- IP routing RIB route max lifetime, 4
- IPv4 BGP received route preferred value, 251
- IPv4 BGP session reset, 307
- IPv6 BGP received route preferred value, 251
- IPv6 BGP session reset, 307
- IPv6 IS-IS LSDB overload bit, 478
- IPv6 PBR node match criteria, 497
- IS-IS ATT bit Level-1 LSP, 160
- IS-IS IS+ circuit level, 143
- IS-IS LSDB overload bit, 159
- OSPF ECMP routes max, 83
- OSPF exit overflow interval, 92
- OSPF log count, 96
- OSPF LSA transmission delay, 87
- OSPF LSDB external LSAs max, 91
- OSPF timer, 86
- OSPFv3 ECMP route max, 430
- OSPFv3 LSA generation interval, 433
- OSPFv3 LSA transmission delay, 432
- OSPFv3 SPF calculation interval, 433
- OSPFv3 timer, 432
- PBR node match criteria, 375
- RIP ECMP route max number, 35
- RIP packet max length, 39
- RIP preference, 32
- RIP triggered update interval, 36
- RIPng ECMP route max, 403
- RIPng preference, 400
- RIPng timer, 401
- RIPng triggered update send interval, 403
- triggered RIP (TRIP) retransmission parameters, 37

SNMP

- BGP SNMP notification enable, 295
- OSPF network management, 93
- SNP IS-IS PDU type, 140

soft reset

- BGP soft reset, 280
- IPv4 BGP manual configuration, 283
- IPv6 BGP manual configuration, 283

SoO

- IPv4 BGP SoO attribute, 268
- IPv6 BGP SoO attribute, 268

source

- IS-IS PPP interface hello packet source address check, 153
- RIP source IP address check, 35

speaker

- BGP, 200

specifying

- BGP TCP connection source address, 232
- IS-IS CSNP packet send interval, 153
- IS-IS hello multiplier, 152
- IS-IS hello packet send interval, 152
- IS-IS LSP length, 155
- IS-IS preference, 146
- OSPF LSA arrival interval, 88
- OSPF LSA generation interval, 88
- OSPF SPF calculation interval, 88
- RIP neighbor, 37

SPF

- IPv6 IS-IS calculation interval, 478
- IS-IS calculation interval, 157
- OSPF SPF calculation interval, 88
- OSPFv3 SPF calculation interval, 433

split horizon, 34, 34

- RIPng configuration, 402

state

- BGP session state change logging, 295
- OSPF neighbor state change logging, 92

static

- IS-IS system ID > host name mapping, 160

routing. See static routing

static routing

- basic configuration, 14
BFD configuration (direct next hop), 16
BFD configuration (indirect next hop), 18
configuration, 9, 14
default route configuration, 24
display, 14
FRR configuration, 21
IPv6. See IPv6 static routing
routing configuration, 9
static routing BFD bidirectional control mode
(direct next hop), 10
static routing BFD bidirectional control mode
(indirect next hop), 10
static routing BFD configuration, 10
static routing BFD single-hop echo mode, 11
static routing FRR configuration, 12
stub
OSPF area configuration, 113
OSPF area configuration (stub), 77
OSPF stub area, 69
OSPF stub router, 89
OSPF totally stub area, 69
OSPFv3 stub area, 425
OSPFv3 stub area configuration, 445
OSPFv3 stub router, 436
substituting
IPv4 BGP AS number substitution, 264
IPv6 BGP AS number substitution, 264
summarizing
BGP route summarization, 207, 237
IPv4 BGP route summarization, 315
IPv4 BGP route summarization
(automatic), 237
IPv4 BGP route summarization (manual), 238
IPv6 BGP route summarization (manual), 238
IS-IS route summarization, 148
OSPF redistributed route summarization
(ASBR), 81
OSPF route summarization, 81
OSPF route summarization (ABR), 81
OSPF route summarization configuration, 110
OSPF summary network discard route, 84
OSPFv3 route summarization, 458
OSPFv3 route summarization (ABR), 428
OSPFv3 route summarization (ASBR), 428
RIPng route summarization, 399
RIPv2 automatic route summarization enable, 30
RIPv2 route summarization configuration, 30
RIPv2 summary route advertisement, 31
suppressing
IPv4 BGP 4-byte AS number suppression, 273
IPv6 BGP 4-byte AS number suppression, 273
IPv6 IS-IS prefix suppression, 479
IS-IS prefix suppression, 162
OSPF prefix suppression, 94
OSPFv3 prefix suppression, 437
RIP suppress timer, 33
switchover
BGP NSR, 294
system
IS-IS system ID, 136
IS-IS system ID > host name mapping, 160
T
table
IP routing, 1
tag
IPv6 IS-IS interface tag value, 478
IS-IS interface tag value, 160
OSPFv3 redistributed route tag, 431
TCP
BGP configuration, 200, 213
BGP TCP connection source address, 232
IPv4 BGP basic configuration, 308
IPv4 BGP BFD configuration, 334
IPv4 BGP COMMUNITY configuration, 321
IPv4 BGP confederation, 326
IPv4 BGP configuration, 308
IPv4 BGP dynamic peer configuration, 345
IPv4 BGP FRR configuration, 338
IPv4 BGP GR configuration, 333
IPv4 BGP load balancing configuration, 318
IPv4 BGP path selection configuration, 330
IPv4 BGP route reflector configuration, 324
IPv4 BGP route summarization, 315
IPv4 BGP+IGP route redistribution, 312
IPv6 BGP basic configuration, 347
IPv6 BGP BFD configuration, 355
IPv6 BGP configuration, 347
IPv6 BGP FRR configuration, 364
IPv6 BGP route reflector configuration, 350
multicast BGP configuration, 341, 367
threshold
IPv4 EBGP peer protection (level 2 threshold exemption), 285
IPv6 EBGP peer protection (level 2 threshold exemption), 285
time
IPv4 BGP hold time, 269
IPv6 BGP hold time, 269
timeout
RIP timeout timer, 33
timer
IS-IS LSP timer configuration, 154
OSPF dead packet, 86
OSPF hello packet, 86
OSPF LSA retransmission packet, 86
OSPF packet, 86
OSPF poll packet, 86
OSPFv3 timer, 432
RIP garbage-collect timer, 33
RIP suppress timer, 33
RIP timeout timer, 33
RIP update timer, 33
RIPng timer configuration, 401
TLV
IPv6 Interface Address, 474
IPv6 IS-IS basic configuration, 484
IPv6 IS-IS BFD configuration, 488
IPv6 IS-IS configuration, 474, 484
IPv6 Reachability, 474
topology
IPv6 default route configuration, 396
IPv6 IS-IS ISPF, 479
IPv6 IS-IS MTR, 482
IPv6 static route configuration, 386
IPv6 static routing basic configuration, 388
IPv6 static routing BFD (direct next hop), 390
IPv6 static routing BFD (indirect next hop), 393
IPv6 static routing configuration, 386, 388
IS-IS ISPF, 162
MTR configuration, 520, 520
Track
IPv6 PBR collaboration, 496
PBR collaboration, 374
static routing configuration, 9
transmitting
OSPFv3 LSU transmit rate, 436
triggered RIP (TRIP) retransmission parameters, 37
trapping
BGP SNMP notification enable, 295
IS-IS network management, 163
OSPF network management, 93, 93
OSPFv3 network management, 435
triggered RIP
protocols and standards, 26
TRIP, 26
triggered RIP (TRIP)
configuration, 37
enabling, 37
retransmission parameters, 37
triggering
OSPF GR, 100
OSPFv3 GR, 439
RIP triggered update interval, 36
RIPng triggered update send interval, 403
troubleshooting
  BGP, 371
  BGP peer connection state, 371
  OSPF configuration, 133
  OSPF incorrect routing information, 133
  OSPF no neighbor relationship established, 133
TTL
  BGP GTSM configuration, 279
tuning
  BGP network, 269
  IPv6 IS-IS network, 477
  IS-IS network, 152
  OSPF network, 86
  OSPFv3 network, 432
  RIP networks, 33
  RIPng network, 401
tunneling
  IPv6 BGP packet IPsec configuration, 359
Type 1 external
  OSPF route type, 71
Type 2 external
  OSPF route type, 71
U
UDP
  RIP configuration, 25, 27, 44
  RIPng basic configuration, 398, 408
  RIPng configuration, 397, 398, 408
  RIPng GR configuration, 404
  RIPng IPsec profile configuration, 419
  RIPng route redistribution, 411
unicast
  BGP dynamic peer, 219
  BGP peer, 217
  IP routing configuration, 1
  IP routing dynamic routing protocols, 2
  IP routing extension attribute redistribution, 4
  IP routing load sharing, 3
IP routing route backup, 3
IP routing route preference, 2
IP routing route recursion, 3
IP routing route redistribution, 3
OSPF network type, 72
updating
  BGP MPLS local label update delay, 286
  BGP update message, 200
  IPv4 BGP route update, 282
  IPv4 BGP route update interval, 271
  IPv6 BGP route update, 282
  IPv6 BGP route update interval, 271
  RIP source IP address check, 35
  RIP triggered update interval, 36
  RIP update timer, 33
  RIPng triggered update send interval, 403
V
value
  BGP received route preferred value, 251
  IPv4 BGP MED default value, 256
  IPv6 BGP MED default value, 256
  IPv6 IS-IS interface tag value, 478
virtual
  OSPF virtual link, 69, 78
  OSPF virtual link configuration, 121
Z
zero field check
  RIPng packet, 402
zero field check (RIPv1), 35