Contents

Configuring OSPFv3

About OSPFv3

This chapter describes how to configure RFC 2740-compliant Open Shortest Path First version 3 (OSPFv3) for an IPv6 network.

Comparison of OSPFv3 with OSPFv2

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.

For more information about OSPFv2, see "Configuring OSPF."

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 2328, *OSPF Version 2*
- RFC 3101, *OSPF Not-So-Stubby Area (NSSA) Option*
- RFC 4552, *Authentication/Confidentiality for OSPFv3*
- RFC 5187, *OSPFv3 Graceful Restart*
- RFC 5329, *Traffic Engineering Extensions to OSPF Version 3*
- RFC 5340, *OSPF for IPv6*
- RFC 5523, *OSPFv3-Based Layer 1 VPN Auto-Discovery*
- RFC 5643, *Management Information Base for OSPFv3*
- RFC 6506, *Supporting Authentication Trailer for OSPFv3*
- RFC 6565, *OSPFv3 as a Provider Edge to Customer Edge (PE-CE) Routing Protocol*
- RFC 6969, *OSPFv3 Instance ID Registry Update*
- RFC 7166, *Supporting Authentication Trailer for OSPFv3*

OSPFv3 tasks at a glance

To configure OSPFv3, perform the following tasks:

1. Enabling OSPFv3
2. (Optional.) Configuring OSPFv3 area parameters
   - Configuring a stub area
   - Configuring an NSSA area
   - Configuring an OSPFv3 virtual link

     Perform this task on an ABR to create a virtual link when connectivity cannot be maintained between a non-backbone area and the backbone, or within the backbone.
3. (Optional.) Configuring OSPFv3 network types
   - Setting the broadcast network type for an OSPFv3 interface
   - Setting the NBMA network type for an OSPFv3 interface
   - Setting the P2MP network type for an OSPFv3 interface

Enabling OSPFv3

About enabling OSPFv3

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.

An OSPFv3 process ID has only local significance. Process 1 on a router can exchange packets with process 2 on another router.

OSPFv3 requires you to manually specify a router ID for each router in an AS. Make sure all assigned router IDs in the AS are unique.

Restrictions and guideline

If a router runs multiple OSPFv3 processes, you must specify a unique router ID for each process.

Procedure

1. Enter system view.

    system-view

2. Enable an OSPFv3 process and enter its view.

    ospfv3 [*process-id* | **vpn-instance** *vpn-instance-name*] *

    By default, no OSPFv3 processes are enabled.

3. Specify a router ID.

    router-id *router-id*

    By default, no router ID is configured.

4. Enter interface view.

    interface *interface-type interface-number*

5. Enable an OSPFv3 process on the interface.

    ospfv3 *process-id* **area** *area-id* [**instance** *instance-id*]

    By default, no OSPFv3 processes are enabled on an interface.

Configuring OSPFv3 area parameters

About OSPFv3 areas

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.

Configuring a stub area

Restrictions and guidelines

To configure a stub area, you must perform this task on all routers attached to the area.

Procedure

1. Enter system view.

    system-view

2. Enter OSPFv3 view.

    ospfv3 [*process-id* | **vpn-instance** *vpn-instance-name*] *

3. Enter OSPFv3 area view.

    area *area-id*

4. Configure the area as a stub area.

    stub [**default-route-advertise-always** | **no-summary**] *

By default, no area is configured as a stub area.

The **no-summary** keyword is only available on the ABR of a stub area. If you specify the **no-summary** keyword, the ABR only advertises a default route in an Inter-Area-Prefix LSA into the stub area.

5. (Optional.) Set a cost for the default route advertised to the stub area.

    default-cost *cost-value*

    By default, the cost for the default route advertised to the stub area is 1.

Configuring an NSSA area

Restrictions and guidelines

To configure an NSSA area, you must perform this task on all routers attached to the area.

Procedure

1. Enter system view.

    system-view

2. Enter OSPFv3 view.

    ospfv3 [*process-id* | **vpn-instance** *vpn-instance-name*] *

3. Enter OSPFv3 area view.

    area *area-id*

4. Configure the area as an NSSA area.

    nssa [**default-route-advertise** [**cost** *cost-value* | **nssa-only** | **route-policy** *route-policy-name* | **tag** *tag* | **type** *type*] * | **no-import-route** | **no-summary** | [**translate-always** | **translate-never**] | **suppress-fa** | **translator-stability-interval** *value*] *

    By default, no area is configured as an NSSA area.

    To configure a totally NSSA area, execute the **nssa no-summary** command on the ABR. The ABR of a totally NSSA area does not advertise inter-area routes into the area.

5. (Optional.) Set a cost for the default route advertised to the NSSA area.

    default-cost *cost-value*

    By default, the cost for the default route advertised to the NSSA area is 1.

    This command takes effect only on the ABR/ASBR of an NSSA or totally NSSA area.

Configuring an OSPFv3 virtual link

About OSPFv3 virtual links

You can configure a virtual link to maintain connectivity between a non-backbone area and the backbone, or in the backbone itself.

Restrictions and guidelines

Both ends of a virtual link are ABRs that must be configured with the **vlink-peer** command.

Procedure

1. Enter system view.

    system-view

2. Enter OSPFv3 view.

    ospfv3 [*process-id* | **vpn-instance** *vpn-instance-name*] *

3. Enter OSPFv3 area view.

   area *area-id*

4. Configure a virtual link.

   vlink-peer *router-id* [**dead** *seconds* | **hello** *seconds* | **instance** *instance-id* | **ipsec-profile** *profile-name* | **retransmit** *seconds* | **trans-delay** *seconds*] *

Configuring OSPFv3 network types

Restrictions and guidelines for OSPFv3 network type configuration

Based on the link layer protocol, OSPFv3 classifies networks into different types, including broadcast, NBMA, P2MP, and P2P.

- If any routers in a broadcast network do not support multicasting, you can change the network type to NBMA.
- If only two routers running OSPFv3 exist on a network segment, you can change the network type to P2P to save costs.

Setting the broadcast network type for an OSPFv3 interface

1. Enter system view.

   system-view

2. Enter interface view.

   interface *interface-type interface-number*

3. Set the network type to broadcast for the OSPFv3 interface.

   ospfv3 network-type broadcast [**instance** *instance-id*]

   By default, the network type of an interface is broadcast.

Setting the NBMA network type for an OSPFv3 interface

Restrictions and guidelines

For NBMA interfaces, you must specify the link-local IP addresses and DR priorities for their neighbors because these interfaces cannot find neighbors by broadcasting hello packets.

Procedure

1. Enter system view.

   system-view

2. Enter interface view.

   interface *interface-type interface-number*

3. Set the network type to NBMA for the OSPFv3 interface.

   ospfv3 network-type nbma [**instance** *instance-id*]

   By default, the network type of an interface is broadcast.

4. (Optional.) Set the router priority for the interface

   ospfv3 dr-priority *priority*

   By default, an interface has a router priority of 1.

An interface's router priority determines its privilege in DR/BDR selection.

5. Specify an NBMA neighbor.

   ospfv3 peer *ipv6-address* [**cost** *cost-value* | **dr-priority** *priority*]
   [**instance** *instance-id*]

   By default, no link-local address is specified for the neighbor interface.

Setting the P2MP network type for an OSPFv3 interface

Restrictions and guidelines

For P2MP interfaces (only when in unicast mode), you must specify the link-local IP addresses of their neighbors because these interfaces cannot find neighbors by broadcasting hello packets.

Procedure

1. Enter system view.

   system-view

2. Enter interface view.

   interface *interface-type interface-number*

3. Set the network type to P2MP for the OSPFv3 interface.

   ospfv3 network-type p2mp [**unicast**] [**instance** *instance-id*]

   By default, the network type of an interface is broadcast.

4. Specify a P2MP unicast neighbor.

   ospfv3 peer *ipv6-address* [**cost** *cost-value* | **dr-priority** *priority*]
   [**instance** *instance-id*]

   By default, no link-local address is specified for the neighbor interface.

Setting the P2P network type for an OSPFv3 interface

1. Enter system view.

   system-view

2. Enter interface view.

   interface *interface-type interface-number*

3. Set the network type to P2P for the OSPFv3 interface.

   ospfv3 network-type p2p [**instance** *instance-id*]

   By default, the network type of an interface is broadcast.

Configuring OSPFv3 route control

Configuring OSPFv3 inter-area route summarization

About OSPFv3 inter-area route summarization

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.

Procedure

1. Enter system view.

```
system-view
```

2. Enter OSPFv3 view.

```
ospfv3 [ process-id | vpn-instance vpn-instance-name ] *
```

3. Enter OSPFv3 area view.

```
area area-id
```

4. Configure route summarization on the ABR.

```
abr-summary ipv6-address prefix-length [ not-advertise ] [ cost
cost-value ]
```

By default, route summarization is not configured on an ABR.

Configuring redistributed route summarization

About redistributed route summarization

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

Procedure

1. Enter system view.

```
system-view
```

2. Enter OSPFv3 view.

```
ospfv3 [ process-id | vpn-instance vpn-instance-name ] *
```

3. Configure route summarization on an ASBR.

```
asbr-summary ipv6-address prefix-length [ cost cost-value |
not-advertise | nssa-only | tag tag ] *
```

By default, route summarization is not configured on an ASBR.

Configuring OSPFv3 received route filtering

About OSPFv3 received route filtering

This task allows you to filter routes calculated by using received LSAs.

Procedure

1. Enter system view.

```
system-view
```

2. Enter OSPFv3 view.

```
ospfv3 [ process-id | vpn-instance vpn-instance-name ] *
```

3. Configure OSPFv3 to filter routes calculated by using received LSAs.

```
filter-policy { ipv6-acl-number [ gateway prefix-list-name ] |
prefix-list prefix-list-name [ gateway prefix-list-name ] | gateway
prefix-list-name | route-policy route-policy-name } import
```

By default, OSPFv3 accepts all routes calculated by using received LSAs.

This command can only filter routes computed by OSPFv3. Only routes not filtered out can be added into the local routing table.

Configuring Inter-Area-Prefix LSA filtering

Restrictions and guidelines

The **filter** command takes effect only on ABRs.

Procedure

1. Enter system view.
   system-view
2. Enter OSPFv3 view.
   ospfv3 [*process-id* | **vpn-instance** *vpn-instance-name*] *
3. Enter OSPFv3 area view.
   area *area-id*
4. Configure OSPFv3 to filter Inter-Area-Prefix LSAs.
   filter { *ipv6-acl-number* | **prefix-list** *prefix-list-name* | **route-policy** *route-policy-name* } { **export** | **import** }

   By default, OSPFv3 accepts all Inter-Area-Prefix LSAs.

Setting an OSPFv3 cost for an interface

About 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.

Setting a cost in interface view

1. Enter system view.
   system-view
2. Enter interface view.
   interface *interface-type interface-number*
3. Set an OSPFv3 cost for the interface.
   ospfv3 cost *cost-value* [**instance** *instance-id*]

   By default, the OSPFv3 cost is 1 for a VLAN interface, is 0 for a loopback interface. The OSPFv3 cost is automatically computed according to the interface bandwidth for other interfaces.

Setting a bandwidth reference value

1. Enter system view.
   system-view
2. Enter OSPFv3 view.

```
ospfv3 [ process-id | vpn-instance vpn-instance-name ] *
```

3. Set a bandwidth reference value.

```
bandwidth-reference value
```

The default bandwidth reference value is 100 Mbps.

Setting the maximum number of OSPFv3 ECMP routes

About OSPFv3 ECMP routes

OSPFv3 might find multiple equal-cost routes to the same destination, which can be used to share the traffic load. This task allows you to set the maximum number of ECMP routes.

Procedure

1. Enter system view.

```
system-view
```

2. Enter OSPFv3 view.

```
ospfv3 [ process-id | vpn-instance vpn-instance-name ] *
```

3. Set the maximum number of ECMP routes.

```
maximum load-balancing number
```

The maximum number of OSPFv3 ECMP routes equals the maximum number of ECMP routes supported by the system.

Setting a preference for OSPFv3

About routing protocol preference

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.

Procedure

1. Enter system view.

```
system-view
```

2. Enter OSPFv3 view.

```
ospfv3 [ process-id | vpn-instance vpn-instance-name ] *
```

3. Set a preference for OSPFv3.

```
preference [ ase ] { preference | route-policy route-policy-name } *
```

By default, the preference of OSPFv3 internal routes is 10, and the preference of OSPFv3 external routes is 150.

Configuring OSPFv3 route redistribution

Restrictions and guidelines

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.

Procedure

1. Enter system view.

```
system-view
```

2. Enter OSPFv3 view.

ospfv3 [*process-id* | **vpn-instance** *vpn-instance-name*] *

3. Configure OSPFv3 to redistribute routes from other routing protocols.

import-route bgp4+ [*as-number*] [**allow-ibgp**] [**cost** *cost-value* | **nssa-only** | **route-policy** *route-policy-name* | **tag** *tag* | **type** *type*] *

import-route { **direct** | **static** } [**cost** *cost-value* | **nssa-only** | **route-policy** *route-policy-name* | **tag** *tag* | **type** *type*] *

import-route { **isisv6** | **ospfv3** | **ripng** } [*process-id* | **all-processes**]

By default, route redistribution is disabled.

The **import-route bgp4+** command redistributes only EBGP routes. The **import-route bgp4+ allow-ibgp** command redistributes both EBGP and IBGP routes, which might cause routing loops. There, use the **import-route bgp4+ allow-ibgp** command with caution.

4. (Optional.) Configure OSPFv3 to filter redistributed routes.

filter-policy { *ipv6-acl-number* | **prefix-list** *prefix-list-name* } **export** [*protocol* [*process-id*]]

By default, OSPFv3 accepts all redistributed routes.

This command filters only routes redistributed by the **import-route** command. If no routes are redistributed by the **import-route** command, this command does not take effect.

5. Set a tag for redistributed routes.

default tag *tag*

By default, the tag of redistributed routes is 1.

Configuring default route redistribution

About default route redistribution

The **import-route** command cannot redistribute a default external route. To redistribute a default route, perform this task.

Procedure

1. Enter system view.

system-view

2. Enter OSPFv3 view.

ospfv3 [*process-id* | **vpn-instance** *vpn-instance-name*] *

3. Redistribute a default route.

default-route-advertise [[**always** | **permit-calculate-other**] | **cost** *cost-value* | **route-policy** *route-policy-name* | **tag** *tag* | **type** *type*] *

By default, no default route is redistributed.

4. Set a tag for redistributed routes.

default tag *tag*

By default, the tag of redistributed routes is 1.

Setting OSPFv3 timers

Setting OSPFv3 packet timers

1. Enter system view.

```
system-view
```

2. Enter interface view.

   interface *interface-type interface-number*

3. Set the hello interval.

   ospfv3 timer hello *seconds* [**instance** *instance-id*]

   The default hello interval on P2P and broadcast interfaces is 10 seconds. The default hello interval on P2MP and NBMA interfaces is 30 seconds.

4. Set the dead interval.

   ospfv3 timer dead *seconds* [**instance** *instance-id*]

   The default dead interval on P2P and broadcast interfaces is 40 seconds. The default dead interval on P2MP and NBMA interfaces is 120 seconds.

   The dead interval set on neighboring interfaces cannot be too short. If the interval is too short, a neighbor is easily down.

5. Set the poll interval.

   ospfv3 timer poll *seconds* [**instance** *instance-id*]

   By default, the poll interval is 120 seconds.

6. Set the LSA retransmission interval.

   ospfv3 timer retransmit *interval* [**instance** *instance-id*]

   The default LSA retransmission interval is 5 seconds.

   The LSA retransmission interval cannot be too short. If the interval is too short, unnecessary retransmissions will occur.

Setting LSA transmission delay

About 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.

Procedure

1. Enter system view.

   ```
   system-view
   ```

2. Enter interface view.

   interface *interface-type interface-number*

3. Set the LSA transmission delay.

   ospfv3 trans-delay *seconds* [**instance** *instance-id*]

   By default, the LSA transmission delay is 1 second.

Setting SPF calculation interval

About 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.

Procedure

1. Enter system view.

   system-view

2. Enter OSPFv3 view.

   ospfv3 [*process-id* | **vpn-instance** *vpn-instance-name*] *

3. Set the SPF calculation interval.

   spf-schedule-interval *maximum-interval* [*minimum-interval* [*incremental-interval*]]

   By default, the maximum interval is 5 seconds, the minimum interval is 50 milliseconds, and the incremental interval is 200 milliseconds.

Setting the LSA generation interval

About 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 $\times 2^{n-2}$ for each generation until the maximum interval is reached. The value *n* is the number of generation times.

Procedure

1. Enter system view.

   system-view

2. Enter OSPFv3 view.

   ospfv3 [*process-id* | **vpn-instance** *vpn-instance-name*] *

3. Set the LSA generation interval.

   lsa-generation-interval *maximum-interval* [*minimum-interval* [*incremental-interval*]]

   By default, the maximum interval is 5 seconds, the minimum interval is 0 milliseconds, and the incremental interval is 0 milliseconds.

Setting the LSU transmit rate

About 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.

Procedure

1. Enter system view.

   system-view

2. Enter OSPFv3 view.

   ospfv3 [*process-id* | **vpn-instance** *vpn-instance-name*] *

3. Set the LSU transmit rate.

   transmit-pacing interval *interval* **count** *count*

   By default, an OSPFv3 interface sends a maximum of three LSU packets every 20 milliseconds.

Setting a DR priority for an interface

About DR priority

The router priority is used for DR election. Interfaces having the priority 0 cannot become a DR or BDR.

Procedure

1. Enter system view.

   system-view

2. Enter interface view.

   interface *interface-type interface-number*

3. Set a router priority.

   ospfv3 dr-priority *priority* [**instance** *instance-id*]

   The default router priority is 1.

Configuring OSPFv3 packet parameters

Ignoring MTU check for DD packets

About 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.

Restrictions and guidelines

A neighbor relationship can be established only if the interface's MTU is the same as that of the peer.

Procedure

1. Enter system view.

   system-view

2. Enter interface view.

   interface *interface-type interface-number*

3. Ignore MTU check for DD packets.

   ospfv3 mtu-ignore [**instance** *instance-id*]

   By default, OSPFv3 does not ignore MTU check for DD packets.

Disabling interfaces from receiving and sending OSPFv3 packets

About 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.

Procedure

1. Enter system view.

   system-view

2. Enter OSPFv3 view.

```
ospfv3 [ process-id | vpn-instance vpn-instance-name ] *
```

3. Disable interfaces from receiving and sending OSPFv3 packets.

```
silent-interface { interface-type interface-number | all }
```

By default, the interfaces can receive and send OSPFv3 packets.

This command disables only the interfaces that run the current process. However, multiple OSPFv3 processes can disable the same interface from receiving and sending OSPFv3 packets.

Configuring prefix suppression

About 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.

Restrictions and guidelines for prefix suppression

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

1. Enter system view.

```
system-view
```

2. Enter OSPFv3 view.

```
ospfv3 [ process-id | vpn-instance vpn-instance-name ] *
```

3. Enable prefix suppression for the OSPFv3 process.

```
prefix-suppression
```

By default, prefix suppression is disabled for an OSPFv3 process.

Enabling prefix suppression for an OSPFv3 process does not suppress the prefixes of loopback interfaces and passive interfaces.

Configuring prefix suppression for an interface

1. Enter system view.

```
system-view
```

2. Enter interface view.

```
interface interface-type interface-number
```

3. Enable prefix suppression for the interface.

```
ospfv3 prefix-suppression [ disable ] [ instance instance-id ]
```
By default, prefix suppression is disabled for an interface.

Configuring a stub router

About 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.

Procedure

1. Enter system view.
   ```
   system-view
   ```
2. Enter OSPFv3 view.
   ```
   ospfv3 [ process-id | vpn-instance vpn-instance-name ] *
   ```
3. Configure the router as a stub router.
   - Configure the router as a stub router and clear the R-bit of the Option field in Type-1 LSAs.
     ```
     stub-router r-bit [ include-stub | on-startup { seconds |
     wait-for-bgp [ seconds ] } ] *
     ```
   - Configure the router as a stub router and advertise the locally generated Type-1 LSAs with the maximum cost of 65535.
     ```
     stub-router max-metric [ external-lsa [ max-metric-value ] |
     summary-lsa [ max-metric-value ] | include-stub | on-startup
     { seconds | wait-for-bgp [ seconds ] } ] *
     ```
   By default, the router is not configured as a stub router.

   A stub router is not related to a stub area.

Configuring OSPFv3 GR

About 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.

Restrictions and guidelines for OSPFv3 GR

You cannot enable OSPFv3 NSR on a device that acts as GR restarter.

Configuring GR restarter

1. Enter system view.
   system-view
2. Enter OSPFv3 view.
   ospfv3 [*process-id* | **vpn-instance** *vpn-instance-name*] *
3. Enable the GR capability.
   graceful-restart enable [**global** | **planned-only**] *
   By default, OSPFv3 GR restarter capability is disabled.
4. (Optional.) Set the GR interval.
   graceful-restart interval *interval*
   By default, the GR interval is 120 seconds.

Configuring GR helper

1. Enter system view.
   system-view
2. Enter OSPFv3 view.
   ospfv3 [*process-id* | **vpn-instance** *vpn-instance-name*] *
3. Enable the GR helper capability.
   graceful-restart helper enable [**planned-only**]
   By default, the GR helper capability is enabled.
4. Enable strict LSA checking.
   graceful-restart helper strict-lsa-checking
   By default, strict LSA checking is disabled.

Triggering OSPFv3 GR

About triggering OSPFv3 GR

OSPFv3 GR is triggered by an active/standby switchover or when this task is performed.

Procedure

To trigger OSPFv3 GR, execute the **reset ospfv3** [*process-id*] **process graceful-restart** command in user view.

Configuring OSPFv3 NSR

About OSPFv3 NSR

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.

Restrictions and guidelines

A device that has OSPFv3 NSR enabled cannot act as GR restarter.

Procedure

1. Enter system view.

   system-view

2. Enter OSPFv3 view.

   ospfv3 [*process-id* | **vpn-instance** *vpn-instance-name*] *

3. Enable OSPFv3 NSR.

   non-stop-routing

   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.

Configuring BFD for OSPFv3

About 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.

Procedure

1. Enter system view.

   system-view

2. Enter OSPFv3 view.

   ospfv3 [*process-id* | **vpn-instance** *vpn-instance-name*] *

3. Specify a router ID.

   router-id *router-id*

4. Quit the OSPFv3 view.

   quit

5. Enter interface view.

   interface *interface-type interface-number*

6. Enable an OSPFv3 process on the interface.

   ospfv3 *process-id* **area** *area-id* [**instance** *instance-id*]

7. Enable BFD on the interface.

   ospfv3 bfd enable [**instance** *instance-id*]

   By default, BFD is disabled on the OSPFv3 interface.

Configuring OSPFv3 FRR

About 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 1 Network diagram for OSPFv3 FRR
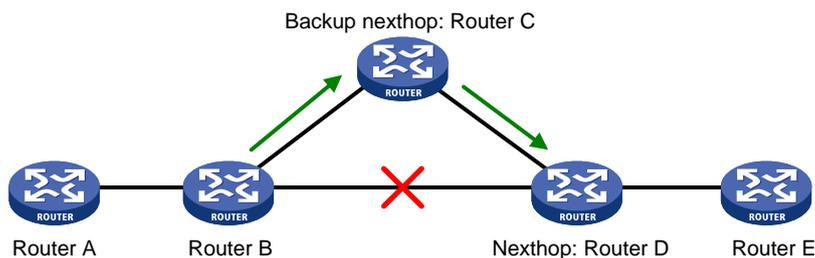
As shown in Figure 1, configure FRR on Router B. OSPFv3 FRR automatically calculates a backup next hop or specifies a backup next hop by using a routing policy. When the primary link fails, OSPFv3 directs packets to the backup next hop. At the same time, OSPFv3 calculates the shortest path based on the 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.

Configuring OSPFv3 FRR to use the LFA algorithm to calculate a backup next hop

Restrictions and guidelines

Do not use the **fast-reroute lfa** command together with the **vlink-peer** command.

Procedure

1. Enter system view.

   system-view

2. Enter interface view.

   interface *interface-type interface-number*

3. (Optional.) Disable LFA on an interface.

   ospfv3 fast-reroute lfa-backup exclude

   By default, the interface on which LFA is enabled can be selected as a backup interface.

4. Return to system view.

   quit

5. Enter OSPFv3 view.

   ospfv3 [*process-id* | **vpn-instance** *vpn-instance-name*] *

6. Enable OSPFv3 FRR to use the LFA algorithm to calculate a backup next hop.

   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 use a backup next hop in a routing policy

About configuring a backup next hop in 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."

Procedure

1. Enter system view.

   system-view

2. Enter interface view.

   interface *interface-type interface-number*

3. (Optional.) Disable LFA on an interface.

   ospfv3 fast-reroute lfa-backup exclude

   By default, the interface is enabled with LFA and it can be selected as a backup interface.

4. Return to system view.

   quit

5. Enter OSPFv3 view.

   ospfv3 [*process-id* | **vpn-instance** *vpn-instance-name*] *

6. Configure OSPFv3 FRR to use a backup next hop in a routing policy.

   fast-reroute route-policy *route-policy-name*

   By default, OSPFv3 FRR is disabled.

Configuring BFD control packet mode for OSPFv3 FRR

About BFD control packet mode for OSPFv3 FRR

By default, OSPFv3 FRR does not use BFD to detect primary link failures. To speed up OSPFv3 convergence, enable BFD control packet mode for OSPFv3 FRR to detect primary link failures. This mode requires BFD configuration on both OSPFv3 routers on the link.

Procedure

1. Enter system view.

   system-view

2. Enter interface view.

   interface *interface-type interface-number*

3. Enable BFD control packet mode for OSPFv3 FRR.

   ospfv3 primary-path-detect bfd ctrl [**instance** *instance-id*]

By default, BFD control packet mode is disabled for OSPFv3 FRR.

Configuring BFD echo packet mode for OSPFv3 FRR

About BFD echo packet mode for OSPFv3 FRR

By default, OSPFv3 FRR does not use BFD to detect primary link failures. To speed up OSPFv3 convergence, enable BFD echo packet mode for OSPFv3 FRR to detect primary link failures. This mode requires BFD configuration on one OSPFv3 router on the link.

Procedure

1. Enter system view.

   `system-view`

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 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`*

4. Enable BFD echo packet mode for OSPFv3 FRR.

   `ospfv3 primary-path-detect bfd echo` [**`instance`** *`instance-id`*]

   By default, BFD echo packet mode is disabled for OSPFv3 FRR.

Applying an IPsec profile for authenticating OSPFv3 packets

About applying an IPsec profile for authenticating OSPFv3 packets

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.

Restrictions and guidelines for applying an IPsec profile

You can configure an IPsec profile for an area, an interface, or a virtual 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.

- 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.

Applying an IPsec profile to an area

1. Enter system view.
   system-view
2. Enter OSPFv3 view.
   ospfv3 [*process-id* | **vpn-instance** *vpn-instance-name*] *
3. Enter OSPFv3 area view.
   area *area-id*
4. Apply an IPsec profile to the area.
   enable ipsec-profile *profile-name*
   By default, no IPsec profile is applied.

Applying an IPsec profile to an interface

1. Enter system view.
   system-view
2. Enter interface view.
   interface *interface-type interface-number*
3. Apply an IPsec profile to the interface.
   ospfv3 ipsec-profile *profile-name*
   By default, no IPsec profile is applied.

Applying an IPsec profile to a virtual link

1. Enter system view.
   system-view
2. Enter OSPFv3 view.
   ospfv3 [*process-id* | **vpn-instance** *vpn-instance-name*] *
3. Enter OSPFv3 area view.
   area *area-id*
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.

Configuring OSPFv3 logging and SNMP notifications

Enabling logging for neighbor state changes

About neighbor state change logging

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*.

Procedure

1. Enter system view.

   system-view

2. Enter OSPFv3 view.

   ospfv3 [*process-id* | **vpn-instance** *vpn-instance-name*] *

3. Enable logging for neighbor state changes.

   log-peer-change

   By default, this feature is enabled.

Setting the maximum number of OSPFv3 logs

About OSPFv3 logs

OSPFv3 logs include route calculation logs, neighbor logs, and LSA aging logs.

Procedure

1. Enter system view.

   system-view

2. Enter OSPFv3 view.

   ospfv3 [*process-id* | **vpn-instance** *vpn-instance-name*] *

3. Set the maximum number of OSPFv3 logs.

   event-log { **lsa-flush** | **peer** | **spf** } **size** *count*

   By default, the maximum number of LSA aging logs, neighbor logs, or route calculation logs is 10.

Configuring OSPFv3 network management

About 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.

Procedure

1. Enter system view.

   system-view

2. Bind MIB to an OSPFv3 process.

   ospfv3 mib-binding *process-id*

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

3. Enable SNMP notifications for OSPFv3.

   snmp-agent trap enable ospfv3 [**grrestarter-status-change** | **grhelper-status-change** | **if-state-change** | **if-cfg-error** | **if-bad-pkt** | **neighbor-state-change** | **nssatranslator-status-change** | **virtif-bad-pkt** | **virtif-cfg-error** | **virtif-state-change** | **virtgrhelper-status-change** | **virtneighbor-state-change**]*

   By default, SNMP notifications for OSPFv3 are enabled.

4. Enter OSPFv3 view.

   ospfv3 [*process-id* | **vpn-instance** *vpn-instance-name*] *

5. Configure an SNMP context for the OSPFv3 process.

   snmp context-name *context-name*

   By default, no SNMP context is configured for the OSPFv3 process.

6. (Optional.) Set the SNMP notification output interval and the maximum number of SNMP notifications that can be output at each interval.

   snmp trap rate-limit interval *trap-interval* **count** *trap-number*

   By default, OSPFv3 outputs a maximum of seven SNMP notifications within 10 seconds.

Display and maintenance commands for OSPFv3

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

Task	Command
Display summary route information on the OSPFv3 ABR.	**display ospfv3** [*process-id*] [**area** *area-id*] **abr-summary** [*ipv6-address prefix-length*] [**verbose**]
Display OSPFv3 neighbor information.	**display ospfv3** [*process-id*] [**area** *area-id*] **peer** [[*interface-type interface-number*] [**verbose**]	*peer-router-id*	**statistics**]
Display OSPFv3 request list information.	**display ospfv3** [*process-id*] [**area** *area-id*] **request-queue** [*interface-type interface-number*] [*neighbor-id*]
Display OSPFv3 retransmission list information.	**display ospfv3** [*process-id*] [**area** *area-id*] **retrans-queue** [*interface-type*

Task	Command
	interface-number] [*neighbor-id*]
Display OSPFv3 topology information.	**display ospfv3** [*process-id*] [**area** *area-id*] **spf-tree** [**verbose**]
Display OSPFv3 process information.	**display ospfv3** [*process-id*] [**verbose**]
Display information about the routes to OSPFv3 ABR and ASBR.	**display ospfv3** [*process-id*] **abr-asbr**
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** { **lsa-flush** │ **peer** │ **spf** }
Display OSPFv3 GR information.	**display ospfv3** [*process-id*] **graceful-restart** [**verbose**]
Display OSPFv3 interface information.	**display ospfv3** [*process-id*] **interface** [*interface-type interface-number* │ **verbose**]
Display OSPFv3 LSDB information.	**display ospfv3** [*process-id*] **lsdb** [{ **external** │ **grace** │ **inter-prefix** │ **inter-router** │ **intra-prefix** │ **link** │ **network** │ **nssa** │ **router** │ **unknown** [*type*] } [*link-state-id*] [**originate-router** *router-id* │ **self-originate**] │ **statistics** │ **total** │ **verbose**]
Display OSPFv3 next hop information.	**display ospfv3** [*process-id*] **nexthop**
Display OSPFv3 NSR information.	**display ospfv3** [*process-id*] **non-stop-routing**
Display OSPFv3 routing information.	**display ospfv3** [*process-id*] **routing** [*ipv6-address prefix-length*]
Display OSPFv3 statistics.	**display ospfv3** [*process-id*] **statistics** [**error**]
Display OSPFv3 virtual link information.	**display ospfv3** [*process-id*] **vlink**
Clear OSPFv3 log information.	**reset ospfv3** [*process-id*] **event-log** [**lsa-flush** │ **peer** │ **spf**]
Restart an OSPFv3 process.	**reset ospfv3** [*process-id*] **process** [**graceful-restart**]
Restart OSPFv3 route redistribution.	**reset ospfv3** [*process-id*] **redistribution**
Clear OSPFv3 statistics.	**reset ospfv3** [*process-id*] **statistics**

OSPFv3 configuration examples

Example: Configuring OSPFv3 stub area

Network configuration

As shown in Figure 2:

● Enable OSPFv3 on all switches.

● Split the AS into three areas.

● Configure Switch B and Switch 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.

Figure 2 Network diagram
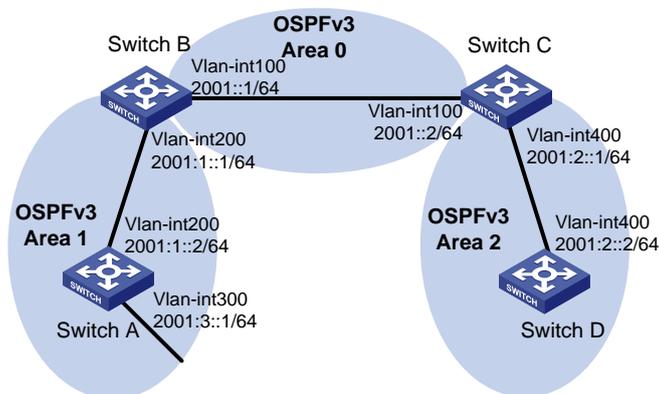
Procedure

1. Configure IPv6 addresses for interfaces. (Details not shown.)
2. Configure basic OSPFv3:

    # On Switch A, enable OSPFv3 and specify the router ID as 1.1.1.1.

    ```
    <SwitchA> system-view
    [SwitchA] ospfv3
    [SwitchA-ospfv3-1] router-id 1.1.1.1
    [SwitchA-ospfv3-1] quit
    [SwitchA] interface vlan-interface 300
    [SwitchA-Vlan-interface300] ospfv3 1 area 1
    [SwitchA-Vlan-interface300] quit
    [SwitchA] interface vlan-interface 200
    [SwitchA-Vlan-interface200] ospfv3 1 area 1
    [SwitchA-Vlan-interface200] quit
    ```

    # On Switch B, enable OSPFv3 and specify the router ID as 2.2.2.2.

    ```
    <SwitchB> system-view
    [SwitchB] ospfv3
    [SwitchB-ospfv3-1] router-id 2.2.2.2
    [SwitchB-ospfv3-1] quit
    [SwitchB] interface vlan-interface 100
    [SwitchB-Vlan-interface100] ospfv3 1 area 0
    [SwitchB-Vlan-interface100] quit
    ```

```
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] ospfv3 1 area 1
[SwitchB-Vlan-interface200] quit
```
On Switch C, enable OSPFv3 and specify the router ID as 3.3.3.3.
```
<SwitchC> system-view
[SwitchC] ospfv3
[SwitchC-ospfv3-1] router-id 3.3.3.3
[SwitchC-ospfv3-1] quit
[SwitchC] interface vlan-interface 100
[SwitchC-Vlan-interface100] ospfv3 1 area 0
[SwitchC-Vlan-interface100] quit
[SwitchC] interface vlan-interface 400
[SwitchC-Vlan-interface400] ospfv3 1 area 2
[SwitchC-Vlan-interface400] quit
```
On Switch D, enable OSPFv3 and specify the router ID as 4.4.4.4.
```
<SwitchD> system-view
[SwitchD] ospfv3
[SwitchD-ospfv3-1] router-id 4.4.4.4
[SwitchD-ospfv3-1] quit
[SwitchD] interface vlan-interface 400
[SwitchD-Vlan-interface400] ospfv3 1 area 2
[SwitchD-Vlan-interface400] quit
```
Display OSPFv3 neighbors on Switch B.
```
[SwitchB] display ospfv3 peer


              OSPFv3 Process 1 with Router ID 2.2.2.2


 Area: 0.0.0.0
 -------------------------------------------------------------------------
 Router ID       Pri State            Dead-Time InstID Interface
 3.3.3.3         1   Full/BDR         00:00:40  0      Vlan100


 Area: 0.0.0.1
 -------------------------------------------------------------------------
 Router ID       Pri State            Dead-Time InstID Interface
 1.1.1.1         1   Full/DR          00:00:40  0      Vlan200
```
Display OSPFv3 neighbors on Switch C.
```
[SwitchC] display ospfv3 peer


              OSPFv3 Process 1 with Router ID 3.3.3.3


 Area: 0.0.0.0
 -------------------------------------------------------------------------
 Router ID       Pri State            Dead-Time InstID Interface
 2.2.2.2         1   Full/DR          00:00:40  0      Vlan100


 Area: 0.0.0.2
 -------------------------------------------------------------------------
```

```
  Router ID       Pri State           Dead-Time InstID Interface
  4.4.4.4          1   Full/BDR        00:00:40   0      Vlan400
```

Display OSPFv3 routing table information on Switch D.

```
[SwitchD] 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: 2001::/64
  Type      : IA                               Cost     : 2
  NextHop   : FE80::F40D:0:93D0:1              Interface: Vlan400
  AdvRouter : 3.3.3.3                          Area     : 0.0.0.2
  Preference : 10

 *Destination: 2001:1::/64
  Type      : IA                               Cost     : 3
  NextHop   : FE80::F40D:0:93D0:1              Interface: Vlan400
  AdvRouter : 3.3.3.3                          Area     : 0.0.0.2
  Preference : 10

 *Destination: 2001:2::/64
  Type      : I                                Cost     : 1
  Nexthop   : ::                               Interface: Vlan400
  AdvRouter : 4.4.4.4                          Area     : 0.0.0.2
  Preference : 10

 *Destination: 2001:3::/64
  Type      : IA                               Cost     : 4
  NextHop   : FE80::F40D:0:93D0:1              Interface: Vlan400
  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 Switch D.

```
[SwitchD] ospfv3
[SwitchD-ospfv3-1] area 2
[SwitchD-ospfv3-1-area-0.0.0.2] stub
```

Configure Switch C, and specify the cost of the default route sent to the stub area as 10.

```
[SwitchC] ospfv3
[SwitchC-ospfv3-1] area 2
[SwitchC-ospfv3-1-area-0.0.0.2] stub
[SwitchC-ospfv3-1-area-0.0.0.2] default-cost 10
```

Display OSPFv3 routing table information on Switch D.

```
[SwitchD] 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::F40D:0:93D0:1                   Interface: Vlan400
    AdvRouter  : 4.4.4.4                               Area     : 0.0.0.2
    Preference : 10


   *Destination: 2001::/64
    Type       : IA                                    Cost     : 2
    NextHop    : FE80::F40D:0:93D0:1                   Interface: Vlan400
    AdvRouter  : 3.3.3.3                               Area     : 0.0.0.2
    Preference : 10


   *Destination: 2001:1::/64
    Type       : IA                                    Cost     : 3
    NextHop    : FE80::F40D:0:93D0:1                   Interface: Vlan400
    AdvRouter  : 3.3.3.3                               Area     : 0.0.0.2
    Preference : 10


   *Destination: 2001:2::/64
    Type       : I                                     Cost     : 1
    Nexthop    : ::                                    Interface: Vlan400
    AdvRouter  : 4.4.4.4                               Area     : 0.0.0.2
    Preference : 10


   *Destination: 2001:3::/64
    Type       : IA                                    Cost     : 4
    NextHop    : FE80::F40D:0:93D0:1                   Interface: Vlan400
    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:

Configure Area 2 as a totally stub area on Switch C.

```
[SwitchC-ospfv3-1-area-0.0.0.2] stub no-summary
```

Display OSPFv3 routing table information on Switch D.

```
[SwitchD] 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::F40D:0:93D0:1                       Interface: Vlan400
      AdvRouter  : 4.4.4.4                                   Area    : 0.0.0.2
      Preference : 10


     *Destination: 2001:2::/64
      Type       : I                                        Cost    : 1
      Nexthop    : ::                                        Interface: Vlan400
      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.

Example: Configuring OSPFv3 NSSA area

Network configuration

As shown in Figure 3:

- Configure OSPFv3 on all switches and split the AS into three areas.
- Configure Switch B and Switch C as ABRs to forward routing information between areas.
- Configure Area 1 as an NSSA area and configure Switch A as an ASBR to redistribute static routes into the AS.

Figure 3 Network diagram
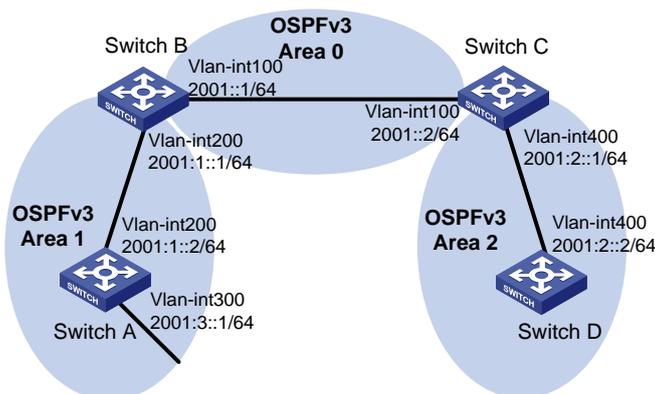
Procedure

1. Configure IPv6 addresses for interfaces. (Details not shown.)
2. Configure basic OSPFv3 (see "Example: Configuring OSPFv3 stub area").

3. Configure Area 1 as an NSSA area:

Configure Switch A.

```
[SwitchA] ospfv3
[SwitchA-ospfv3-1] area 1
[SwitchA-ospfv3-1-area-0.0.0.1] nssa
[SwitchA-ospfv3-1-area-0.0.0.1] quit
[SwitchA-ospfv3-1] quit
```

Configure Switch B.

```
[SwitchB] ospfv3
[SwitchB-ospfv3-1] area 1
[SwitchB-ospfv3-1-area-0.0.0.1] nssa
[SwitchB-ospfv3-1-area-0.0.0.1] quit
[SwitchB-ospfv3-1] quit
```

Display OSPFv3 routing information on Switch A.

```
[SwitchA] display ospfv3 1 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::20C:29FF:FE74:59C6        Interface: Vlan200
  AdvRouter   : 2.2.2.2                         Area      : 0.0.0.1
  Preference  : 10


 *Destination: 2001:1::/64
  Type        : I                              Cost      : 1
  Nexthop     : ::                             Interface: Vlan200
  AdvRouter   : 1.1.1.1                         Area      : 0.0.0.1
  Preference  : 10


 *Destination: 2001:2::/64
  Type        : IA                             Cost      : 3
  NextHop     : FE80::20C:29FF:FE74:59C6        Interface: Vlan200
  AdvRouter   : 2.2.2.2                         Area      : 0.0.0.1
  Preference  : 10


 Total: 3
 Intra area: 1         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 Switch A.

```
[SwitchA] ipv6 route-static 1234:: 64 null 0
[SwitchA] ospfv3 1
[SwitchA-ospfv3-1] import-route static
```

```
[SwitchA-ospfv3-1] quit
```

Display OSPFv3 routing information on Switch D.

```
[SwitchD] display ospfv3 1 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::20C:29FF:FEB9:F2EF        Interface: Vlan400
  AdvRouter : 3.3.3.3                         Area      : 0.0.0.2
  Preference : 10


 *Destination: 2001:1::/64
  Type      : IA                              Cost      : 3
  NextHop   : FE80::20C:29FF:FEB9:F2EF        Interface: Vlan400
  AdvRouter : 3.3.3.3                         Area      : 0.0.0.2
  Preference : 10


 *Destination: 2001:2::/64
  Type      : I                               Cost      : 1
  NextHop   : ::                              Interface: Vlan400
  AdvRouter : 4.4.4.4                         Area      : 0.0.0.2
  Preference : 10


 *Destination: 1234::/64
  Type      : E2                              Cost      : 1
  NextHop   : FE80::20C:29FF:FEB9:F2EF        Interface: Vlan400
  AdvRouter : 2.2.2.2                         Area      : 0.0.0.2
  Preference : 10


 Total: 4
 Intra area: 1        Inter area: 2        ASE: 1         NSSA: 0
```

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

Example: Configuring OSPFv3 DR election

Network configuration

As shown in Figure 4:

- Configure router priority 100 for Switch A, the highest priority on the network, so it will become the DR.
- Configure router priority 2 for Switch C, the second highest priority on the network, so it will become the BDR.
- Configure router priority 0 for Switch B, so it cannot become a DR or BDR.
- Switch D uses the default router priority 1.

Figure 4 Network diagram

Procedure

1. Configure IPv6 addresses for interfaces. (Details not shown.)
2. Configure basic OSPFv3:

   # On Switch A, enable OSPFv3 and specify the router ID as 1.1.1.1.

   ```
   <SwitchA> system-view
   [SwitchA] ospfv3
   [SwitchA-ospfv3-1] router-id 1.1.1.1
   [SwitchA-ospfv3-1] quit
   [SwitchA] interface vlan-interface 100
   [SwitchA-Vlan-interface100] ospfv3 1 area 0
   [SwitchA-Vlan-interface100] quit
   ```

   # On Switch B, enable OSPFv3 and specify the router ID as 2.2.2.2.

   ```
   <SwitchB> system-view
   [SwitchB] ospfv3
   [SwitchB-ospfv3-1] router-id 2.2.2.2
   [SwitchB-ospfv3-1] quit
   [SwitchB] interface vlan-interface 200
   [SwitchB-Vlan-interface200] ospfv3 1 area 0
   [SwitchB-Vlan-interface200] quit
   ```

   # On Switch C, enable OSPFv3 and specify the router ID as 3.3.3.3.

   ```
   <SwitchC> system-view
   [SwitchC] ospfv3
   [SwitchC-ospfv3-1] router-id 3.3.3.3
   [SwitchC-ospfv3-1] quit
   [SwitchC] interface vlan-interface 100
   [SwitchC-Vlan-interface100] ospfv3 1 area 0
   [SwitchC-Vlan-interface100] quit
   ```

   # On Switch D, enable OSPFv3 and specify the router ID as 4.4.4.4.

   ```
   <SwitchD> system-view
   [SwitchD] ospfv3
   [SwitchD-ospfv3-1] router-id 4.4.4.4
   [SwitchD-ospfv3-1] quit
   [SwitchD] interface vlan-interface 200
   [SwitchD-Vlan-interface200] ospfv3 1 area 0
   ```

```
[SwitchD-Vlan-interface200] quit
```

Display neighbor information on Switch A. The switches have the same default DR priority 1, so Switch D (the switch with the highest router ID) is elected as the DR, and Switch C is the BDR.

```
[SwitchA] 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         1   2-Way/DROther    00:00:36  0      Vlan200
 3.3.3.3         1   Full/BDR         00:00:35  0      Vlan100
 4.4.4.4         1   Full/DR          00:00:33  0      Vlan200
```

Display neighbor information on Switch D. The neighbor states are all full.

```
[SwitchD] display ospfv3 peer


            OSPFv3 Process 1 with Router ID 4.4.4.4


 Area: 0.0.0.0
 ------------------------------------------------------------------------
 Router ID       Pri State           Dead-Time InstID Interface
 1.1.1.1         1   Full/DROther     00:00:30  0      Vlan100
 2.2.2.2         1   Full/DROther     00:00:37  0      Vlan200
 3.3.3.3         1   Full/BDR         00:00:31  0      Vlan100
```

3. Configure router priorities for interfaces:

Set the router priority of VLAN-interface 100 to 100 on Switch A.

```
[SwitchA] interface Vlan-interface 100
[SwitchA-Vlan-interface100] ospfv3 dr-priority 100
[SwitchA-Vlan-interface100] quit
```

Set the router priority of VLAN-interface 200 to 0 on Switch B.

```
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] ospfv3 dr-priority 0
[SwitchB-Vlan-interface200] quit
```

Set the router priority of VLAN-interface 100 to 2 on Switch C.

```
[SwitchC] interface Vlan-interface 100
[SwitchC-Vlan-interface100] ospfv3 dr-priority 2
[SwitchC-Vlan-interface100] quit
```

Display neighbor information on Switch A. Router priorities have been updated, but the DR and BDR are not changed.

```
[SwitchA] 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      Vlan200
```

```
  3.3.3.3         2   Full/BDR           00:00:35  0      Vlan200
  4.4.4.4         1   Full/DR            00:00:33  0      Vlan200
```

Display neighbor information on Switch D. Switch D is still the DR.

```
[SwitchD] display ospfv3 peer


           OSPFv3 Process 1 with Router ID 4.4.4.4


 Area: 0.0.0.0
 ------------------------------------------------------------------------
 Router ID       Pri State           Dead-Time InstID Interface
 1.1.1.1         100 Full/DROther       00:00:30  0      Vlan100
 2.2.2.2         0   Full/DROther       00:00:37  0      Vlan200
 3.3.3.3         2   Full/BDR           00:00:31  0      Vlan100
```

4. Restart DR and BDR election:

Use the **shutdown** and **undo shutdown** commands on interfaces to restart DR and BDR election. (Details not shown.)

Display neighbor information on Switch A. The output shows that Switch C becomes the BDR.

```
[SwitchA] 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   Full/DROther       00:00:36  0      Vlan200
 3.3.3.3         2   Full/BDR           00:00:35  0      Vlan100
 4.4.4.4         1   Full/DROther       00:00:33  0      Vlan200
```

Display neighbor information on Switch D.

```
[SwitchD] display ospfv3 peer


           OSPFv3 Process 1 with Router ID 4.4.4.4


 Area: 0.0.0.0
 ------------------------------------------------------------------------
 Router ID       Pri State           Dead-Time InstID Interface
 1.1.1.1         100 Full/DR            00:00:30  0      Vlan100
 2.2.2.2         0   2-Way/DROther      00:00:37  0      Vlan200
 3.3.3.3         2   Full/BDR           00:00:31  0      Vlan100
```

The output shows that Switch A becomes the DR.

Example: Configuring OSPFv3 route redistribution

**Network configuration**

As shown in Figure 5:

- Switch A, Switch B, and Switch C are in Area 2.
- OSPFv3 process 1 and OSPFv3 process 2 run on Switch B. Switch B communicates with Switch A and Switch 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 Switch B, and set the default metric for redistributed routes to 3. Switch C can then learn the routes destined for 1::0/64 and 2::0/64, and Switch A cannot learn the routes destined for 3::0/64 or 4::0/64.

Figure 5 Network diagram
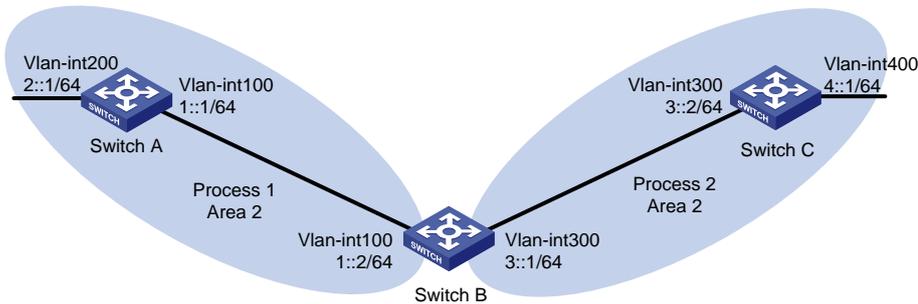
Procedure

1. Configure IPv6 addresses for interfaces. (Details not shown.)
2. Configure basic OSPFv3:

Enable OSPFv3 process 1 on Switch A.

```
<SwitchA> system-view
[SwitchA] ospfv3 1
[SwitchA-ospfv3-1] router-id 1.1.1.1
[SwitchA-ospfv3-1] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ospfv3 1 area 2
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 200
[SwitchA-Vlan-interface200] ospfv3 1 area 2
[SwitchA-Vlan-interface200] quit
```

Enable OSPFv3 process 1 and OSPFv3 process 2 on Switch B.

```
<SwitchB> system-view
[SwitchB] ospfv3 1
[SwitchB-ospfv3-1] router-id 2.2.2.2
[SwitchB-ospfv3-1] quit
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ospfv3 1 area 2
[SwitchB-Vlan-interface100] quit
[SwitchB] ospfv3 2
[SwitchB-ospfv3-2] router-id 3.3.3.3
[SwitchB-ospfv3-2] quit
[SwitchB] interface vlan-interface 300
[SwitchB-Vlan-interface300] ospfv3 2 area 2
[SwitchB-Vlan-interface300] quit
```

Enable OSPFv3 process 2 on Switch C.

```
<SwitchC> system-view
[SwitchC] ospfv3 2
[SwitchC-ospfv3-2] router-id 4.4.4.4
[SwitchC-ospfv3-2] quit
```

```
[SwitchC] interface vlan-interface 300
[SwitchC-Vlan-interface300] ospfv3 2 area 2
[SwitchC-Vlan-interface300] quit
[SwitchC] interface vlan-interface 400
[SwitchC-Vlan-interface400] ospfv3 2 area 2
[SwitchC-Vlan-interface400] quit
```
Display the routing table on Switch C.
```
[SwitchC] display ipv6 routing-table

Destinations : 7 Routes : 7

Destination: ::1/128                              Protocol  : Direct
NextHop    : ::1                                  Preference: 0
Interface  : InLoop0                              Cost      : 0


Destination: 3::/64                               Protocol  : Direct
NextHop    : ::                                   Preference: 0
Interface  : Vlan300                              Cost      : 0


Destination: 3::2/128                             Protocol  : Direct
NextHop    : ::1                                  Preference: 0
Interface  : InLoop0                              Cost      : 0


Destination: 4::/64                               Protocol  : Direct
NextHop    : ::                                   Preference: 0
Interface  : Vlan400                              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
NextHop    : ::                                   Preference: 0
Interface  : NULL0
```
3. Configure OSPFv3 route redistribution:

Configure OSPFv3 process 2 to redistribute direct routes and the routes from OSPFv3 process 1 on Switch B.
```
[SwitchB] ospfv3 2
[SwitchB-ospfv3-2] default cost 3
[SwitchB-ospfv3-2] import-route ospfv3 1
[SwitchB-ospfv3-2] import-route direct
[SwitchB-ospfv3-2] quit
```
Display the routing table on Switch C.
```
[SwitchC] display ipv6 routing-table
```

37

```
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  : Vlan300                               Cost      : 3

Destination: 2::/64                                Protocol  : O_ASE2
NextHop    : FE80::200:CFF:FE01:1C03               Preference: 150
Interface  : Vlan300                               Cost      : 3

Destination: 3::/64                                Protocol  : Direct
NextHop    : ::                                    Preference: 0
Interface  : Vlan300                               Cost      : 0

Destination: 3::2/128                              Protocol  : Direct
NextHop    : ::1                                   Preference: 0
Interface  : InLoop0                               Cost      : 0

Destination: 4::/64                                Protocol  : Direct
NextHop    : ::                                    Preference: 0
Interface  : Vlan400                               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
NextHop    : ::                                    Preference: 0
Interface  : NULL0
```

Example: Configuring OSPFv3 route summarization

**Network configuration**

As shown in Figure 6:

- Switch A, Switch B, and Switch C are in Area 2.
- OSPFv3 process 1 and OSPFv3 process 2 run on Switch B. Switch B communicates with Switch A and Switch C through OSPFv3 process 1 and OSPFv3 process 2, respectively.
- On Switch A, configure IPv6 addresses 2:1:1::1/64, 2:1:2::1/64, and 2:1:3::1/64 for VLAN-interface 200.

- On Switch B, configure OSPFv3 process 2 to redistribute direct routes and the routes from OSPFv3 process 1. Switch C can then learn the routes destined for 2::/64, 2:1:1::/64, 2:1:2::/64, and 2:1:3::/64.

- On Switch B, configure route summarization to advertise only summary route 2::/16 to Switch C.

Figure 6 Network diagram
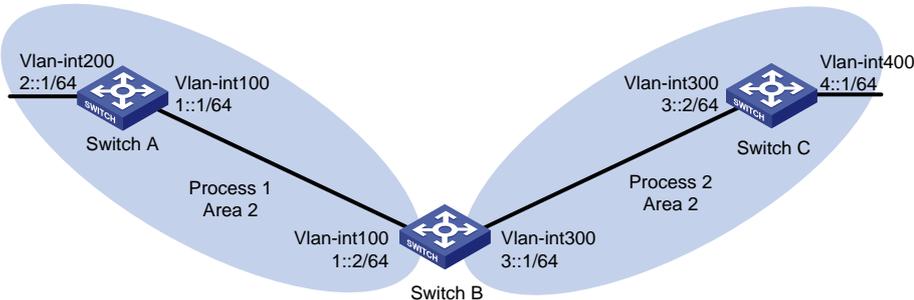
Procedure

1. Configure IPv6 addresses for interfaces. (Details not shown.)

2. Configure OSPFv3:

   # Enable OSPFv3 process 1 on Switch A.

   ```
   <SwitchA> system-view
   [SwitchA] ospfv3 1
   [SwitchA-ospfv3-1] router-id 1.1.1.1
   [SwitchA-ospfv3-1] quit
   [SwitchA] interface vlan-interface 100
   [SwitchA-Vlan-interface100] ospfv3 1 area 2
   [SwitchA-Vlan-interface100] quit
   [SwitchA] interface vlan-interface 200
   [SwitchA-Vlan-interface200] ipv6 address 2:1:1::1 64
   [SwitchA-Vlan-interface200] ipv6 address 2:1:2::1 64
   [SwitchA-Vlan-interface200] ipv6 address 2:1:3::1 64
   [SwitchA-Vlan-interface200] ospfv3 1 area 2
   [SwitchA-Vlan-interface200] quit
   ```

   # Enable OSPFv3 process 1 and OSPFv3 process 2 on Switch B.

   ```
   <SwitchB> system-view
   [SwitchB] ospfv3 1
   [SwitchB-ospfv3-1] router-id 2.2.2.2
   [SwitchB-ospfv3-1] quit
   [SwitchB] interface vlan-interface 100
   [SwitchB-Vlan-interface100] ospfv3 1 area 2
   [SwitchB-Vlan-interface100] quit
   [SwitchB] ospfv3 2
   [SwitchB-ospfv3-2] router-id 3.3.3.3
   [SwitchB-ospfv3-2] quit
   [SwitchB] interface vlan-interface 300
   [SwitchB-Vlan-interface300] ospfv3 2 area 2
   [SwitchB-Vlan-interface300] quit
   ```

   # Enable OSPFv3 process 2 on Switch C.

```
<SwitchC> system-view
[SwitchC] ospfv3 2
[SwitchC-ospfv3-2] router-id 4.4.4.4
[SwitchC-ospfv3-2] quit
[SwitchC] interface vlan-interface 300
[SwitchC-Vlan-interface300] ospfv3 2 area 2
[SwitchC-Vlan-interface300] quit
[SwitchC] interface vlan-interface 400
[SwitchC-Vlan-interface400] ospfv3 2 area 2
[SwitchC-Vlan-interface400] quit
```

3. Configure OSPFv3 route redistribution:

   # Configure OSPFv3 process 2 to redistribute direct routes and the routes from OSPFv3 process 1 on Switch B.

```
[SwitchB] ospfv3 2
[SwitchB-ospfv3-2] import-route ospfv3 1
[SwitchB-ospfv3-2] import-route direct
[SwitchB-ospfv3-2] quit
```

   # Display the routing table on Switch C.

```
[SwitchC] 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  : Vlan300                                  Cost      : 1

Destination: 2::/64                                   Protocol  : O_ASE2
NextHop    : FE80::200:CFF:FE01:1C03                  Preference: 150
Interface  : Vlan300                                  Cost      : 1

Destination: 2:1:1::/64                               Protocol  : O_ASE2
NextHop    : FE80::200:CFF:FE01:1C03                  Preference: 150
Interface  : Vlan300                                  Cost      : 1

Destination: 2:1:2::/64                               Protocol  : O_ASE2
NextHop    : FE80::200:CFF:FE01:1C03                  Preference: 150
Interface  : Vlan300                                  Cost      : 1

Destination: 2:1:3::/64                               Protocol  : O_ASE2
NextHop    : FE80::200:CFF:FE01:1C03                  Preference: 150
Interface  : Vlan300                                  Cost      : 1

Destination: 3::/64                                   Protocol  : Direct
NextHop    : 3::2                                     Preference: 0
```

```
Interface  : Vlan300                              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  : Vlan400                              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
NextHop    : ::                                   Preference: 0
Interface  : NULL0
```

4. Configure ASBR route summarization:

On Switch B, configure OSPFv3 process 2 to advertise a single route 2::/16.

```
[SwitchB] ospfv3 2
[SwitchB-ospfv3-2] asbr-summary 2:: 16
[SwitchB-ospfv3-2] quit
```

Display the routing table on Switch C.

```
[SwitchC] 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  : Vlan300                              Cost      : 1


Destination: 2::/16                               Protocol  : O_ASE2
NextHop    : FE80::200:CFF:FE01:1C03              Preference: 150
Interface  : Vlan300                              Cost      : 1


Destination: 3::/64                               Protocol  : Direct
NextHop    : 3::2                                 Preference: 0
Interface  : Vlan300                              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  : Vlan400                           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
        NextHop    : ::                               Preference: 0
        Interface  : NULL0
```
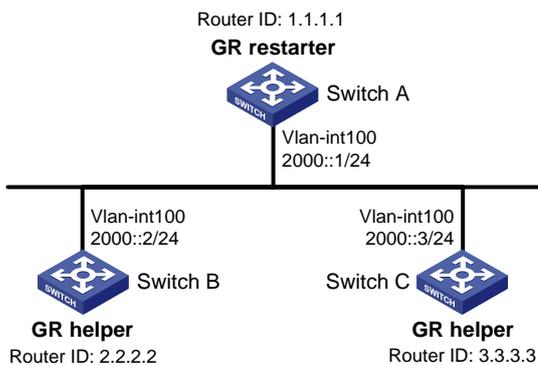
Example: Configuring OSPFv3 GR

Network configuration

As shown in Figure 7:

- Switch A, Switch B, and Switch C that reside in the same AS and the same OSPFv3 routing domain are GR capable.
- Switch A acts as the GR restarter. Switch B and Switch C act as the GR helpers, and synchronize their LSDBs with Switch A through GR.

Figure 7 Network diagram

Procedure

1. Configure IPv6 addresses for interfaces. (Details not shown.)
2. Configure basic OSPFv3:

    # On Switch A, enable OSPFv3 process 1, enable GR, and set the router ID to 1.1.1.1.
    ```
    <SwitchA> system-view
    [SwitchA] ospfv3 1
    [SwitchA-ospfv3-1] router-id 1.1.1.1
    [SwitchA-ospfv3-1] graceful-restart enable
    ```

```
[SwitchA-ospfv3-1] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ospfv3 1 area 1
[SwitchA-Vlan-interface100] quit
```
On Switch B, enable OSPFv3 and set the router ID to 2.2.2.2. (By default, GR helper is enabled on Switch B.)
```
<SwitchB> system-view
[SwitchB] ospfv3 1
[SwitchB-ospfv3-1] router-id 2.2.2.2
[SwitchB-ospfv3-1] quit
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ospfv3 1 area 1
[SwitchB-Vlan-interface100] quit
```
On Switch C, enable OSPFv3 and set the router ID to 3.3.3.3. (By default, GR helper is enabled on Switch C.)
```
<SwitchC> system-view
[SwitchC] ospfv3 1
[SwitchC-ospfv3-1] router-id 3.3.3.3
[SwitchC-ospfv3-1] quit
[SwitchC] interface vlan-interface 100
[SwitchC-Vlan-interface100] ospfv3 1 area 1
[SwitchC-Vlan-interface100] quit
```

Verifying the configuration

Perform a master/backup switchover on Switch A to trigger an OSPFv3 GR operation. (Details not shown.)

Example: Configuring OSPFv3 NSR

Network configuration

As shown in Figure 8, Switch S, Switch A, and Switch B belong to the same AS and OSPFv3 routing domain. Enable OSPFv3 NSR on Switch S to ensure correct routing when an active/standby switchover occurs on Switch S.

Figure 8 Network diagram
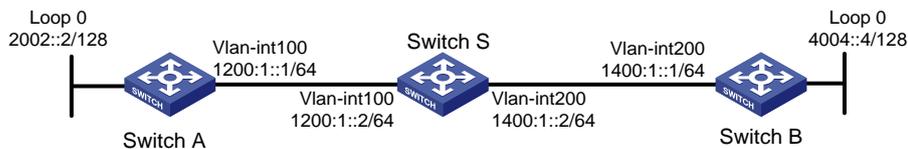
Procedure

1. Configure IP addresses and subnet masks for interfaces on the switches. (Details not shown.)
2. Configure OSPFv3 on the switches to ensure that Switch S, Switch A, and Switch B can communicate with each other at Layer 3. (Details not shown.)
3. Configure OSPFv3:

   # On Switch A, enable OSPFv3, and set the router ID to 1.1.1.1.
```
<SwitchA> system-view
[SwitchA] ospfv3 1
[SwitchA-ospfv3-1] router-id 1.1.1.1
```

```
[SwitchA-ospfv3-1] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ospfv3 1 area 1
[SwitchA-Vlan-interface100] quit
```
On Switch B, enable OSPFv3, and set the router ID to 2.2.2.2.
```
<SwitchB> system-view
[SwitchB] ospfv3 1
[SwitchB-ospfv3-1] router-id 2.2.2.2
[SwitchB-ospfv3-1] quit
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] ospfv3 1 area 1
[SwitchB-Vlan-interface200] quit
```
On Switch S, enable OSPFv3, set the router ID to 3.3.3.3, and enable NSR.
```
<SwitchS> system-view
[SwitchS] ospfv3 1
[SwitchS-ospfv3-1] router-id 3.3.3.3
[SwitchS-ospfv3-1] non-stop-routing
[SwitchS-ospfv3-1] quit
[SwitchS] interface vlan-interface 100
[SwitchS-Vlan-interface100] ospfv3 1 area 1
[SwitchS-Vlan-interface100] quit
[SwitchS] interface vlan-interface 200
[SwitchS-Vlan-interface200] ospfv3 1 area 1
[SwitchS-Vlan-interface200] quit
```

Verifying the configuration

Verify the following:

- When an active/standby switchover occurs on Switch S, the neighbor relationships and routing information on Switch A and Switch B have not changed. (Details not shown.)
- The traffic from Switch A to Switch B has not been impacted. (Details not shown.)

Example: Configuring BFD for OSPFv3

Network configuration

As shown in Figure 9:

- Configure OSPFv3 on Switch A, Switch B and Switch C and configure BFD over the link Switch A<—>L2 Switch<—>Switch B.
- After the link Switch A<—>L2 Switch<—>Switch B fails, BFD can quickly detect the failure and notify OSPFv3 of the failure. Then Switch A and Switch B communicate through Switch C.

Figure 9 Network diagram
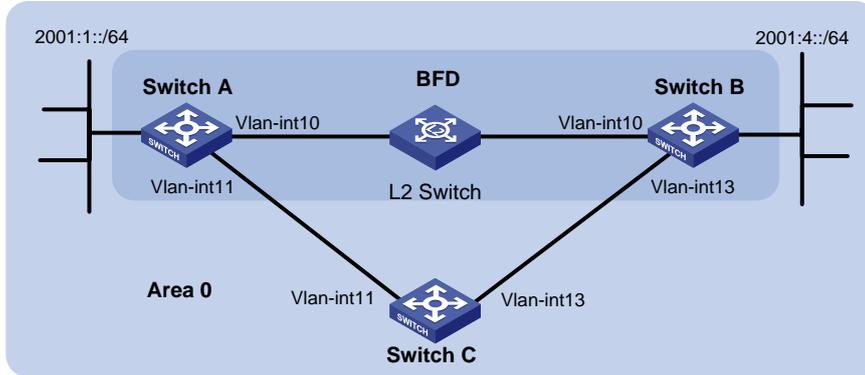
Table 1 Interface and IP address assignment

Device	Interface	IPv6 address
Switch A	Vlan-int10	2001::1/64
Switch A	Vlan-int11	2001:2::1/64
Switch B	Vlan-int10	2001::2/64
Switch B	Vlan-int13	2001:3::2/64
Switch C	Vlan-int11	2001:2::2/64
Switch C	Vlan-int13	2001:3::1/64

Procedure

1. Configure IPv6 addresses for the interfaces. (Details not shown.)
2. Configure basic OSPFv3:

   # On Switch A, enable OSPFv3 and specify the router ID as 1.1.1.1.

   ```
   <SwitchA> system-view
   [SwitchA] ospfv3
   [SwitchA-ospfv3-1] router-id 1.1.1.1
   [SwitchA-ospfv3-1] quit
   [SwitchA] interface vlan-interface 10
   [SwitchA-Vlan-interface10] ospfv3 1 area 0
   [SwitchA-Vlan-interface10] quit
   [SwitchA] interface vlan-interface 11
   [SwitchA-Vlan-interface11] ospfv3 1 area 0
   [SwitchA-Vlan-interface11] quit
   ```

   # On Switch B, enable OSPFv3 and specify the router ID as 2.2.2.2.

   ```
   <SwitchB> system-view
   [SwitchB] ospfv3
   [SwitchB-ospfv3-1] router-id 2.2.2.2
   [SwitchB-ospfv3-1] quit
   [SwitchB] interface vlan-interface 10
   [SwitchB-Vlan-interface10] ospfv3 1 area 0
   [SwitchB-Vlan-interface10] quit
   [SwitchB] interface vlan-interface 13
   [SwitchB-Vlan-interface13] ospfv3 1 area 0
   ```

```
[SwitchB-Vlan-interface13] quit
```
On Switch C, enable OSPFv3 and specify the router ID as 3.3.3.3.
```
<SwitchC> system-view
[SwitchC] ospfv3
[SwitchC-ospfv3-1] router-id 3.3.3.3
[SwitchC-ospfv3-1] quit
[SwitchC] interface vlan-interface 11
[SwitchC-Vlan-interface11] ospfv3 1 area 0
[SwitchC-Vlan-interface11] quit
[SwitchC] interface vlan-interface 13
[SwitchC-Vlan-interface13] ospfv3 1 area 0
[SwitchC-Vlan-interface13] quit
```
3. Configure BFD:

Enable BFD and configure BFD parameters on Switch A.
```
[SwitchA] bfd session init-mode active
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] ospfv3 bfd enable
[SwitchA-Vlan-interface10] bfd min-transmit-interval 500
[SwitchA-Vlan-interface10] bfd min-receive-interval 500
[SwitchA-Vlan-interface10] bfd detect-multiplier 7
[SwitchA-Vlan-interface10] return
```
Enable BFD and configure BFD parameters on Switch B.
```
[SwitchB] bfd session init-mode active
[SwitchB] interface vlan-interface 10
[SwitchB-Vlan-interface10] ospfv3 bfd enable
[SwitchB-Vlan-interface10] bfd min-transmit-interval 500
[SwitchB-Vlan-interface10] bfd min-receive-interval 500
[SwitchB-Vlan-interface10] bfd detect-multiplier 6
```

Verifying the configuration

Display the BFD information on Switch A.
```
<SwitchA> display bfd session

 Total 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 VLAN-interface 10 on
Switch A)
   Destination IP: FE80::20F:FF:FE00:1200 (link-local address of VLAN-interface 10 on
Switch B)
   Session State: Up                  Interface: Vlan10
        Hold Time: 2319ms
```
Display routes destined for 2001:4::0/64 on Switch A.
```
<SwitchA> 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  : Vlan10                               Cost      : 1
```

The output information shows that Switch A communicates with Switch B through VLAN-interface 10. The link over VLAN-interface 10 fails.

Display routes to 2001:4::0/64 on Switch A.

```
<SwitchA> 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  : Vlan11                               Cost      : 2
```
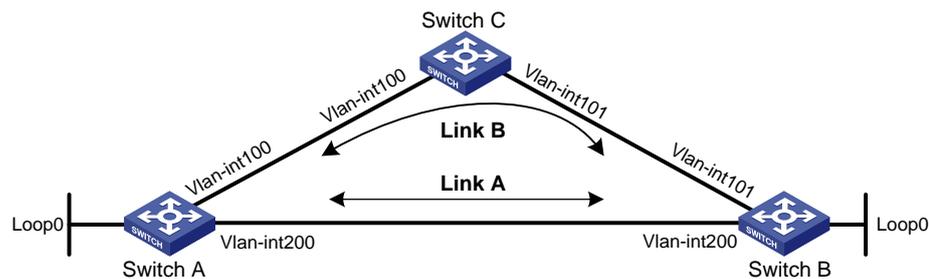
The output shows that Switch A communicates with Switch B through VLAN-interface 11.

Example: Configuring OSPFv3 FRR

Network configuration

As shown in Figure 10, Switch A, Switch B, and Switch C reside in the same OSPFv3 domain. Configure OSPFv3 FRR so that when Link A fails, traffic is immediately switched to Link B.

Figure 10 Network diagram

Table 2 Interface and IP address assignment

Device	Interface	IP address	Device	Interface	IP address
Switch A	Vlan-int100	1::1/64	Switch B	Vlan-int101	3::1/64
	Vlan-int200	2::1/64		Vlan-int200	2::2/64
	Loop0	10::1/128		Loop0	20::1/128
Switch C	Vlan-int100	1::2/64			
	Vlan-int101	3::2/64			

Procedure

1. Configure IPv6 addresses and subnet masks for interfaces on the switches. (Details not shown.)

2. Configure OSPFv3 on the switches to ensure that Switch A, Switch B, and Switch C can communicate with each other at the network layer. (Details not shown.)

3. Configure OSPFv3 FRR to automatically calculate the backup next hop:

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.

- o (Method 1.) Enable OSPFv3 FRR to calculate the backup next hop by using the LFA algorithm:

  # Configure Switch A.
  ```
  <SwitchA> system-view
  [SwitchA] ospfv3 1
  [SwitchA-ospfv3-1] fast-reroute lfa
  [SwitchA-ospfv3-1] quit
  ```
  # Configure Switch B.
  ```
  <SwitchB> system-view
  [SwitchB] ospfv3 1
  [SwitchB-ospfv3-1] fast-reroute lfa
  [SwitchB-ospfv3-1] quit
  ```

- o (Method 2.) Enable OSPFv3 FRR to designate a backup next hop by using a routing policy:

  # Configure Switch A.
  ```
  <SwitchA> system-view
  [SwitchA] ipv6 prefix-list abc index 10 permit 20::1 128
  [SwitchA] route-policy frr permit node 10
  [SwitchA-route-policy-frr-10] if-match ipv6 address prefix-list abc
  [SwitchA-route-policy-frr-10] apply ipv6 fast-reroute backup-interface
  vlan-interface 100 backup-nexthop 1::2/64
  [SwitchA-route-policy-frr-10] quit
  [SwitchA] ospfv3 1
  [SwitchA-ospfv3-1] fast-reroute route-policy frr
  [SwitchA-ospfv3-1] quit
  ```
  # Configure Switch B.
  ```
  <SwitchB> system-view
  [SwitchB] ipv6 prefix-list abc index 10 permit 10::1 128
  [SwitchB] route-policy frr permit node 10
  [SwitchB-route-policy-frr-10] if-match ipv6 address prefix-list abc
  [SwitchB-route-policy-frr-10] apply ipv6 fast-reroute backup-interface
  vlan-interface 101 backup-nexthop 3::2/64
  [SwitchB-route-policy-frr-10] quit
  [SwitchB] ospfv3 1
  [SwitchB-ospfv3-1] fast-reroute route-policy frr
  [SwitchB-ospfv3-1] quit
  ```

Verifying the configuration

Display the route 20::1/128 on Switch A to view the backup next hop information.
```
[SwitchA] 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: Vlan-interface200
 BkTunnel ID: Invalid             BkInterface: Vlan-interface100
     FtnIndex: 0x0               TrafficIndex: N/A
    Connector: N/A                    PathID: 0x0
```

Display the route 10::1/128 on Switch B to view the backup next hop information.

```
[SwitchB] display ipv6 routing-table 10::1 128 verbose

Summary count : 1

Destination: 10::1/128
     Protocol: O_INTRA
   Process ID: 1
    SubProtID: 0x1                         Age: 00h03m10s
         Cost: 1                    Preference: 10
        IpPre: N/A                  QosLocalID: N/A
          Tag: 0                         State: Active Adv
    OrigTblID: 0x0                     OrigVrf: default-vrf
      TableID: 0xa                      OrigAs: 0
        NibID: 0x23000006              LastAs: 0
       AttrID: 0xffffffff            Neighbor: ::
        Flags: 0x10041            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: Vlan-interface200
 BkTunnel ID: Invalid             BkInterface: Vlan-interface101
     FtnIndex: 0x0               TrafficIndex: N/A
    Connector: N/A                    PathID: 0x0
```
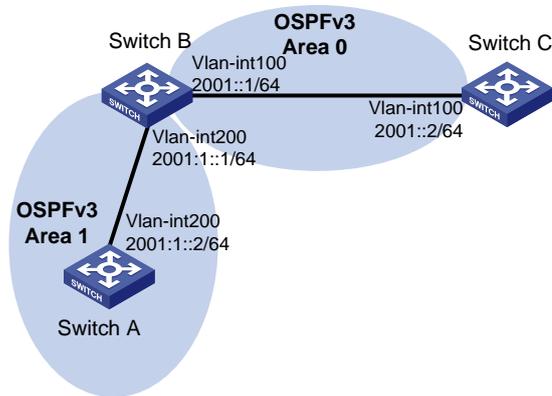
Example: Configuring OSPFv3 IPsec profile

Network configuration

As shown in Figure 11, all switches run OSPFv3, and the AS is divided into two areas.

Configure IPsec profiles on the switches to authenticate and encrypt protocol packets.

Figure 11 Network diagram

Procedure

1. Configure IPv6 addresses for interfaces. (Details not shown.)
2. Configure OSPFv3 basic features:

   # On Switch A, enable OSPFv3 and specify the router ID as 1.1.1.1.

   ```
   <SwitchA> system-view
   [SwitchA] ospfv3 1
   [SwitchA-ospfv3-1] router-id 1.1.1.1
   [SwitchA-ospfv3-1] quit
   [SwitchA] interface vlan-interface 200
   [SwitchA-Vlan-interface200] ospfv3 1 area 1
   [SwitchA-Vlan-interface200] quit
   ```

   # On Switch B, enable OSPFv3 and specify the router ID as 2.2.2.2.

   ```
   <SwitchB> system-view
   [SwitchB] ospfv3 1
   [SwitchB-ospfv3-1] router-id 2.2.2.2
   [SwitchB-ospfv3-1] quit
   [SwitchB] interface vlan-interface 100
   [SwitchB-Vlan-interface100] ospfv3 1 area 0
   [SwitchB-Vlan-interface100] quit
   [SwitchB] interface vlan-interface 200
   [SwitchB-Vlan-interface200] ospfv3 1 area 1
   [SwitchB-Vlan-interface200] quit
   ```

   # On Switch C, enable OSPFv3 and specify the router ID as 3.3.3.3.

   ```
   <SwitchC> system-view
   [SwitchC] ospfv3 1
   [SwitchC-ospfv3-1] router-id 3.3.3.3
   [SwitchC-ospfv3-1] quit
   [SwitchC] interface vlan-interface 100
   [SwitchC-Vlan-interface100] ospfv3 1 area 0
   [SwitchC-Vlan-interface100] quit
   ```

3. Configure OSPFv3 IPsec profiles:

   o On Switch A:

   # Create an IPsec transform set named **trans**.

   ```
   [SwitchA] ipsec transform-set trans
   ```

Specify the encapsulation mode as **transport**.

```
[SwitchA-ipsec-transform-set-trans] encapsulation-mode transport
```

Specify the ESP encryption and authentication algorithms.

```
[SwitchA-ipsec-transform-set-trans] protocol esp
[SwitchA-ipsec-transform-set-trans] esp encryption-algorithm aes-cbc-128
[SwitchA-ipsec-transform-set-trans] esp authentication-algorithm sha1
[SwitchA-ipsec-transform-set-trans] quit
```

Create a manual IPsec profile named **profile001**.

```
[SwitchA] ipsec profile profile001 manual
```

Use IPsec transform set **trans**.

```
[SwitchA-ipsec-profile-manual-profile001] transform-set trans
```

Configure the inbound and outbound SPIs for ESP.

```
[SwitchA-ipsec-profile-manual-profile001] sa spi outbound esp 123456
[SwitchA-ipsec-profile-manual-profile001] sa spi inbound esp 123456
```

Configure the inbound and outbound SA keys for ESP.

```
[SwitchA-ipsec-profile-manual-profile001] sa string-key outbound esp simple
abcdefg
[SwitchA-ipsec-profile-manual-profile001] sa string-key inbound esp simple
abcdefg
[SwitchA-ipsec-profile-manual-profile001] quit
```

o   On Switch B:

Create an IPsec transform set named **trans**.

```
[SwitchB] ipsec transform-set trans
```

Specify the encapsulation mode as **transport**.

```
[SwitchB-ipsec-transform-set-trans] encapsulation-mode transport
```

Specify the ESP encryption and authentication algorithms.

```
[SwitchB-ipsec-transform-set-trans] protocol esp
[SwitchB-ipsec-transform-set-trans] esp encryption-algorithm aes-cbc-128
[SwitchB-ipsec-transform-set-trans] esp authentication-algorithm sha1
[SwitchB-ipsec-transform-set-trans] quit
```

Create a manual IPsec profile named **profile001**.

```
[SwitchB] ipsec profile profile001 manual
```

Use IPsec transform set **trans**.

```
[SwitchB-ipsec-profile-manual-profile001] transform-set trans
```

Configure the inbound and outbound SPIs for ESP.

```
[SwitchB-ipsec-profile-manual-profile001] sa spi outbound esp 123456
[SwitchB-ipsec-profile-manual-profile001] sa spi inbound esp 123456
```

Configure the inbound and outbound SA keys for ESP.

```
[SwitchB-ipsec-profile-manual-profile001] sa string-key outbound esp simple
abcdefg
[SwitchB-ipsec-profile-manual-profile001] sa string-key inbound esp simple
abcdefg
[SwitchB-ipsec-profile-manual-profile001] quit
```

Create a manual IPsec profile named **profile002**.

```
[SwitchB] ipsec profile profile002 manual
```

Use IPsec transform set **trans**.

```
[SwitchB-ipsec-profile-manual-profile002] transform-set trans
```

Configure the inbound and outbound SPIs for ESP.

```
[SwitchB-ipsec-profile-manual-profile002] sa spi outbound esp 256

[SwitchB-ipsec-profile-manual-profile002] sa spi inbound esp 256
```

Configure the inbound and outbound SA keys for ESP.

```
[SwitchB-ipsec-profile-manual-profile002] sa string-key outbound esp simple
byebye

[SwitchB-ipsec-profile-manual-profile001] sa string-key inbound esp simple byebye

[SwitchB-ipsec-profile-manual-profile001] quit
```

o On Switch C:

Create an IPsec transform set named **trans**.

```
[SwitchC] ipsec transform-set trans
```

Specify the encapsulation mode as **transport**.

```
[SwitchC-ipsec-transform-set-trans] encapsulation-mode transport
```

Specify the ESP encryption and authentication algorithms.

```
[SwitchC-ipsec-transform-set-trans] protocol esp

[SwitchC-ipsec-transform-set-trans] esp encryption-algorithm aes-cbc-128

[SwitchC-ipsec-transform-set-trans] esp authentication-algorithm sha1

[SwitchC-ipsec-transform-set-trans] quit
```

Create a manual IPsec profile named **profile002**.

```
[SwitchC] ipsec profile profile002 manual
```

Use IPsec transform set **trans**.

```
[SwitchC-ipsec-profile-manual-profile002] transform-set trans
```

Configure the inbound and outbound SPIs for ESP.

```
[SwitchC-ipsec-profile-manual-profile002] sa spi outbound esp 256

[SwitchC-ipsec-profile-manual-profile002] sa spi inbound esp 256
```

Configure the inbound and outbound SA keys for ESP.

```
[SwitchC-ipsec-profile-manual-profile002] sa string-key outbound esp simple
byebye

[SwitchC-ipsec-profile-manual-profile001] sa string-key inbound esp simple byebye

[SwitchC-ipsec-profile-manual-profile001] quit
```

4. Apply the IPsec profiles to areas:

Configure Switch A.

```
[SwitchA] ospfv3 1

[SwitchA-ospfv3-1] area 1

[SwitchA-ospfv3-1-area-0.0.0.1] enable ipsec-profile profile001

[SwitchA-ospfv3-1-area-0.0.0.1] quit

[SwitchA-ospfv3-1] quit
```

Configure Switch B.

```
[SwitchB] ospfv3 1

[SwitchB-ospfv3-1] area 0

[SwitchB-ospfv3-1-area-0.0.0.0] enable ipsec-profile profile002

[SwitchB-ospfv3-1-area-0.0.0.0] quit

[SwitchB-ospfv3-1] area 1

[SwitchB-ospfv3-1-area-0.0.0.1] enable ipsec-profile profile001

[SwitchB-ospfv3-1-area-0.0.0.1] quit

[SwitchB-ospfv3-1] quit
```

Configure Switch C.

```
[SwitchC] ospfv3 1
[SwitchC-ospfv3-1] area 0
[SwitchC-ospfv3-1-area-0.0.0.0] enable ipsec-profile profile002
[SwitchC-ospfv3-1-area-0.0.0.0] quit
[SwitchC-ospfv3-1] quit
```

Verifying the configuration

Verify that OSPFv3 packets between Switches A, B, and C are protected by IPsec. (Details not shown.)