
Contents

1 Configuring OSPFv3.....	1
1.1 Introduction.....	1
1.1.1 Overview.....	1
1.1.2 Basic Concepts.....	1
1.1.3 Principles.....	10
1.1.4 Protocols and Standards.....	18
1.2 Configuration Task Summary.....	18
1.3 Configuring Basic OSPFv3 Functions.....	19
1.3.1 Overview.....	19
1.3.2 Restrictions and Guidelines.....	19
1.3.3 Configuration Tasks.....	19
1.3.4 Configuring OSPFv3.....	19
1.3.5 Creating a Virtual Link.....	20
1.4 Configuring OSPFv3 Network Types.....	21
1.4.1 Overview.....	21
1.4.2 Restrictions and Guidelines.....	21
1.4.3 Prerequisites.....	21
1.4.4 Procedure.....	22
1.5 Configuring OSPFv3 Route Advertisement.....	22
1.5.1 Overview.....	22
1.5.2 Configuration Tasks.....	22
1.5.3 Configuring External Route Redistribution.....	23

1.5.4	Generating a Default Route.....	23
1.5.5	Configuring a Device as ASBR.....	24
1.5.6	Restrictions and Guidelines.....	24
1.6	Configuring Stub Area and NSSA.....	25
1.6.1	Overview.....	25
1.6.2	Restrictions and Guidelines.....	25
1.6.3	Prerequisites.....	25
1.6.4	Procedure.....	25
1.7	Configuring OSPFv3 Route Summarization.....	26
1.7.1	Overview.....	26
1.7.2	Restrictions and Guidelines.....	26
1.7.3	Prerequisites.....	26
1.7.4	Procedure.....	26
1.8	Configuring OSPFv3 Route Filtering.....	27
1.8.1	Overview.....	27
1.8.2	Restrictions and Guidelines.....	27
1.8.3	Prerequisites.....	27
1.8.4	Procedure.....	27
1.9	Adjusting OSPFv3 Routing.....	28
1.9.1	Overview.....	28
1.9.2	Restrictions and Guidelines.....	28
1.9.3	Prerequisites.....	29
1.9.4	Procedure.....	29
1.10	Adjusting OSPFv3 Network Convergence Speed.....	30

1.10.1 Overview.....	30
1.10.2 Prerequisites.....	30
1.10.3 Configuration Tasks.....	30
1.10.4 Configuring Transmission Time of OSPFv3 Packets.....	30
1.10.5 Configuring OSPFv3 Route Computation Time.....	31
1.11 Enabling OSPFv3 Authentication.....	33
1.11.1 Overview.....	33
1.11.2 Restrictions and Guidelines.....	33
1.11.3 Prerequisites.....	33
1.11.4 Configuration Tasks.....	33
1.11.5 Configuring Area Authentication and Encryption.....	33
1.11.6 Configuring Interface Authentication and Encryption.....	34
1.12 Enabling Two-Way Maintenance.....	35
1.12.1 Overview.....	35
1.12.2 Prerequisites.....	35
1.12.3 Procedure.....	35
1.13 Correlating OSPFv3 with BFD.....	36
1.13.1 Overview.....	36
1.13.2 Restrictions and Guidelines.....	36
1.13.3 Prerequisites.....	36
1.13.4 Procedure.....	36
1.14 Enabling the GR Function.....	37
1.14.1 Overview.....	37
1.14.2 Restrictions and Guidelines.....	37

1.14.3 Prerequisites.....	37
1.14.4 Procedure.....	37
1.15 Enabling NSR.....	37
1.15.1 Overview.....	37
1.15.2 Restrictions and Guidelines.....	38
1.15.3 Prerequisites.....	38
1.15.4 Procedure.....	38
1.16 Modifying the Maximum Number of Concurrent Neighbors.....	38
1.16.1 Overview.....	38
1.16.2 Procedure.....	38
1.17 Configuring Network Management Functions.....	39
1.17.1 Overview.....	39
1.17.2 Restrictions and Guidelines.....	39
1.17.3 Prerequisites.....	39
1.17.4 Procedure.....	39
1.18 Disabling MTU Verification.....	40
1.18.1 Overview.....	40
1.18.2 Prerequisites.....	40
1.18.3 Procedure.....	40
1.19 Enabling OSPFv3 on a Super VLAN.....	40
1.19.1 Overview.....	40
1.19.2 Restrictions and Guidelines.....	40
1.19.3 Prerequisites.....	41
1.19.4 Procedure.....	41

1.20 Monitoring.....	41
1.21 Configuration Examples.....	42
1.21.1 Configuring Basic Functions of OSPFv3.....	42
1.21.2 Configuring OSPFv3 Authentication.....	48
1.21.3 Configuring a Stub Area.....	49
1.21.4 Configuring an NSSA.....	51
1.21.5 Selecting an OSPFv3 DR.....	53
1.21.6 Configuring BFD for OSPFv3.....	56
1.21.7 Configuring OSPFv3 Route Summarization.....	60

1 Configuring OSPFv3

1.1 Introduction

1.1.1 Overview

The open shortest path first version 3 (OSPFv3) is an Interior Gateway Protocol (IGP) that is used within the autonomous system (AS) to allow routers to obtain a route to a remote network.

Note

- OSPFv2 is applicable to IPv4, and OSPFv3 is applicable to IPv6. The protocol running mechanism and most configurations are the same.
-

OSPFv3 has the following characteristics:

- Wide scope of application: OSPFv3 is applicable to a larger-scale network that supports hundreds of routers.
- Fast convergence: Once the network topology changes, advertisements can be quickly sent between routers to update routes.
- No self-loop: Only the link status information is synchronized between routers. Each router computes routes independently, and a self-loop will not occur.
- Area division: A large routing domain is divided into multiple small areas to save system resources and network bandwidth and ensure stability and reliability of routes.
- Route classification: Routes are classified into several types to support flexible control.
- Equivalent routes: OSPFv3 supports equivalent routes.
- Authentication: OSPFv3 supports packet authentication to ensure security of protocol interaction.
- Multicast transmission: Protocol packets are sent using the multicast address to avoid interfering with irrelevant entities and save system resources.

Note

- In this chapter, the term "router" refers to any network device that supports the routing function. These network devices can be layer-3 (L3) switches, routers, or firewalls.
-

1.1.2 Basic Concepts

1. Routing domain

All routers in an AS must be interconnected and use the same routing protocol. Therefore, an AS is also called a routing domain.

An AS in which OSPFv3 runs is also called OSPFv3 routing domain (short for OSPFv3 domain).

2. OSPFv3 process

OSPFv3 supports multiple instances, and each instance corresponds to an OSPFv3 process.

One or more OSPFv3 processes can be started on a router. Each OSPFv3 process runs OSPFv3 independently, and the processes are mutually isolated.

An OSPFv3 packet header contains the Instance ID field, and multiple OSPFv3 instances can run concurrently on a single link. The process ID is valid only on the local device.

3. Router ID

The router ID uniquely identifies a router in an OSPFv3 domain. Router IDs of any two routers cannot be the same.

If multiple OSPFv3 processes exist on a router, each OSPFv3 process uses one router ID. Router IDs of any two OSPFv3 processes cannot be the same.

4. OSPFv3 areas

OSPFv3 supports multiple areas. An OSPFv3 domain is divided into multiple areas to ease the computing pressure of a large-scale network.

An area is a logical group of routers, and each group is identified by an area ID. The border between areas is a router. A router may belong to one area or multiple areas. One network segment (link) can belong to only one area, or each OSPFv3 interface must belong to a specified area.

- Backbone area and normal area

Area 0 is a backbone area, and other areas are normal areas. Normal areas must be directly connected to the backbone area.

- Stub area

Configuring an OSPFv3 stub area can reduce the number of Link-State Advertisements (LSAs) in the area. The area border router (ABR) in the stub area will not transfer the Type 5 LSA (external route), and will advertise the default route to the stub area.

- Totally stub area


A totally stub area is upgraded from a stub area. The router in the totally stub area will not transfer Type 3 LSA (inter-domain route) and Type 5 LSA (external route), and will advertise the default route to the stub area.

- NSSA

A not-so-stubby area (NSSA) is similar to a stub area, but allows AS boundary routers (ASBRs). The route redistributed by an ASBR will be transferred in the NSSA in the form of Type 7 LSA, and the Type 7 LSA will be translated to Type 5 LSA on ABR and then transferred to other areas. The ABR also advertises the default route to the NSSA.

- Totally NSSA

The relationship between the totally NSSA and NSSA is similar to that between the totally stub area and stub area. The totally NSSA forbids transfer of the Type 3 LSA (inter-domain route) on the basis of NSSA.

 Caution

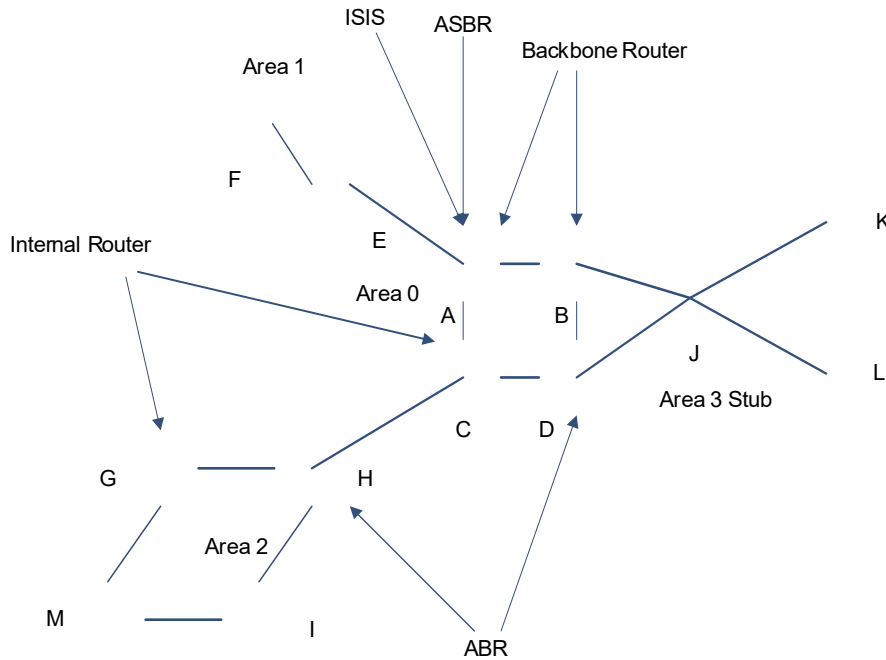
The backbone area cannot be a stub area, totally stub area, NSSA, or totally NSSA.

The stub area and totally stub area cannot contain any ASBR.

The stub area, totally stub area, NSSA, and totally NSSA cannot contain any virtual link.

The stub area, totally stub area, NSSA, and totally NSSA are special forms of normal areas and help reduce the load of routers and enhance reliability of OSPFv3 routes.

Figure 1-1 Classification of OSPFv3 Areas



5. OSPFv3 routers

The following types of routers are defined in OSPFv3 and assigned with different responsibilities:

- Internal router
All interfaces of an internal router belong to the same OSPFv3 area, for example, A, C, F, G, I, M, J, K, and L shown in [Figure 1-1](#).
- ABR
An ABR is used to connect the backbone area with a normal area. An ABR belongs to two or more areas, and one of the areas must be the backbone area, for example, B, D, E, and H shown in [Figure 1-1](#).
- Backbone router
A backbone router has at least one interface that belongs to the backbone area. All ABRs and all routers in area 0 are backbone routers, for example, A, B, C, D, E, and H shown in [Figure 1-1](#).
- ASBR
An ASBR is used to exchange routing information with other ASs. An ASBR is not necessarily located on the border of an AS. It may be a router inside an area or an ABR, for example, A shown in [Figure 1-1](#).

6. OSPFv3 Route Types

Each OSPFv3 route is marked to indicate the type of the route. There are six types of OSPFv3 routes:

- O: Internal route

This type of route describes how to arrive at a destination network in the local area. The cost of this type of route is equal to the cost of the route from the local router to the destination network.

- **OL: Inter-area route**

This type of route describes how to arrive at a destination network in another area. The cost of this type of route is equal to the cost of the route from the local router to the destination network.

- **OE1: Type 1 external route**

This type of route describes how to arrive at a destination network outside the AS. The cost of this type of route is equal to the cost of the route from the local router to the ASBR plus the cost of the route from the ASBR to the destination network. This type of route does not exist on routers in the stub or NSSA area.

- **OE2: Type 2 external route**

This type of route describes how to arrive at a destination network outside the AS. The cost of this type of route is equal to the cost of the route from the ASBR to the destination network. This type of route does not exist on routers in the stub or NSSA area.

- **ON1: Type 1 external route of the NSSA**

This type of route describes how to arrive at a destination network outside the AS through the ASBR in the NSSA. The cost of this type of route is equal to the cost of the route from the local router to the ASBR plus the cost of the route from the ASBR to the destination network. This type of route exists only on routers in the NSSA.

- **ON2: Type 2 external route of the NSSA**

This type of route describes how to arrive at a destination network outside the AS through the ASBR in the NSSA. The cost of this type of route is equal to the cost of the route from the ASBR to the destination network. This type of route exists only on routers in the NSSA.

Note

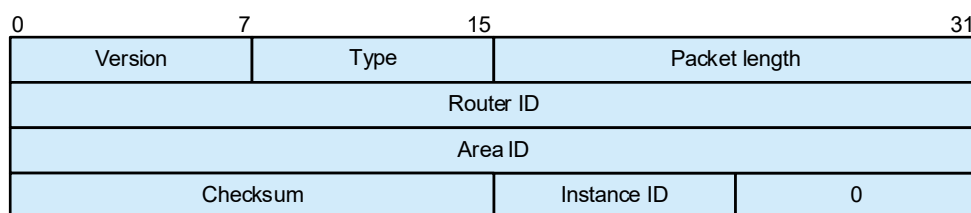
Reliability of OE2 and ON2 routes is poor. OSPFv3 believes that the cost of the route from the ASBR to a destination network outside an AS is far greater than the cost of the route to the ASBR within the AS.

Therefore, when the route cost is computed, only the cost of the route from the ASBR to a destination network outside an AS is considered.

7. OSPFv3 packets

The following table lists the OSPFv3 packets. These OSPFv3 packets are encapsulated in IP packets and transmitted in multicast or unicast mode.

Figure 1-1 OSPFv3 packet format



Version: indicates an OSPF version. The value is 3 for OSPFv3.

Type: indicates an OSPFv3 packet type.

Packet length: indicates the length of an OSPFv3 packet plus the packet head, in bytes.

Router ID: indicates the ID of a router that sends OSPFv3 packets.

Area ID: indicates the area of a router that sends OSPFv3 packets.

Checksum: indicates the checksum of an OSPFv3 packet, excluding the authentication field.

Instance ID: indicates an OSPFv3 instance ID.

0: reserved value.

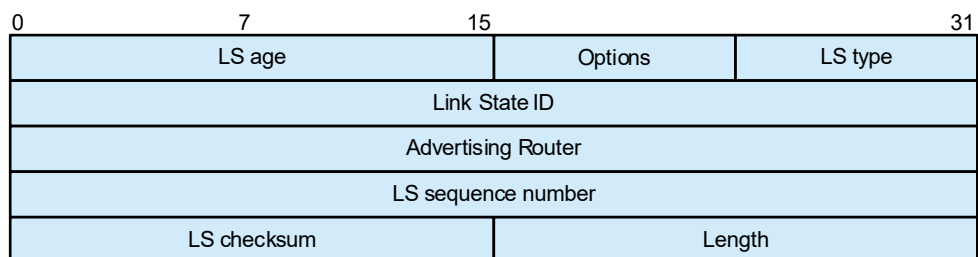
Table 1-1 Types of OSPFv3 Packets

Packet Type	Description
Hello	Hello messages are sent periodically to discover and maintain OSPFv3 neighbor relationships. The value of this OSPFv3 packet type is 1 .
Database description (DD)	DD packets carry brief information about the local link-state database (LSDB) and are used to synchronize databases between OSPFv3 neighbors. The value of this OSPFv3 packet type is 2 .
Link state request (LSR)	LSR packets are sent only after DD packets are exchanged successfully between OSPFv3 neighbors, and are used to request LSAs. The value of this OSPFv3 packet type is 3 .
Link state update (LSU)	LSU packets are used to send the required LSAs to peers. The value of this OSPFv3 packet type is 4 .
Link state acknowledgment (LSAck)	LSAck packets are used to acknowledge the received LSAs. The value of this OSPFv3 packet type is 5 .

8. LSA

OSPFv3 describes the routing information by means of LSAs.

Figure 1-1 LSA Packet Format



LS age: indicates the LS aging time of an LSA after it is generated, in seconds.

Option: is an optional field that decides whether to broadcast AS-external-LSAs, forward IP multicast packets, and process NSSA LSAs and on-demand links.

LS type: indicates different LSAs.

Link State ID: specifies a unique LSA in a routing domain together with the LSA type.

Advertising Router: indicates the ID of a router that generates this LSA.

LS sequence number: indicates the sequence number of an LSA, which is used to describe the generated sequence of LSAs.

LS checksum: indicates checksum of fields except the LS age field.

Length: indicates the total length of an LSA packet plus header, in bytes.

Table 1-1 Types of OSPFv3 LSAs

LSA Type	Description
Router-LSA (Type1)	This LSA is originated by every router. It describes the link state and cost of the router, and is advertised only within the area where the originating router is located.
Network-LSA (Type2)	This LSA is originated by a designated router (DR). It describes the state of the current link, and is advertised only within the area where the DR is located.
Inter-Area-Prefix-LSA (Type3)	This LSA is originated by an ABR. It describes a route to another area, and is advertised to areas except totally stub areas and NSSAs.
Inter-Area-Router-LSA (Type4)	This LSA is originated by an ABR. It describes a route to an ASBR, and is advertised to areas except the area where the ASBR is located.
AS-external-LSA (Type5)	This LSA is originated by an ASBR. It describes a route to a destination outside the AS, and is advertised to all areas except stub areas and NSSAs.
NSSA LSA (Type7)	This LSA is originated by an ASBR. It describes a route to a destination outside the AS, and is advertised only within the NSSA.
Link-LSA (Type8)	This LSA is originated by every router. It describes the link-local address and IPv6 prefix address of each link, and provides the link option that will be set in the Network-LSA. It is advertised only on the current link.
Intra-Area-Prefix-LSA (Type9)	Every router or DR generates one or more this type of LSAs, which are advertised in the area to which the router or DR belongs. The LSAs generated by a router describe the prefix of an IPv6 address associated with the Route-LSA. The LSAs generated by a DR describe the prefix of an IPv6 address associated with the Network-LSA.

9. OSPFv3 neighbor state

In the OSPFv3 network, neighbor devices need to reach the adjacency state before exchanging link information. There are several OSPFv3 neighbor states listed below. When a neighbor enters the full state, the adjacency relationship is established.

Table 1-1 OSPFv3 Neighbor State Machine and Description

State	Description
Down	The state of the first OSPFv3 neighbor, which indicates that the neighbor's hello packet is not received within the neighbor dead interval.
Attempt	The attempt state router sends a hello packet to the manually configured neighbor periodically. The attempt state applies to the interfaces of NBMA type only.
Init	A hello packet has been received from the neighbor, but the packet does not contain the router ID of the neighbor receiving router, that is, the peer end does not receive the hello packet sent by the local end.
Two-Way	Indicates mutual neighbors. When the neighbor router ID field in the received hello packet is each other's router ID, and both ends receive the hello packet sent from the peer end, a neighbor relationship is established. After this phase ends, DR and backup designated router (BDR) will be selected for broadcast and non-broadcast multi-access.
Exstart	Indicates negotiation about the master/slave relationship. The initial sequence number for forming an adjacency is selected, and the master/slave relationship ensures orderly transmission in the subsequent exchange of DD packets.
Exchange	Indicates exchange of DD packets. Checks whether the neighbor can provide new or updated link state information.
Loading	Indicates that, based on the information provided by DBD, the router will send LSR and interactive LSU to implement synchronization with LSDB.
Full	Indicates establishment of an adjacency. Indicates that the LSDBs of the two devices have been synchronized, and the adjacency state has been established between the local device and the neighbor device.

10. OSPFv3 network types

A router does not necessarily need to exchange LSAs with every neighbor or set up an adjacency with every neighbor. To improve efficiency, OSPFv3 classifies networks that use various link layer protocols into five types so that LSAs are exchanged in different ways to set up an adjacency.

By default, Ethernet and FDDI belong to the broadcast type, X.25, frame relay, and ATM belong to the NBMA type, and PPP, HDLC, and LAPB belong to the P2P type.

Table 1-1 Introduction to OSPFv3 Network Types

Network Type	Link Layer Protocol	Neighbor Relationship and DR Election
Broadcast	Ethernet and FDDI belong to the broadcast network type by default.	<ul style="list-style-type: none"> Neighbors are automatically discovered, and the DR and BDR are elected. The DR or BDR exchanges LSAs with all other routers to set up an adjacency. Except the DR and BDR, all other routers do not exchange LSAs with each other, and the adjacency is not set up.
NBMA	X.25, frame relay, and ATM belong to NBMA networks by default.	<ul style="list-style-type: none"> Neighbors are manually configured, and the DR and BDR are elected. The DR or BDR exchanges LSAs with all other routers to set up an adjacency. Except the DR and BDR, all other routers do not exchange LSAs with each other, and the adjacency is not set up.
Point-to-Point (P2P)	PPP, HDLC, and LAPB belong to the P2P network type by default.	<ul style="list-style-type: none"> Neighbors are automatically discovered, and the DR or BDR is not elected. LSAs are exchanged between routers at both ends of the link, and the adjacency is set up.
Point-to-Multipoint (P2MP)	Networks without any link layer protocol belong to the P2MP network type by default.	<ul style="list-style-type: none"> Neighbors are automatically discovered, and the DR or BDR is not elected. LSAs are exchanged between any two routers, and the adjacency is set up.
P2MP broadcast	Networks without any link layer protocol belong to the P2MP network type by default.	<ul style="list-style-type: none"> Neighbors are manually configured, and the DR or BDR is not elected. LSAs are exchanged between any two routers, and the adjacency is set up.

11. DR and BDR

In the broadcast or NBMA network, many unwanted LSAs will be created when an adjacency is set up with related routers. If there are n routers, $n \times (n-1)/2$ adjacency relationships will be set up, and n^2 LSAs will be generated in the network. In the process of setting up the adjacency and exchanging LSAs, many unwanted copies will be produced, which leads to chaos in the flooding of a multi-access network. To avoid these problems on a multi-access network, OSPFv3 defines the concepts of DR and BDR.

After the DR and BDR are elected, all routers will set up an adjacency relationship with the DR and BDR only, send information to the DR/BDR, and the DR will broadcast the network link state. The routers other than DR and BDR are called DROther routers and they will no longer set up an adjacency relationship or exchange any

routing information with each other, thus reducing the number of adjacency relationships between routers on the broadcast and NBMA networks.

Figure 1-1 Number of Adjacency Relationships Before DR Election

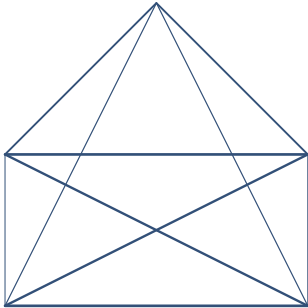
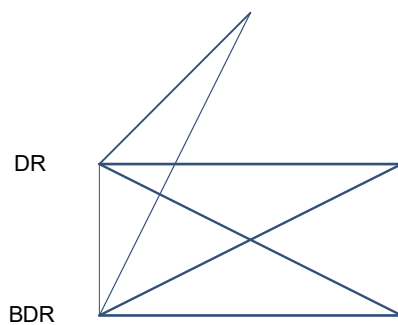


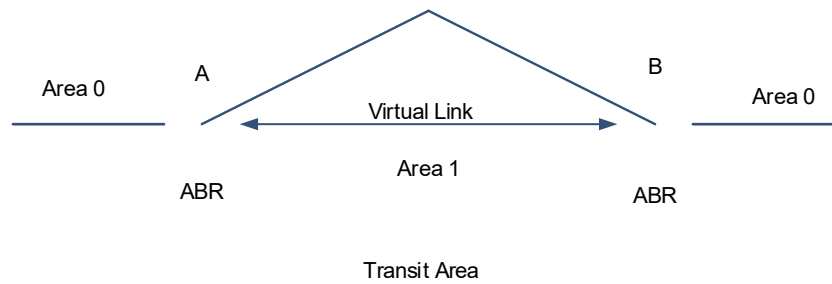
Figure 1-2 Number of Adjacency Relationships After DR Election



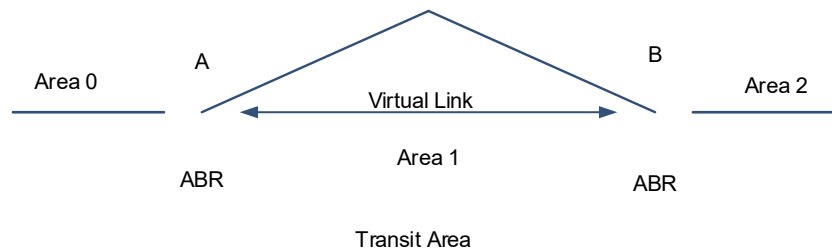
12. Virtual link

OSPFv3 supports virtual links. A virtual link is a logical link that belongs to the backbone area. It is used to resolve the problems such as a discontinuous backbone area or a failure to directly connect a normal area to the backbone area on the physical network. A virtual link supports traversal of only one normal area, and this area is called transit area. Routers on both ends of a virtual link are ABRs.

A virtual link relies on an OSPFv3 intra-domain route, making two ABRs adjacent. The OSPFv3 packet information exchanged by ABRs is transparent to the intermediate device.

Figure 1-1 Discontinuous Backbone Area on the Physical Network

As shown in [Figure 1-1](#), a virtual link is set up between A and B to connect to Area 0. Area 1 is a transit area, and A and B are ABRs of Area 1.

Figure 1-2 Failure to Directly Connect a Normal Area to the Backbone Area on the Physical Network

As shown in [Figure 1-2](#), a virtual link is set up between A and B to extend Area 0 to B so that Area 0 can be directly connected to Area 2 on B. Area 1 is a transit area, A is an ABR of Area 1, and B is an ABR of Area 1 and Area 2.

1.1.3 Principles

1. Simple principles

OSPFv3 is a type of link-state routing protocols. Its working process consists of three phases:

(1) Neighbor discovery > Bidirectional communication

An OSPFv3 neighbor relationship is set up between adjacent routers, and bidirectional communication is maintained.

(2) Database synchronization > Full adjacency

A router uses LSAs to advertise all its link states. LSAs are exchanged between neighbors and the LSDB is synchronized to achieve full adjacency.

(3) Shortest Path Tree (SPT) computation > Formation of a routing table

The router computes the shortest path to each destination network based on the LSDB and forms an OSPFv3 routing table.

- Neighbor discovery > Bidirectional communication

Routers send hello packets through all OSPFv3-enabled interfaces or virtual links. If hello packets can be exchanged between two routers, and parameters carried in the hello packets can be successfully

negotiated, the two routers become neighbors. When routers that are mutual neighbors find their own router IDs from hello packets sent from neighbors, bidirectional communication is set up.

A hello packet includes, but is not limited to, the following information:

- ID of the originating router
- Area ID of the originating router interface or virtual link
- Instance ID of the originating router interface or virtual link
- Interface ID of the originating router interface or virtual link
- Priority of the originating router interface (used for DR/BDR election)
- Hello interval of the originating router interface or virtual link
- Neighbor dead interval of the originating router interface or virtual link
- IDs of the DR and BDR
- Router ID of the neighbor of the originating router
- Database synchronization > Full adjacency

After bidirectional communication is set up between neighbor routers, the DD, LSR, LSU, and LSAck packets are used to exchange LSAs and set up the adjacency. The brief process is as follows:

- A router generates an LSA to describe all link states on the router.
- The LSA is exchanged between neighbors. When a router receives the LSA from its neighbor, it copies the LSA and saves the copy in the local LSDB, and then advertises the LSA to other neighbors.
- When the router and its neighbors obtain the same LSDB, full adjacency is achieved.

Note

OSPFv3 will be very stable without change in link cost or network addition or deletion. If any change takes place, the changed link states are advertised to quickly synchronize the LSDB.

- SPT computation > Formation of a routing table

After the complete LSDB is obtained from the router, the Dijkstra algorithm is run to generate an SPT from the local router to each destination network. The SPT records the destination networks, next-hop addresses, and cost. OSPFv3 generates a routing table based on the SPTs.

If change in link cost or network addition or deletion takes place, the LSDB will be updated. The router again runs the Dijkstra algorithm, generates a new SPT, and updates the routing table.

Note

The Dijkstra algorithm is used to find the shortest path from a vertex to other vertices in a weighted directed graph.

2. OSPFv3 routing

- Routing cost

If redundancy links or devices exist in the network, multiple paths may exist from the local device to the destination network. OSPFv3 selects the path with the minimum total cost to form an OSPFv3 route. The

total cost of a path is equal to the sum of the costs of individual links along the path. The total cost of a path can be minimized by modifying the costs of individual links along the path. In this way, OSPFv3 selects this path to form a route.

With configuration commands, you can modify the following link costs:

- o Cost from the interface to the directly-connected network segment
 - o Cost from the interface to the neighbor (from local device to a specified neighbor)
 - o Cost from the ABR to the default network segment (cost of the default route that the ABR automatically advertises to the stub area and NSSA)
 - o Cost from the ASBR to an external network segment (cost of the default route that the ABR automatically advertises to the stub area and NSSA)
 - o Cost from the ASBR to the default network segment (cost of the default route that is manually introduced)
- OSPFv3 administrative distance

The administrative distance (AD) is used to evaluate the reliability of various route sources. Its value is an integer ranging from 0 to 255. A smaller AD value indicates that the route is more trustworthy. If there are multiple routes to the same destination, the router preferentially selects a route with a smaller AD value. The route with a greater AD value becomes a floating route, that is, a standby route of the optimum route.

By default, the route coming from one source corresponds to an AD value. The AD value is a local concept. Modifying the AD value affects route selection only on the current router.

Table 1-1 Routing Protocols and Default Administrative Distances

Route Source	Directly-connected network	Static route	EBGP route	OSPFv3 route	IS-IS route	RIP route	IBGP route	Unreachable route
Default AD	0	1	20	110	115	120	200	255

3. OSPFv3 route advertisement

- Route redistribution

Route redistribution refers to the process of introducing routes of other routing protocols, routes of other OSPFv3 processes, static routes, and direct routes that exist on the device to an OSPFv3 process so that these routes can be advertised to neighbors using Type 5 and Type 7 LSAs. A default route cannot be introduced during route redistribution.

Route redistribution is often used for interworking between ASs. You can configure route redistribution on an ASBR to advertise routes outside an AS to the interior of the AS, or routes inside an AS to the exterior of the AS.

- Default route introduction

By configuring a command on an ASBR, you can introduce a default route to an OSPFv3 process so that the route can be advertised to neighbors using Type 5 and Type 7 LSAs.

Default route introduction is often used for interworking between ASs. One default route is used to replace all the routes outside an AS.

After configuration of route redistribution and introduction of a default route, the router automatically becomes an ASBR.

4. OSPFv3 route summarization

Route summarization is a process of summarizing routing information with the same prefix into one route, and advertising the summarized route (replacing a large number of individual routes) to neighbors. Route summarization helps reduce the protocol interaction load and the size of the routing table.

By default, the ABR advertises inter-area routing information by using Type 3 LSAs within a network segment, and advertises redistributed routing information by using Type 5 and Type 7 LSAs. If continuous network segments exist, you are advised to configure route summarization.

After route summarization is configured, the ABR sends only Type 3 LSAs that summarize prefix of IPv6 addresses, and the ASBR sends only Type 5 and Type 7 LSAs that summarize prefix of IPv6 addresses and will not send LSAs with the prefix of IPv6 addresses.

5. OSPFv3 route filtering

OSPFv3 allows filtering the learned and exchanged routes and LSAs so as to meet the security requirements in specific scenarios, for example, the routes of some network segments are not intended to be learned by other areas.

With configuration commands, you can configure route filtering for the following items:

- Interface: The interface is prevented from sending routing information (any LSA) or exchanging routing information (any LSA) with neighbors.
- Routing information outside an AS: Only the routing information that meets the filtering conditions can be redistributed to the OSPFv3 process (Type 5 and Type 7 LSAs).
- LSAs received by a router: In the OSPFv3 routing table, only the routes that are computed based on the LSAs meeting the filtering conditions can be advertised.

6. Stub area and NSSA

The stub/totally stub area and NSSA/totally NSSA help reduce the protocol interaction load and the size of the routing table.

- If an appropriate area is configured as a stub/totally stub area or NSSA/totally NSSA, advertisement of a large number of Type 5 and Type 3 LSAs can be avoided within the area.

Table 1-1 LSAs in Stub Area/NSSA

Area	LSA Types 1 and 2	LSA Type 3	LSA Type 4	LSA Type 5	LSA Type 7
Non-stub/totally stub area and non-NSSA/totally NSSA	Allowed	Allowed	Allowed	Allowed	Not allowed
Stub area	Allowed	Allowed	Not allowed	Not allowed	Not allowed

Area	LSA Types 1 and 2	LSA Type 3	LSA Type 4	LSA Type 5	LSA Type 7
		(containing one default route)			
Totally stub area	Allowed	Only one default route is allowed.	Not allowed	Not allowed	Not allowed
NSSA	Allowed	Allowed (containing one default route)	Allowed	Not allowed	Allowed
Totally NSSA	Allowed	Only one default route is allowed.	Allowed	Not allowed	Allowed

Note

- The ABR uses Type 3 LSAs to advertise a default route to the stub/totally stub area or NSSA/totally NSSA.
- The ABR translates Type 7 LSAs in the NSSA and totally NSSA to Type 5 LSAs, and advertises Type 5 LSAs to the backbone area.

- If an appropriate area is configured as a stub/totally stub area or NSSA/totally NSSA, a large number of OE1, OE2, and OI routes will not be added to the routing table of a router in the area.

Table 1-2 Route Types in Stub Areas/NSSAs

Area	Routes Available in the Routing Table of a Router Inside the Area
Non-stub/totally stub area and non-NSSA/totally NSSA	O: a route to a destination network in the local area OI: a route to a destination network segment in another area OE1 or OE2: a route or default route to a destination network segment outside the AS (via any ASBR in the AS)
Stub area	O: a route to a destination network in the local area OI: a route or a default route to a destination network segment in another area
Totally stub area	O: a route to a destination network in the local area OI: a default route
NSSA	O: a route to a destination network in the local area OI: a route or a default route to a destination network segment in another area ON1 or ON2: a route or default route to a destination network

Area	Routes Available in the Routing Table of a Router Inside the Area
	segment outside the AS (via an ASBR in the local area)
Totally NSSA	O: a route to a destination network in the local area OI: a default route ON1 or ON2: a route or default route to a destination network segment outside the AS (via an ASBR in the local area)

Note

- A backbone area cannot be configured as a stub area or an NSSA.
- A transit area with virtual links going through cannot be configured as a stub area or an NSSA.
- An area containing an ASBR cannot be configured as a stub area.

7. Enhanced security and reliability

The functions such as authentication and bidirectional forwarding detection (BFD) correlation are used to enhance security, stability, and reliability of OSPFv3.

- Authentication

OSPFv3 uses IPv6 to provide two authentication mechanisms: authentication header (AH) and encapsulating security payload (ESP), to prevent illegal routers from accessing the network and prevent hosts that forge OSPFv3 packets from participating in OSPFv3 route switching. OSPFv3 packets received on the OSPFv3 interface or at both ends of a virtual link are authenticated. If authentication fails, the packets are discarded and no adjacency can be set up. Enabling authentication can avoid learning unauthenticated or invalid routes, thus preventing advertising valid routes to unauthenticated devices. In the broadcast-type network, authentication also prevents unauthenticated devices from becoming designated devices, ensuring stability of the routing system and protecting the routing system against intrusions.

Authentication is classified into following two types:

- Area authentication: This area-level authentication authenticates the packets transmitted by all the interfaces in the area. This authentication type is configured in OSPFv3 routing process mode.
- Interface authentication: This neighbor-level authentication authenticates the packets transmitted on the related interface. This authentication type is configured in interface mode.

- MTU verification

Upon receiving a DD packet, OSPFv3 checks whether the MTU of the neighbor interface is the same as that of the local interface. If the MTU of the interface specified in the received DD packet is greater than that of the interface that receives the packet, the adjacency cannot be set up. Disabling MTU verification can avoid this problem.

- Two-way maintenance

OSPFv3 routers periodically send hello packets to each other to maintain the adjacency. In a large network, a lot of packets may be sent or received, occupying a great proportion of CPU and memory. As a

result, some packets are delayed or discarded. If the processing time of hello packets exceeds the dead interval, the adjacency will be destroyed.

If the two-way maintenance function is enabled, in addition to the hello packets, the DD, LSU, LSR, and LSAck packets can also be used to maintain the bidirectional communication between neighbors, which makes the adjacency more stable.

- Concurrent neighbor interaction restriction

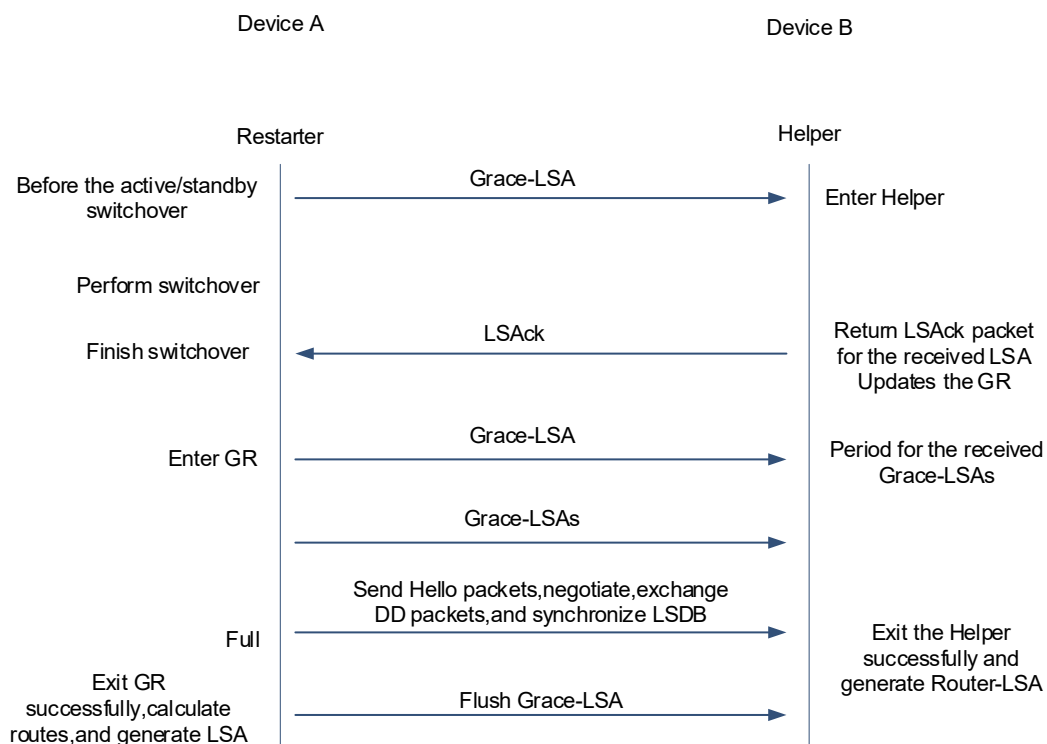
When a router simultaneously exchanges data with multiple neighbors, its performance may be affected. If the maximum number of neighbors that concurrently initiate or accept interaction with the OSPFv3 process is restricted, the router can interact with neighbors by batches, which ensures data forwarding and other key services.

- GR

The control and forwarding separated technology is widely used among routers. On a relatively stable network topology, when a graceful restart (GR) enabled router is restarted on the control plane, data forwarding can continue on the forwarding plane. In addition, actions (such as adjacency re-forming and route computation) performed on the control plane do not affect functions of the forwarding plane. In this way, service interruption caused by route flapping can be avoided, thus enhancing reliability of the entire network.

Currently, the GR function is used only during active/standby switchover and system upgrade.

Figure 1-1 Normal OSPFv3 GR Process



- The GR process requires collaboration between the restarter and the helper. The restarter is the router where GR occurs. The helper is a neighbor of the restarter.
- When entering or exiting the GR process, the restarter sends a grace-LSA to the neighbor, notifying the

neighbor to enter or exit the helper state.

- When the adjacency between the restarter and the helper reaches the full state, the router can exit the GR process successfully.

- **Fast hello**

- Correlation with BFD

After a link fails, it takes a period of time (about 40s) before OSPFv3 can sense the failure of the neighbor. Then, OSPFv3 advertises the information and re-computes the SPT. During this period, traffic is interrupted.

- After the fast hello function is enabled (that is, the neighbor dead interval is set to 1s), OSPFv3 can sense the failure of the neighbor within 1s once a link is faulty. This accelerates route convergence and prevents traffic interruption.
- BFD is used to test connectivity between devices. A link fault can be detected in as short as 150 ms. After OSPFv3 is correlated with BFD, OSPFv3 can sense the failure of a neighbor in as short as 150 ms once a link is faulty. This accelerates route convergence and prevents traffic interruption.

8. Network management functions

Functions such as management information base (MIB) and Syslog are used to facilitate OSPFv3 management.

- **MIB**

MIB is the device state information set maintained by a device. You can use the management program to view and set the MIB node.

Multiple OSPFv3 processes can be simultaneously started on a router, but the OSPFv3 MIB can be bound to only one OSPFv3 process.

- **Trap**

A trap message is a notification generated when the system detects a fault. This message contains the related fault information.

If the trap function is enabled, the router can actively send the trap messages to the network management device.

- **Syslog**

The syslog records the operations (such as command configuration) performed by users on routers and specific events (such as network connection failures).

If the syslog is allowed to record the adjacency changes, the network administrator can view the logs to learn the entire process from OSPFv3 adjacency setup to maintenance.

1.1.4 Protocols and Standards

- RFC 2740: This document describes the modifications to OSPFv3 to support version 6 of the Internet Protocol (IPv6).
- draft-ietf-ospf-ospfv3-graceful-restart: This document describes the OSPFv3 graceful restart. The OSPFv3 graceful restart is identical to OSPFv3v2 except for the differences described in this document. These differences include the format of the grace Link State Advertisements (LSA) and other considerations.
- draft-ietf-ospf-ospfv3-mib-11: This memo defines a portion of the Management Information Base (MIB) for

use with network management protocols in IPv6-based Internet. In particular, it defines objects for managing the Open Shortest Path First Routing Protocol for IPv6.

1.2 Configuration Task Summary

OSPFv3 configuration includes the following tasks:

- (1) Configuring Basic OSPFv3 Functions
 - a Configuring OSPFv3
 - b (Optional) [Creating a Virtual Link](#)
- (2) (Optional) [Configuring OSPFv3 Network Types](#)
- (3) (Optional) [Configuring OSPFv3 Route Advertisement](#). The following configuration tasks are optional. Select tasks for configuration according to the actual condition.
 - o Configuring External Route Redistribution
 - o Generating a Default Route
 - o Configuring a Device as ASBR
- (4) (Optional) [Configuring Stub Area and NSSA](#)
- (5) (Optional) [Configuring OSPFv3 Route Summarization](#)
- (6) (Optional) [Configuring OSPFv3 Route Filtering](#)
- (7) (Optional) [Adjusting OSPFv3 Routing](#)
- (8) (Optional) [Adjusting OSPFv3 Network Convergence Speed](#). The following configuration tasks are optional. Select tasks for configuration according to the actual condition.
 - o Configuring Transmission Time of OSPFv3 Packets
 - o Configuring OSPFv3 Route Computation Time
- (9) (Optional) [Enabling OSPFv3 Authentication](#). The following configuration tasks are optional. Select tasks for configuration according to the actual condition.
 - o Configuring Area Authentication and Encryption
 - o Configuring Interface Authentication and Encryption
- (10) (Optional) [Enabling Two-Way Maintenance](#)
- (11) (Optional) [Correlating OSPFv3 with BFD](#)
- (12) (Optional) [Enabling the GR Function](#)
- (13) (Optional) [Enabling NSR](#)
- (14) (Optional) [Modifying the Maximum Number of Concurrent Neighbors](#)
- (15) (Optional) [Configuring Network Management Functions](#)
- (16) (Optional) [Disabling MTU Verification](#)
- (17) (Optional) [Enabling OSPFv3 on a Super VLAN](#)

1.3 Configuring Basic OSPFv3 Functions

1.3.1 Overview

Set up an OSPFv3 routing domain in the network to provide IPv6 unicast routing service for users in the network.

1.3.2 Restrictions and Guidelines

- Ensure that the IPv6 routing function is enabled, that is, the **ipv6 routing** command is not disabled; otherwise, OSPFv3 cannot be enabled.
- The interface is configured with an IPv6 address.

1.3.3 Configuration Tasks

Basic OSPFv3 function configuration includes the following tasks:

- (1) Configuring OSPFv3
- (2) (Optional) [Creating a Virtual Link](#)

1.3.4 Configuring OSPFv3

1. Overview

The basic OSPFv3 functions are the prerequisites of all OSPFv3 functions. An OSPFv3 process must be created, a router ID can be specified for this process, and OSPFv3 must be configured on the interface.

2. Restrictions and Guidelines

- The configuration is mandatory for every OSPFv3 router.
- You are advised to configure the router ID.
- Run the **ipv6 ospf area** command in interface configuration mode to enable the OSPFv3 function on the interface, and then run the **ipv6 router ospf** command to configure an OSPFv3 process. After the OSPFv3 process is configured, the interface will automatically participate in the related process. The adjacency can be set up only between devices with the same instance ID.

3. Procedure

- (1) Enter the privileged EXEC mode.
enable
- (2) Enter the global configuration mode.
configure terminal
- (3) Create an OSPFv3 process and enter OSPFv3 configuration mode.
ipv6 router ospf [process-id [vrf vrf-name]]
- (4) (Optional) Configure a router ID.
router-id router-id

By default, the OSPFv3 routing process elects the largest IPv4 address among all the loopback interfaces as the router ID. If the loopback interfaces configured with IP addresses are not available, the OSPFv3 process elects the largest one among the IP addresses of all its physical interfaces as the router ID.

- (5) Return to the global configuration mode.

exit

- (6) Enter the interface configuration mode.

interface *interface-type interface-number*

- (7) Enable OSPFv3 on the interface and specify an area ID.

ipv6 ospf *process-id area area-id [instance instance-id]*

OSPFv3 is disabled on an interface by default.

1.3.5 Creating a Virtual Link

1. Overview

In an OSPFv3 AS, all areas must be connected to the backbone area to properly learn the routing information of the entire OSPFv3 AS. If an area cannot be directly connected to the backbone area, the virtual link can be used to connect this area to the backbone area.

2. Restrictions and Guidelines

- The area where the virtual link is located cannot be a stub area or NSSA.
- At both ends of neighbors between which the virtual link is set up, settings of **hello-interval**, **dead-interval**, and **instance** must be consistent; otherwise, the adjacency cannot be set up properly.

3. Procedure

- (1) Enter the privileged EXEC mode.

enable

- (2) Enter the global configuration mode.

configure terminal

- (3) Enter the OSPFv3 configuration mode.

ipv6 router ospf [*process-id [vrf vrf-name]*]

- (4) Configure a virtual link.

area *area-id virtual-link router-id [dead-interval dead-interval | hello-interval hello-interval | instance instance-id | retransmit-interval retransmit-interval | transmit-delay transmit-delay]* * [**authentication ipsec spi** *spi* { **md5** | **sha1** } [0 | 7] *key* | **encryption ipsec spi spi esp** [3des | aes-cbc { 128 | 192 | 256 } [0 | 7] *des-key* | des [0 | 7] *des-key* | **null**] { **md5** | **sha1** } [0 | 7] *key*]

No virtual link is configured by default.

1.4 Configuring OSPFv3 Network Types

1.4.1 Overview

If the physical network is X.25, frame relay, or ATM, OSPFv3 can also run to provide the IPv6 unicast routing service.

OSPFv3 classifies networks into five types according to the link layer protocol type so that LSAs are exchanged in different ways to set up an adjacency. You can configure to forcibly change the network type of an interface.

1.4.2 Restrictions and Guidelines

- The broadcast network sends OSPFv3 multicast packets, automatically discovers neighbors, and elects a DR and a BDR.
- The P2P network sends OSPFv3 multicast packets and automatically discovers neighbors.
- The NBMA network sends OSPFv3 unicast packets. Neighbors must be manually specified, and a DR and a BDR must be elected.
- The P2MP network (without carrying the **non-broadcast** parameter) sends OSPFv3 multicast packets and automatically discovers neighbors.
- The P2MP network (carrying the **non-broadcast** parameter) sends OSPFv3 unicast packets. Neighbors must be manually specified.
- On a broadcast network, a DR or BDR must be elected. During the DR/BDR election, the device with a higher priority will be preferentially elected as a DR or BDR. If the priority is the same, the device with a larger router ID will be preferentially elected as a DR or BDR. A device with the priority 0 does not participate in the DR or BDR election.

1.4.3 Prerequisites

The basic OSPFv3 functions must be configured before this function is used.

1.4.4 Procedure

- (1) Enter the privileged EXEC mode.

```
enable
```

- (2) Enter the global configuration mode.

```
configure terminal
```

- (3) Enter the interface configuration mode.

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

- (4) Configure a network type for the interface.

```
ipv6 ospf network { broadcast | non-broadcast | point-to-multipoint [ non-broadcast ] | point-to-point } [ instance instance-id ]
```

No interface type of OSPFv3 is configured by default. Routers at both ends of a link must be configured with the same network type.

- (5) (Optional) Configure neighbors.

```
ipv6 ospf neighbor ipv6-address [ cost cost | [ poll-interval poll-interval | priority value ] * ] [ instance instance-id ]
```

No neighbor is configured by default.

(6) (Optional) Configure the interface priority.

```
ipv6 ospf priority priority [ instance instance-id ]
```

The priority value is 1 by default.

1.5 Configuring OSPFv3 Route Advertisement

1.5.1 Overview

The function aims to introduce unicast routes for other AS domains or default routes to other AS domains to the OSPFv3 domain and provides the unicast routing service to other AS domains for users in the OSPFv3 domain. The router that introduces routes will automatically become an ASBR.

OSPFv3 has two types of external routes. The metric of the Type 1 external route changes, but the metric of the Type 2 external route is fixed. If two parallel paths to the same destination network have the same route metric, the priority of Type 1 route is higher than that of Type 2 route. Therefore, running the **show ipv6 route** command displays only the Type 1 route.

1.5.2 Configuration Tasks

The following configuration tasks are optional. Select tasks for configuration according to the actual condition.

- Configuring External Route Redistribution
- Generating a Default Route
- Configuring a Device as ASBR

1.5.3 Configuring External Route Redistribution

1. Overview

Configure external route redistribution if external routes of the OSPFv3 domain need to be introduced to an ASBR.

2. Restrictions and Guidelines

- Configure **redistribute** on an ASBR.
- During redistribution of IS-IS routes, **level-1**, **level-2**, or **level-1-2** parameters can be configured to indicate that IS-IS routes of the specified levels are configured. By default, level-2 IS-IS routes are redistributed.

3. Procedure

(1) Enter the privileged EXEC mode.

```
enable
```

(2) Enter the global configuration mode.

```
configure terminal
```

(3) Enter the OSPFv3 configuration mode.

```
ipv6 router ospf [ process-id [ vrf vrf-name ] ]
```

(4) Configure external route redistribution.

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

The route redistribution function is not enabled by default. The default metric type is 2.

Level-2 routes are redistributed by default during IS-IS redistribution.

OSPFv3 routes of all sub-types are redistributed by default during OSPFv3 redistribution. The **route map** is not associated by default.

1.5.4 Generating a Default Route

1. Overview

A default route needs to be introduced to an ASBR so that other routers in the OSPFv3 domain access other AS domains through this ASBR by default.

2. Restrictions and Guidelines

- When the **redistribute** or **default-information** command is executed, the OSPFv3 router automatically becomes an ASBR.
- The ASBR, however, does not automatically generate or advertise a default route to all routers in the OSPFv3 routing domain. To enable an ASBR to generate a default route, run the **default-information originate** command.
- If the **always** parameter is specified, the OSPFv3 process advertises an external default route to neighbors no matter whether a default route exists in the core routing table. This default route, however, is not displayed on the local router. To confirm whether the default route is generated, run the **show ipv6 ospf database** command to display the OSPFv3 link status database. On an OSPFv3 neighbor, you can run the **show ipv6 route ospf** command to see the default route.
- The metric of the external default route can be defined only by the **default-information originate** command, instead of the **default-metric** command.
- A router in a stub area cannot generate an external default route.

3. Procedure

(1) Enter the privileged EXEC mode.

```
enable
```

(2) Enter the global configuration mode.

```
configure terminal
```

(3) Enter the OSPFv3 configuration mode.

```
ipv6 router ospf [ process-id [ vrf vrf-name ] ]
```

(4) Generate a default route.

```
default-information originate [ always | metric metric | metric-type type | route-map map ] *
```

No default route is generated by default.

1.5.5 Configuring a Device as ASBR

1. Overview

Configure a device as ASBR in the AS domain or AS boundary.

1.5.6 Restrictions and Guidelines

After the **redistribute** or **default-information** command is executed, an OSPFv3 router automatically becomes an ASBR. If you want the device to become an ASBR without configuring the above command, run the **asbr enable** command.

If the **asbr enable** command is deleted, but the **redistribute** or **default-information** command configuration remains valid, the device is still an ASBR.

1. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPFv3 configuration mode.

ipv6 router ospf [*process-id* [**vrf** *vrf-name*]]

(4) Configure a device as ASBR.

asbr enable

No device is an ASBR by default.

1.6 Configuring Stub Area and NSSA

1.6.1 Overview

The function is used to configure an area located on the stub as a stub area to reduce interaction of routing information and the size of routing table, and enhance stability of routes. Devices in a stub area cannot learn the external routes (Type 5 LSAs) of the AS. In practice, external routes take up a large proportion of the LSDB. Therefore, devices in a stub area can learn only a small amount of routing information, which reduces the amount of system resources required to run the OSPFv3 protocol.

To reduce the size of the routing table on routers in the area and introduce OSPFv3 external routes to the area, configure the stub area as an NSSA.

1.6.2 Restrictions and Guidelines

- A backbone or transit area cannot be configured as a stub area or an NSSA.
- A router in the stub area cannot introduce external routes, but a router in the NSSA can introduce external routes.
- An area located on the stub of a network can be configured as a stub area. You must run the **area stub** command on all routers in a stub area.
- To configure a totally stub area, add the **no-summary** keyword when you are running the **area stub**

command on the ABR.

- To configure a totally NSSA, you can configure the **no-summary** parameter on the ABR to prevent the ABR from sending the summary LSAs (Type 3 LSAs) to the NSSA.

1.6.3 Prerequisites

The basic OSPFv3 functions must be configured before this function is used.

1.6.4 Procedure

- (1) Enter the privileged EXEC mode.

enable

- (2) Enter the global configuration mode.

configure terminal

- (3) Enter the OSPFv3 routing process configuration mode.

ipv6 router ospf [*process-id* [**vrf** *vrf-name*]]

- (4) Configure a special OSPFv3 area. Configure one of the following tasks.

- Configure a stub area.

area *area-id* **stub** [**no-summary**]

The stub area function is disabled by default.

- Configure an NSSA.

area *area-id* **nssa** [**default-information-originate** [**metric** *metric* | **metric-type** *metric-type*] * | **no-redistribution** | **no-summary** | **translator** [**always** | **stability-interval** *stability-interval*] *] *

The NSSA function is disabled by default.

1.7 Configuring OSPFv3 Route Summarization

1.7.1 Overview

Summarize routes to reduce interaction of routing information and the size of routing table, and enhance stability of routes.

Route summarization is classified into two types:

- Inter-area route summarization means to summarize routes between OSPFv3 areas.
- External route summarization means to summarize external routes of an OSPFv3 routing domain.

1.7.2 Restrictions and Guidelines

- The address range of the routes to be summarized may exceed the actual network range in the routing table. If data is sent to a network beyond the summarization range, a routing loop may be formed and the router processing load may increase. To prevent these problems, a discard route must be added to the routing table to shield or filter routes.
- Inter-area route summarization is configured and only takes effect on an ABR.
- External route summarization is configured on the ASBR that introduces routes.
- When configured on the NSSA ABR translator, **summary-prefix** summarizes redistributed routes and routes

obtained based on the LSAs that are translated from Type 7 to Type 5. When configured on the ASBR (not an NSSA ABR translator), **summary-prefix** summarizes only redistributed routes.

1.7.3 Prerequisites

The basic OSPFv3 functions must be configured before this function is used.

1.7.4 Procedure

- (1) Enter the privileged EXEC mode.

enable

- (2) Enter the global configuration mode.

configure terminal

- (3) Enter the OSPFv3 routing process configuration mode.

ipv6 router ospf [*process-id* [**vrf** *vrf-name*]]

- (4) (Optional) Configure inter-area route summarization.

area *area-id* **range** *ipv6-prefix/prefix-length* [**advertise** | **not-advertise**]

Inter-area route summarization is not performed by default.

- (5) (Optional) Configure external route summarization.

summary-prefix *ipv6-prefix/prefix-length* [[**cost** *cost* | **tag** *tag-value*] * | **not-advertise**]

Route summarization is disabled by default.

1.8 Configuring OSPFv3 Route Filtering

1.8.1 Overview

Route filtering can prevent routes from being loaded to the routing table or advertised to neighbors. Network users cannot access the specified destination network.

Routes are filtered using the following three methods:

- When an interface is configured as a passive interface, it no longer sends or receives hello packets.
- External routes are introduced to the ASBR.
- To prevent users from accessing the specified destination network, run the **distribute-list in** command to filter routes that are computed based on the received LSAs. Only routes meeting the filtering conditions can be forwarded. The command does not affect the LSDB or the routing tables of neighbors.

1.8.2 Restrictions and Guidelines

- The **passive-interface** command takes effect only on OSPFv3 interfaces, not on virtual links.
- The **distribute-list out** command is used with the **redistribute** command generally. The ACL filtering rules and prefix list filtering rules are mutually exclusive in the configuration. If the ACL is used for filtering routes coming from a source, the prefix list cannot be configured to filter the same routes.
- Filtering routes by using the **distribute-list in** command affects forwarding of local routes only, but does not affect route computation based on LSAs. Therefore, if route filtering is configured on the ABR, Type 3 LSAs will still be generated and advertised to other areas because routes can still be computed based on LSAs. As a result, black hole routes are generated. In this case, you can run the **area filter-list** or **area range**

(containing the **not-advertise** parameter) command on the ABR to prevent generation of black-hole routes.

1.8.3 Prerequisites

The basic OSPFv3 functions must be configured before this function is used.

1.8.4 Procedure

- (1) Enter the privileged EXEC mode.

enable

- (2) Enter the global configuration mode.

configure terminal

- (3) Enter the OSPFv3 routing process configuration mode.

ipv6 router ospf [*process-id* [**vrf** *vrf-name*]]

- (4) (Optional) Configure a passive interface.

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

The passive mode of interfaces is disabled by default, and all interfaces are allowed to send and receive OSPFv3 packets.

- (5) (Optional) Configure redistributed route filtering.

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

By default, the filtering function of redistributed routes is disabled, that is, all the redistributed routes pass the filtering rules.

- (6) Configure learned route filtering.

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

By default, the function of filtering routes computed based on the received LSAs is disabled, that is, all these routes get passed.

1.9 Adjusting OSPFv3 Routing

1.9.1 Overview

In actual network scenario, the network administrator expects to control OSPFv3 routes so that traffic passes or bypasses some nodes or to adjust priority of a type of OSPFv3 routes.

1.9.2 Restrictions and Guidelines

There are two methods of adjusting OSPFv3 routes:

- Adjust cost values.
 - Configure the reference bandwidth.

The default value of OSPFv3 reference bandwidth is 100 Mbps, and the cost is the actual bandwidth divided by the reference bandwidth. In the Gigabit and 10 Gigabit network environments, the computed cost value is 1, so the default bandwidth value cannot adapt to the current high-speed transport network. A router is connected to lines with different bandwidths. You are advised to adjust the

configuration according to the actual bandwidth if you want to preferentially select the line with a larger bandwidth.

- Configure the interface cost.

Modifying the interface cost of OSPFv3 can optimize routing. A lower cost value of a link indicates a higher priority during routing.

- Configure cost of the default route in a stub area or an NSSA.

After an area is configured as a stub area/NSSA, the ABR will advertise the default route to the stub area/NSSA, ensuring that the routes from the stub area/NSSA to other areas are reachable. The default cost value of the default route is 1. To lower the routing priority of the default route, you can set the cost to a greater value.

- Configure redistributed route cost.

When redistributing external routes, you can configure the cost values of external routes to adjust routing flexibly.

- Modify the administrative distance.

The administrative distance is used to select the best path when multiple routing protocols are used to reach the same target. Administrative distance defines the reliability of a routing protocol. A smaller administrative distance indicates higher reliability and higher routing priority. The default administrative distance values of OSPFv3 intra-domain routes, inter-domain routes, and external routes are all **110**. The administrative distance can be set to different values to control routing.

1.9.3 Prerequisites

The basic OSPFv3 functions must be configured before this function is used.

1.9.4 Procedure

- (1) Enter the privileged EXEC mode.

enable

- (2) Enter the global configuration mode.

configure terminal

- (3) Enter the OSPFv3 routing process configuration mode.

ipv6 router ospf [*process-id* [**vrf** *vrf-name*]]

- (4) (Optional) Configure the reference bandwidth.

auto-cost reference-bandwidth *reference-bandwidth*

The default reference bandwidth value computed based on the metric of an interface is **100** Mbps.

- (5) (Optional) Configure the interface cost.

ipv6 ospf cost *cost* [**instance** *instance-id*]

The default cost value of an OSPFv3 interface is **100** Mbps/Bandwidth. Bandwidth indicates the bandwidth of the interface and it is configured by running the **bandwidth** command in interface configuration mode. The configured bandwidth overwrites the cost automatically computed.

The default costs of OSPFv3 interfaces on several typical lines are as follows:

- For the 64 kbps serial line, the cost is **1562**.

- For the E1 line, the cost is **48**.
 - For the 10 Mbps Ethernet, the cost is **10**.
 - For the 100 Mbps Ethernet, the cost is **1**.
- (6) (Optional) Configure the cost value of the default route in a stub area or an NSSA.

area *area-id* **default-cost** *cost*

This command takes effect only on an ABR in a stub area or on an ABR/ASBR in an NSSA.

This command must be used with the **redistribute** command. This command does not take effect on external routes that are injected to the OSPFv3 routing domain by the **default-information originate** command.

- (7) (Optional) Configure the default metric for redistribution.

default-metric *metric*

The default metric of a redistributed route is **20**.

- (8) (Optional) Configure an administrative distance.

distance { *distance* | **ospf** { **external** *distance* | **inter-area** *distance* | **intra-area** *distance* } * }

The default administrative distance of all OSPFv3 routes is **110**. A smaller administrative distance indicates a higher route priority. If the administrative distance of a route entry is set to **255**, the route entry is not trustworthy and does not participate in packet forwarding.

1.10 Adjusting OSPFv3 Network Convergence Speed

1.10.1 Overview

The OSPFv3 network convergence speed is controlled by adjusting the transmission time and route computation time of OSPFv3 packets.

1.10.2 Prerequisites

The basic OSPFv3 functions must be configured before this function is used.

1.10.3 Configuration Tasks

The following configuration tasks are optional. Select tasks for configuration according to the actual condition.

- Configuring Transmission Time of OSPFv3 Packets
- Configuring OSPFv3 Route Computation Time

1.10.4 Configuring Transmission Time of OSPFv3 Packets

1. Overview

The OSPFv3 network convergence speed is controlled by adjusting the hello packet sending interval, dead interval and LSU transmission time of an OSPFv3 interface.

2. Restrictions and Guidelines

- Hello packet sending interval
 - A shorter hello interval indicates that OSPFv3 can detect topology changes more quickly, but the

- network traffic increases.
- By default, the neighbor dead interval is four times the hello packet sending interval. If the hello packet sending interval is modified, the dead interval is modified automatically.
- The neighbor dead interval cannot be shorter than the hello packet sending interval.
- The hello packet sending intervals and the neighbor dead intervals must be the same on all routers in the same network segment.
- Dead interval
 - The dead interval cannot be smaller than the hello packet sending interval.
 - The dead interval must be the same on all routers in the same network segment.
- The sending delay and line transmission delay of the interface must be considered when the **transmit-delay** command is configured. For a low-speed line, the transmission delay of the interface must be set to a value greater than the default value.
- If no acknowledgment is received from the neighbor within the time defined by the **retransmit-interval** command, the LSU packet is retransmitted. The retransmission delay can be set to a value greater than the default value on a serial line or virtual link to prevent unwanted retransmission.

3. Procedure

- (1) Enter the privileged EXEC mode.

enable

- (2) Enter the global configuration mode.

configure terminal

- (3) Enter the interface configuration mode.

interface *interface-type interface-number*

- (4) (Optional) Configure the hello interval.

ipv6 ospf hello-interval *hello-interval* [**instance** *instance-id*]

The default hello packet sending interval of the broadcast and P2P networks is **10** seconds. The default hello packet sending interval of the P2MP and NBMA networks is **30** seconds.

- (5) (Optional) Configure the dead interval.

ipv6 ospf dead-interval { *dead-interval* | **minimal hello-multiplier** *multiplier* } [**instance** *instance-id*]

The fast hello function is disabled by default, and the neighbor dead interval is four times the sending interval of hello packets.

- (6) (Optional) Configure the LSU transmission time.

ipv6 ospf transmit-delay *transmit-delay* [**instance** *instance-id*]

The default LSU packet transmission time is **1** second.

- (7) (Optional) Configure the LSU retransmission interval.

ipv6 ospf retransmit-interval *retransmit-interval* [**instance** *instance-id*]

The default LSU retransmission interval is **5** seconds.

1.10.5 Configuring OSPFv3 Route Computation Time

1. Overview

OSPFv3 route convergence speed is controlled by adjusting the LSA generation time, LSA group refresh time, SPF computation time, and route computation time.

2. Restrictions and Guidelines

- LSA generation time
 - If a high requirement is raised for network convergence during link change, you can set *delay-time* to a smaller value. You can also appropriately increase the values of the preceding parameters to reduce the CPU usage.
 - The value of *hold-time* cannot be smaller than the value of *delay-time*, and the value of *max-wait-time* cannot be smaller than the value of *hold-time*.
- LSA group refresh time
 - Every LSA has a time to live (TTL) age. When the LSA age reaches 1800s, a refreshment is needed to prevent LSAs from being cleared because their ages reaching the maximum. If LSA update and aging computation are performed for every LSA, the device will consume a lot of CPU resources. To use CPU resources effectively, you can refresh LSAs by group on the device. The interval of group refreshment is called group pacing interval. The group refreshment operation is to organize the LSAs generated within a group pacing interval into a group and refresh the group as a whole.
 - If the total number of LSAs does not change, a larger group pacing interval indicates that more LSAs need to be processed after timeout. To maintain the CPU stability, the number of LSAs to be processed upon each timeout cannot be too large. If the number of LSAs is large, you are advised to reduce the group pacing interval. For example, if there are 10,000 LSAs in the database, you can reduce the pacing interval; if there are 40 to 100 LSAs, you can set the pacing interval to 10-20 minutes.
- LSA group sending interval

If the number of LSAs is large and the device load is heavy in an environment, properly configuring *transmit-time* and *transmit-count* can limit the number of LS-UPD packets flooded in the network. If the CPU usage is not high and the network bandwidth load is not heavy, reducing the value of *transmit-time* and increasing the value of *transmit-count* can accelerate the environment convergence.
- SPF computation time
 - The *spf-delay* and *spf-holdtime* can be set to smaller values to accelerate topology convergence, and *spf-max-waittime* can be set to a larger value to reduce SPF computation.
 - The value of *spf-holdtime* cannot be smaller than that of *spf-delay*; otherwise, the value of *spf-holdtime* will be automatically set to the value of *spf-delay*.
 - The value of *spf-max-waittime* cannot be smaller than that of *spf-holdtime*; otherwise, *spf-max-waittime* will be automatically set to the value of *spf-holdtime*.
 - The configurations of **timers throttle spf** and **timers spf** are mutually overwritten.
 - When neither **timers spf** nor **timers throttle spf** is configured, the default value of **timers throttle spf** prevails.
- Computation delays of inter-area routes and external routes

If a lot of inter-area or external routes exist in the network and the network is not stable, adjust the corresponding delays and optimize route computation to reduce the load on the device.

3. Procedure

- (1) Enter the privileged EXEC mode.

enable

- (2) Enter the global configuration mode.

configure terminal

- (3) Enter the OSPFv3 configuration mode.

ipv6 router ospf [*process-id* [**vrf** *vrf-name*]]

- (4) (Optional) Configure the LSA generation time.

timers throttle lsa all *delay-time hold-time max-wait-time*

The default minimum delay of LSA generation is **0** ms, the minimum interval between the first update and the second update of LSA is **5000** ms, and the maximum interval between consecutive LSA updates is **5000** ms.

- (5) (Optional) Configure the LSA group refresh time.

timers pacing lsa-group *update-time*

The default group refresh time of LSAs is **30** seconds.

- (6) (Optional) Configure LSA group sending interval.

timers pacing lsa-transmit *transmit-time transmit-count*

The default LSA group sending interval is **40** ms, and the number of LS-UPD packets in each group is **1**.

- (7) (Optional) Configure the SPF computation delay.

timers throttle spf *spf-delay spf-holdtime spf-max-waittime*

The default delay for SPF computation is **1000** ms, the minimum interval between two SPF computations is **5000** ms, and the maximum interval between two SPF computations is **10000** ms.

- (8) Configure the computation delays of inter-area routes and external routes.

timers throttle route { **ase** *ase-delay* | **inter-area** *ia-delay* }

The default delay for inter-area route and external route computation is **0** ms.

- (9) (Optional) Configure duplicate LSA receiving delay.

timers lsa arrival *arrival-time*

The default delay for receiving a duplicate LSA is **1000** ms.

1.11 Enabling OSPFv3 Authentication

1.11.1 Overview

OSPFv3 uses the authentication mechanism, that is, IP authentication header (AH) and IP encapsulating security payload (ESP), provided by IPv6 to prevent unauthorized routers from accessing the network and hosts that forge OSPFv3 packets from participating in OSPFv3 routing.

1.11.2 Restrictions and Guidelines

- If SA authentication is configured for an area, the configuration takes effect on all interfaces that belong to this area.
- Authentication priority of OSPFv3 instances, areas, and interfaces are as follows: OSPFv3 instance authentication < area authentication < interface authentication.

1.11.3 Prerequisites

The basic OSPFv3 functions must be configured before this function is used.

1.11.4 Configuration Tasks

The following configuration tasks are optional. Select tasks for configuration according to the actual condition.

- Configuring Area Authentication and Encryption
- Configuring Interface Authentication and Encryption

1.11.5 Configuring Area Authentication and Encryption

1. Overview

When area authentication and encryption are enabled, the authentication mode and password of all devices in an area must be consistent to ensure normal setup of neighbor relationship.

2. Restrictions and Guidelines

- The device supports three authentication types:
 - No authentication (when authentication is not configured)
 - MD5
 - SHA1
- The device supports three encryption types:
 - DES
 - 3DES
 - AES-CBC
- After an OSPFv3 area is configured with encryption and authentication, the configuration takes effect on all interfaces (except virtual links) in the area, but the interface encryption and authentication configuration takes precedence over the area configuration.

3. Procedure

(1) Enter the privileged EXEC mode.

```
enable
```

(2) Enter the global configuration mode.

```
configure terminal
```

(3) Enter the OSPFv3 routing process configuration mode.

```
ipv6 router ospf [ process-id [ vrf vrf-name ] ]
```

- (4) (Optional) Configure area authentication.

```
area area-id authentication ipsec spi spi { md5 [ string-key ] | sha1 } [ 0 | 7 ] key
```

The OSPFv3 area authentication function is disabled by default.

- (5) (Optional) Configure area encryption.

```
area area-id encryption ipsec spi spi esp { { 3des | aes-cbc { 128 | 192 | 256 } | des } [ 0 | 7 ] des-key | null } { md5 | sha1 } [ 0 | 7 ] key
```

Encryption is disabled by default.

1.11.6 Configuring Interface Authentication and Encryption

1. Overview

Applied between neighbor devices, interface authentication has higher priority than area authentication. The authentication mode and password for neighbor devices must be the same.

2. Restrictions and Guidelines

- The device supports three authentication types:
 - No authentication (when authentication is not configured)
 - MD5
 - SHA1
- The device supports three encryption types:
 - DES
 - 3DES
 - AES-CBC
- The OSPFv3 encryption and authentication parameters configured on interfaces must be consistent.

3. Procedure

- (1) Enter the privileged EXEC mode.

```
enable
```

- (2) Enter the global configuration mode.

```
configure terminal
```

- (3) Enter the interface configuration mode.

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

- (4) (Optional) Configure interface encryption.

```
ipv6 ospf encryption { ipsec spi spi esp { { 3des | aes-cbc { 128 | 192 | 256 } | des } [ 0 | 7 ] des-key | null } { md5 | sha1 } [ 0 | 7 ] key | null } [ instance instance-id ]
```

Encryption is disabled by default.

1.12 Enabling Two-Way Maintenance

1.12.1 Overview

If the two-way maintenance function is enabled, in addition to the hello packets, the DD, LSU, LSR, and LSAck packets from a neighbor can also be used to maintain the bidirectional communication between neighbors. This prevents termination of the adjacency caused by delayed or discarded hello packets.

1.12.2 Prerequisites

The basic OSPFv3 functions must be configured before this function is used.

1.12.3 Procedure

- (1) Enter the privileged EXEC mode.

enable

- (2) Enter the global configuration mode.

configure terminal

- (3) Enter the OSPFv3 routing process configuration mode.

ipv6 router ospf [*process-id* [**vrf** *vrf-name*]]

- (4) Enable two-way maintenance.

two-way-maintain

The two-way maintenance function of OSPFv3 is enabled by default.

1.13 Correlating OSPFv3 with BFD

1.13.1 Overview

The OSPFv3 protocol dynamically discovers a neighbor by using hello packets. After BFD is enabled, OSPFv3 establishes a BFD session with a neighbor in the full neighbor relationship. The neighbor state is detected using the BFD mechanism. When the BFD neighbor fails, OSPFv3 immediately performs network convergence. This configuration helps shorten the traffic interruption time.

1.13.2 Restrictions and Guidelines

- The BFD parameters must be configured for the interface in advance.
- If BFD is configured for both a process and an interface, the interface-based configuration takes effect preferentially.

1.13.3 Prerequisites

The basic OSPFv3 functions must be configured before this function is used.

1.13.4 Procedure

- (1) Enter the privileged EXEC mode.

enable

- (2) Enter the global configuration mode.

configure terminal

- (3) Configure an OSPFv3 interface correlation with BFD.

- a Enter the interface configuration mode.

interface *interface-type interface-number*

- b Configure an OSPFv3 interface correlation with BFD.

ipv6 ospf bfd [**disable**]

The BFD function is disabled on an interface by default, and the BFD configuration is subject to the configuration in the OSPFv3 process configuration mode.

- (4) Exit the interface configuration mode.

exit

- (5) Configure OSPFv3 correlation with BFD.

- a Enter the OSPFv3 routing process configuration mode.

ipv6 router ospf [*process-id* [**vrf** *vrf-name*]]

- b Configure an OSPFv3 interface correlation with BFD.

bfd all-interfaces

The BFD function is disabled on all interfaces by default.

1.14 Enabling the GR Function

1.14.1 Overview

When a GR-enabled router is restarted on the control plane, data forwarding can be still guided on the forwarding plane. In addition, actions such as neighbor relationship re-forming and route computation performed on the control plane do not affect functions of the forwarding plane. In this way, service interruption caused by route flapping can be avoided, thus enhancing reliability of the entire network.

When a router implements GR, GR helper sends a Grace-LSA to notify all neighbor routers. If the GR helper function is enabled on the local router, the local router becomes the GR helper upon receiving the Grace-LSA, and helps the neighbor routers to complete GR.

1.14.2 Restrictions and Guidelines

- The neighbor router must support the GR helper.
- The GR time cannot be shorter than the neighbor relationship maintenance time of the neighbor router.

1.14.3 Prerequisites

The basic OSPFv3 functions must be configured before this function is used.

1.14.4 Procedure

- (1) Enter the privileged EXEC mode.

enable

- (2) Enter the global configuration mode.

configure terminal

- (3) Enter the OSPFv3 configuration mode.

```
ipv6 router ospf [ process-id [ vrf vrf-name ] ]
```

- (4) Enable the GR function.

```
graceful-restart [ grace-period grace-period | inconsistent-lsa-checking ]
```

The GR function is enabled by default.

- (5) Enable the OSPFv3 GR helper function.

```
graceful-restart helper { disable | internal-lsa-checking | strict-lsa-checking }
```

The GR helper capability is enabled by default. After the GR helper is enabled on the device, LSA changes are not checked.

1.15 Enabling NSR

1.15.1 Overview

During nonstop routing (NSR), OSPFv3-related information is backed up from the active supervisor module of a distributed device to the standby supervisor module, or from the active host of a virtual switching unit (VSU) to the standby host. In this way, the device can automatically recover the link state and re-generate routes without the help of the neighbor devices during the active/standby switchover. Information that should be backed up includes the neighbor relationship and link state.

1.15.2 Restrictions and Guidelines

- This command is used to enable the NSR function. For the same OSPFv3 process, either NSR or GR is enabled because they are mutually exclusive. Nevertheless, when NSR is enabled, the GR helper capability is supported.
- The switchover of devices in distributed or VSU mode takes a period of time. If OSPFv3 neighbor keepalive duration is shorter than the switchover duration, the OSPFv3 neighbor relationship with the neighbor device is removed, and services are interrupted during the switchover. Therefore, it is recommended that the OSPFv3 neighbor keepalive duration be no smaller than the default value when the NSR function is enabled. When the fast hello function is enabled, the OSPFv3 neighbor keepalive duration is less than 1s. As a result, it is recommended that the NSR function be disabled.

1.15.3 Prerequisites

The basic OSPFv3 functions must be configured before this function is used.

1.15.4 Procedure

- (1) Enter the privileged EXEC mode.

```
enable
```

- (2) Enter the global configuration mode.

```
configure terminal
```

- (3) Enter the OSPFv3 configuration mode.

```
ipv6 router ospf [ process-id [ vrf vrf-name ] ]
```

- (4) Enable the NSR function.

nsr

The NSR function is disabled by default.

1.16 Modifying the Maximum Number of Concurrent Neighbors

1.16.1 Overview

When the performance of a router is affected because the router exchanges data with multiple neighbors, you can configure this command to restrict the maximum number of neighbors with which each OSPFv3 instance can concurrently initiate or accept interaction. The maximum number of neighbors can be configured at the process or device level.

1.16.2 Procedure

- (1) Enter the privileged EXEC mode.

enable

- (2) Enter the global configuration mode.

configure terminal

- (3) (Optional) Configure the maximum number of concurrent neighbors of all processes.

ipv6 router ospf max-concurrent-dd *number*

The maximum number of neighbors is **10** by default.

- (4) Enter the OSPFv3 routing process configuration mode.

ipv6 router ospf [*process-id* [**vrf *vrf-name*]]**

- (5) (Optional) Configure the maximum number of concurrent neighbors of the current process.

max-concurrent-dd *number*

The default maximum number of concurrent neighbors for a single process is **5**.

1.17 Configuring Network Management Functions

1.17.1 Overview

Use the network management software to manage OSPFv3 parameters and monitor the OSPFv3 running status.

1.17.2 Restrictions and Guidelines

- To enable the MIB function of the OSPFv3, you must enable the MIB function of the SNMP server.
- To enable the Trap function of the OSPFv3, you must enable the Trap function of the SNMP server.
- To output the OSPFv3 logs, you must enable the logging function of the device.

1.17.3 Prerequisites

The basic OSPFv3 functions must be configured before this function is used.

1.17.4 Procedure

- (1) Enter the privileged EXEC mode.

enable

- (2) Enter the global configuration mode.

configure terminal

- (3) Enter the OSPFv3 configuration mode.

```
ipv6 router ospf [ process-id [ vrf vrf-name ] ]
```

- (4) Bind the MIB with an OSPFv3 process.

enable mib-binding

The MIB is bound to the OSPFv3 process with the minimum process ID by default.

- (5) Configure the Trap function.

```
enable traps [ error [ IfConfigError | IfRxBadPacket | VirtIfConfigError | VirtIfRxBadPacket ] * | state-change [ IfStateChange | NbrStateChange | NssaTranslatorStatusChange | VirtIfStateChange | VirtNbrStateChange | RestartStatusChange | NbrRestartHelperStatusChange | VirtNbrRestartHelperStatusChange ] * ]
```

The Trap function is disabled by default.

- (6) (Optional) Configure the logging function.

log-adj-changes [**detail**]

The logging function is enabled by default, without the **detail** parameter. The log records the log information of the following four types of events only: the adjacency reaches the full state; the adjacency leaves the full state; the adjacency reaches the down state; the adjacency leaves the down state.

1.18 Disabling MTU Verification

1.18.1 Overview

When receiving a DD packet, OSPFv3 verifies whether the MTU of the neighbor's interface is the same as that of its own interface. If the neighbor interface MTU specified in the local received DD packet is greater than the MTU of the local interface, the neighbor relationship cannot be set up. After this function is enabled, adjacency can be set up and the unicast routing service can be provided even if the MTUs of interfaces on neighbor routers are different.

1.18.2 Prerequisites

The basic OSPFv3 functions must be configured before this function is used.

1.18.3 Procedure

- (1) Enter the privileged EXEC mode.

enable

- (2) Enter the global configuration mode.

configure terminal

- (3) Enter the interface configuration mode.

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

- (4) Disable MTU verification.

ipv6 ospf mtu-ignore

The MTU verification function is disabled by default.

1.19 Enabling OSPFv3 on a Super VLAN

1.19.1 Overview

In normal cases, a super VLAN contains multiple sub VLANs. Multicast packets of a super VLAN are also sent to its sub VLANs. In this case, when OSPFv3 multicast packets are sent over a super VLAN containing multiple sub VLANs, the OSPFv3 multicast packets are replicated multiple times, and the device processing capability is insufficient. As a result, a large number of packets are discarded, causing protocol flapping. In most scenarios, the OSPFv3 function does not need to be enabled in a super VLAN, and it is disabled by default. In some other scenarios, OSPFv3 needs to be run in the super VLAN, but packets need to be sent to only one sub VLAN. In this case, run this command to specify a particular sub VLAN. You must be cautious when configuring packet transmission to all sub VLANs, as the large number of sub VLANs may cause a device processing bottleneck, which will lead to the neighbor flapping.

1.19.2 Restrictions and Guidelines

- The specified sub VLAN must be connected to neighbors.

1.19.3 Prerequisites

The basic OSPFv3 functions must be configured before this function is used.

1.19.4 Procedure

- (1) Enter the privileged EXEC mode.

enable

- (2) Enter the global configuration mode.

configure terminal

- (3) Enter the interface configuration mode.

interface *vlan vlan-id*

- (4) Configure OSPFv3 to run on a super VLAN.


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

The OSPFv3 function takes effect in super VLANs only and is disabled by default.

1.20 Monitoring

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

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

 Caution

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

Run the **clear** commands to clear information.

⚠ Caution

Running the **clear** command may lose vital information and thus interrupt services.

Table 1-1 Monitoring

Command	Purpose
show ipv6 ospf [<i>process-id</i>]	Displays the configuration information of the OSPFv3 process.
show ipv6 ospf [<i>process-id</i>] database [<i>lsa-type</i> [adv-router <i>router-id</i>]]	Displays the OSPFv3 LSDB.
show ipv6 ospf [<i>process-id</i>] interface [<i>interface-type</i> <i>interface-number</i> brief]	Displays the OSPFv3 interface.
show ipv6 ospf [<i>process-id</i>] neighbor [<i>interface-type</i> <i>interface-number</i> [detail] <i>neighbor-id</i> detail]	Displays the neighbor list of OSPFv3.
show ipv6 ospf [<i>process-id</i>] route [count]	Displays the OSPFv3 routing table.
show ipv6 ospf [<i>process-id</i>] summary-prefix	Displays the summarized routes of OSPFv3 redistributed routes.
show ipv6 ospf [<i>process-id</i>] topology [area <i>area-id</i>]	Displays the OSPFv3 network topology information.
show ipv6 ospf [<i>process-id</i>] virtual-links	Displays the OSPFv3 virtual links.
clear ipv6 ospf [<i>process-id</i>] process	Clears and resets the OSPFv3 process.
debug ipv6 ospf events [abr asbr os nssa router vlink]	Debugs the OSPFv3 events.
debug ipv6 ospf ifsm [events status timers]	Debugs the OSPFv3 interfaces.
debug ipv6 ospf nfm [events status timers]	Debugs the OSPFv3 neighbors.
debug ipv6 ospf nsm [interface redistribute route]	Debugs the OSPFv3 NSM.
debug ipv6 ospf lsa [flooding generate install maxage refresh]	Debugs the OSPFv3 LSAs.
debug ipv6 ospf packet [dd detail hello ls-ack ls-request ls-update recv send]	Debugs the OSPFv3 packets.
debug ipv6 ospf route [ase ia install spf time]	Debugs the OSPFv3 routes.

1.21 Configuration Examples

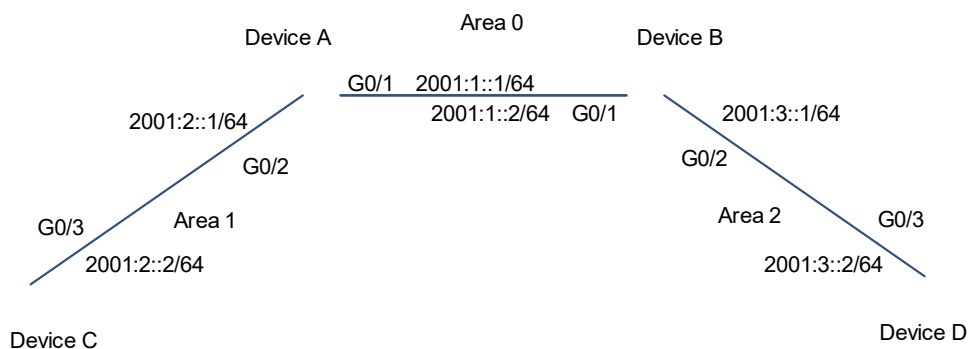
1.21.1 Configuring Basic Functions of OSPFv3

1. Requirements

OSPFv3 is enabled on all the devices, and three areas are defined in total. Device A and device B are used as ABRs forwarding inter-area routes so as to implement the interworking between all networks.

2. Topology

Figure 1-1 Topology of Basic SNMPv3 Function



3. Notes

- Configure interface IP addresses on all the devices.
- Enable the IPv4 unicast routing function on all the devices. (This function is enabled by default.)
- Configure OSPFv3 instances and router IDs on all the devices.
- Configure OSPFv3 on interfaces of all the devices.

4. Procedure

- (1) Perform the following configurations on Device A.

Enable the OSPFv3 process and configure a router ID.

```
Device A> enable
Device A# configure terminal
Device A(config)# ipv6 router ospf 1
Device A(config-router)# router-id 1.1.1.1
Device A(config-router)# exit
```

Configure an IP address for the interface and enable OSPFv3 on the interface.

```
Device A(config)# interface gigabitethernet 0/1
Device A(config-if-GigabitEthernet 0/1)# ipv6 enable
Device A(config-if-GigabitEthernet 0/1)# ipv6 address 2001:1::1/64
Device A(config-if-GigabitEthernet 0/1)# ipv6 ospf 1 area 0
```

```
Device A(config-if-GigabitEthernet 0/1)# exit
Device A(config)# interface gigabitethernet 0/2
Device A(config-if-GigabitEthernet 0/2)# ipv6 enable
Device A(config-if-GigabitEthernet 0/2)# ipv6 address 2001:2::1/64
Device A(config-if-GigabitEthernet 0/2)# ipv6 ospf 1 area 1
Device A(config-if-GigabitEthernet 0/2)# exit
```

- (2) Perform the following configurations on Device B.

Enable the OSPFv3 process and configure a router ID.

```
Device B> enable
Device B# configure terminal
Device B(config)# ipv6 router ospf 1
Device B(config-router)# router-id 2.2.2.2
Device B(config-router)# exit
```

Configure an IP address for the interface and enable OSPFv3 on the interface.

```
Device B(config)# interface gigabitethernet 0/1
Device B(config-if-GigabitEthernet 0/1)# ipv6 enable
Device B(config-if-GigabitEthernet 0/1)# ipv6 address 2001:1::2/64
Device B(config-if-GigabitEthernet 0/1)# ipv6 ospf 1 area 0
Device B(config-if-GigabitEthernet 0/1)# exit
Device B(config)# interface gigabitethernet 0/2
Device B(config-if-GigabitEthernet 0/2)# ipv6 enable
Device B(config-if-GigabitEthernet 0/2)# ipv6 address 2001:3::1/64
Device B(config-if-GigabitEthernet 0/2)# ipv6 ospf 1 area 2
Device B(config-if-GigabitEthernet 0/2)# exit
```

- (3) Perform the following configurations on Device C.

Enable the OSPFv3 process and configure a router ID.

```
Device C> enable
Device C# configure terminal
Device C(config)# ipv6 router ospf 1
Device C(config-router)# router-id 3.3.3.3
Device C(config-router)# exit
```

Configure an IP address for the interface and enable OSPFv3 on the interface.

```
Device C(config)# interface gigabitethernet 0/3
Device C(config-if-GigabitEthernet 0/3)# ipv6 enable
Device C(config-if-GigabitEthernet 0/3)# ipv6 address 2001:2::2/64
Device C(config-if-GigabitEthernet 0/3)# ipv6 ospf 1 area 1
Device C(config-if-GigabitEthernet 0/3)# exit
```

- (4) Perform the following configurations on Device D.

Enable the OSPFv3 process and configure a router ID.

```
Device D> enable
Device D# configure terminal
Device D(config)# ipv6 router ospf 1
Device D(config-router)# router-id 4.4.4.4
```



```
Device D(config-router)# exit
```

Configure an IP address for the interface and enable OSPFv3 on the interface.

```
Device D(config)# interface gigabitethernet 0/3
Device D(config-if-GigabitEthernet 0/3)# ipv6 enable
Device D(config-if-GigabitEthernet 0/3)# ipv6 address 2001:3::2/64
Device D(config-if-GigabitEthernet 0/3)# ipv6 ospf 1 area 2
Device D(config-if-GigabitEthernet 0/3)# exit
```

5. Verification

- (1) Display the following information on Device A.

Display OSPFv3 neighbor information.

```
Device A# show ipv6 ospf neighbor
OSPFv3 Process (1), 1 Neighbors, 1 is Full:
Neighbor ID      Pri   State           Dead Time   Instance ID  Interface
2.2.2.2          1    Full/BDR        00:00:30   0            GigabitEthernet 0/1
3.3.3.3          1    Full/BDR        00:00:35   0            GigabitEthernet 0/2
```

Display OSPFv3 routing table.

```
Device A# show ipv6 route ospf

IPv6 routing table name - Default - 0 entries
Codes: C - Connected, L - Local, S - Static
       R - RIP, O - OSPFv3, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPFv3 NSSA external type 1, N2 - OSPFv3 NSSA external type 2
       E1 - OSPFv3 external type 1, E2 - OSPFv3 external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area

O IA 2001:3::/64 [110/20] via FE80::2D0:F8FF:FE22:4524, GigabitEthernet 0/1
```

- (2) Display the following information on Device B.

Display OSPFv3 neighbor information.

```
Device B# show ipv6 ospf neighbor
OSPFv3 Process (1), 1 Neighbors, 1 is Full:
Neighbor ID      Pri   State           Dead Time   Instance ID  Interface
1.1.1.1          1    Full/DR         00:00:30   0            GigabitEthernet 0/1
4.4.4.4          1    Full/BDR        00:00:35   0            GigabitEthernet 0/2
```

Display OSPFv3 routing table.

```
Device B# show ipv6 route ospf

IPv6 routing table name - Default - 0 entries
```

```

Codes: C - Connected, L - Local, S - Static
       R - RIP, O - OSPFv3, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPFv3 NSSA external type 1, N2 - OSPFv3 NSSA external type 2
       E1 - OSPFv3 external type 1, E2 - OSPFv3 external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area

O IA 2001:2::/64 [110/20] via FE80::2D0:F8FF:FE22:4536, GigabitEthernet 0/1

```

(3) Display the following information on Device C.

Display OSPFv3 neighbor information.

```

Device C# show ipv6 ospf neighbor
OSPFv3 Process (1), 1 Neighbors, 1 is Full:
Neighbor ID      Pri   State           Dead Time   Instance ID  Interface
1.1.1.1          1    Full/DR         00:00:30   0            GigabitEthernet 0/3

```

Display OSPFv3 routing table.

```

Device C# show ipv6 route ospf

IPv6 routing table name - Default - 0 entries
Codes: C - Connected, L - Local, S - Static
       R - RIP, O - OSPFv3, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPFv3 NSSA external type 1, N2 - OSPFv3 NSSA external type 2
       E1 - OSPFv3 external type 1, E2 - OSPFv3 external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area

O IA 2001:1::/64 [110/2] via FE80::2D0:F8FF:FE22:4537, GigabitEthernet 0/3
O IA 2001:3::/64 [110/3] via FE80::2D0:F8FF:FE22:4537, GigabitEthernet 0/3

```

(4) Display the following information on Device D.

Display OSPFv3 neighbor information.

```

Device D# show ipv6 ospf neighbor
OSPFv3 Process (1), 1 Neighbors, 1 is Full:
Neighbor ID      Pri   State           Dead Time   Instance ID  Interface
2.2.2.2          1    Full/DR         00:00:30   0            GigabitEthernet 0/3

```

Display OSPFv3 routing table.

```

Device D# show ipv6 route ospf

IPv6 routing table name - Default - 0 entries
Codes: C - Connected, L - Local, S - Static
       R - RIP, O - OSPFv3, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPFv3 NSSA external type 1, N2 - OSPFv3 NSSA external type 2
       E1 - OSPFv3 external type 1, E2 - OSPFv3 external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

```

```
IA - Inter area
```

```
O IA 2001:1::/64 [110/2] via FE80::2D0:F8FF:FE22:4547, GigabitEthernet 0/3
O IA 2001:2::/64 [110/3] via FE80::2D0:F8FF:FE22:4547, GigabitEthernet 0/3
```

Verify that 2001:2::2/64 can be pinged successfully on Device D.

```
Device D# ping 2001:2::2
Sending 5, 100-byte ICMP Echoes to 2001:2::2, timeout is 2 seconds:
< press Ctrl+C to break >
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/9/14 ms.
```

6. Configuration Files

- Device A configuration file

```
!
ipv6 router ospf 1
 router-id 1.1.1.1
!
interface gigabitethernet 0/1
 ipv6 enable
 ipv6 address 2001:1::1/64
 ipv6 ospf 1 area 0
!
interface gigabitethernet 0/2
 ipv6 enable
 ipv6 address 2001:2::1/64
 ipv6 ospf 1 area 1
!
```

- Device B configuration file

```
!
ipv6 router ospf 1
 router-id 2.2.2.2
!
interface gigabitethernet 0/1
 ipv6 enable
 ipv6 address 2001:1::2/64
 ipv6 ospf 1 area 0
!
interface gigabitethernet 0/2
 ipv6 enable
 ipv6 address 2001:3::1/64
 ipv6 ospf 1 area 2
!
```

- Device C configuration file

```
!
```

```

ipv6 router ospf 1
  router-id 3.3.3.3
!
interface gigabitethernet 0/3
  ipv6 enable
  ipv6 address 2001:2::2/64
  ipv6 ospf 1 area 1
!

```

- Device D configuration file

```

!
ipv6 router ospf 1
  router-id 4.4.4.4
!
interface gigabitethernet 0/3
  ipv6 enable
  ipv6 address 2001:3::2/64
  ipv6 ospf 1 area 2
!

```

7. Common Errors

- No IPv6 address is configured for the interface.
- OSPFv3 cannot be enabled because the IPv6 unicast routing function is disabled.
- The area IDs configured for adjacent interfaces are inconsistent.
- The same router ID is configured on multiple devices, resulting in a router ID conflict.

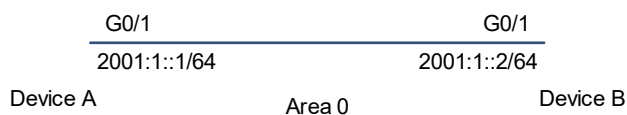
1.21.2 Configuring OSPFv3 Authentication

1. Requirements

OSPFv3 runs between Device A and Device B. MD5 authentication is configured to improve security of an OSPFv3 network.

2. Topology

Figure 1-1 Topology of OSPFv3 Authentication



3. Notes

Configure MD5 authentication on interfaces of all the devices.

4. Procedure

- (1) Configure basic OSPFv3 functions (omitted).
- (2) Enable OSPFv3 authentication on an interface.

Configure Device A.

```
Device A> enable
Device A# configure terminal
Device A(config)# interface gigabitethernet 0/1
Device A(config-if-GigabitEthernet 0/1)# ipv6 ospf authentication ipsec spi 256
md5 01234567890123456789012345678912
```

Configure Device B.

```
Device B> enable
Device B# configure terminal
Device B(config)# interface gigabitethernet 0/1
Device B(config-if-GigabitEthernet 0/1)# ipv6 ospf authentication ipsec spi 256
md5 01234567890123456789012345678912
```

5. Verification

Verify whether neighbors of Device A and Device B are established.

- Check the neighbor information of Device A.

```
Device A# show ipv6 ospf neighbor
OSPFv3 Process (1), 1 Neighbors, 1 is Full:
Neighbor ID      Pri   State           Dead Time   Instance ID  Interface
2.2.2.2          1    Full/DR         00:00:38   0            GigabitEthernet
0/1
```

- Check the neighbor information of Device B.

```
Device B# show ipv6 ospf neighbor
OSPFv3 Process (1), 1 Neighbors, 1 is Full:
Neighbor ID      Pri   State           Dead Time   Instance ID  Interface
1.1.1.1          1    Full/BDR        00:00:38   0            GigabitEthernet
0/1
```

6. Configuration Files

- Device A configuration file

```
!
interface gigabitethernet 0/1
    ipv6 ospf authentication ipsec spi 256 md5 01234567890123456789012345678912
!
```

- Device B configuration file

```
!
```

```
interface gigabitethernet 0/1
  ipv6 ospf authentication ipsec spi 256 md5 01234567890123456789012345678912
!
```

7. Common Errors

- The configured authentication modes are inconsistent.
- The configured authentication keys are inconsistent.

1.21.3 Configuring a Stub Area

1. Requirements

Devices A, B, C, and D are interconnected through the OSPFv3 routing protocol.

As ABRs, Devices A and B are responsible for the routing information transfer between OSPFv3 areas, and Device D functions as an ASBR to introduce the external static routes.

To reduce the number of LSAs in Area 1 and save the device performance, Area 1 is configured as a totally stub area.

2. Topology

Figure 1-1 Topology for a Stub Area

Totally stub area

3. Notes

- Configure IPv6 addresses on interfaces of all the devices.
- Configure the basic OSPFv3 functions for all the devices.
- Introduce an external static route to Device D.
- Configure Area 1 as a stub area on Device A and Device C.

4. Procedure

- (1) Configure IPv6 addresses on interfaces of all the devices and enable basic OSPFv3 functions (omitted).
- (2) Introduce an external static route to Device D.

```
Device D> enable
```

```
Device D# configure terminal
Device D(config)# ipv6 router ospf 1
Device D(config-router)# redistribute static
```

- (3) Configure Area 1 as a stub area on Device A and filter Type 3 LSAs.

```
Device A> enable
Device A# configure terminal
Device A(config)# ipv6 router ospf 1
Device A(config-router)# area 1 stub no-summary
```

- (4) Configure Area 1 as a stub area on Device C.

```
Device C> enable
Device C# configure terminal
Device C(config)# ipv6 router ospf 1
Device C(config-router)# area 1 stub
```

5. Verification

Run the **show ipv6 route ospf** command on Device C to display the routing table. Verify that there is only one default inter-area route, and no external static route is introduced from Device D.

```
Device C# show ipv6 route ospf

IPv6 routing table name - Default - 0 entries
Codes: C - Connected, L - Local, S - Static
        R - RIP, O - OSPFv3, B - BGP, I - IS-IS, V - Overflow route
        N1 - OSPFv3 NSSA external type 1, N2 - OSPFv3 NSSA external type 2
        E1 - OSPFv3 external type 1, E2 - OSPFv3 external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area

O IA::/0 [110/3] via FE80::2D0:F8FF:FE22:4547, GigabitEthernet 0/2
```

6. Configuration Files

- Device A configuration file

```
!
ipv6 router ospf 1
area 1 stub no-summary
!
```

- Device C configuration file

```
!
ipv6 router ospf 1
area 1 stub
!
```

- Device D configuration file

```
!
ipv6 router ospf 1
redistribute static
```

```
!
```

7. Common Errors

- Configurations of the area type are inconsistent on devices in the same area.
- External routes cannot be introduced because route redistribution is configured on a device in the stub area.

1.21.4 Configuring an NSSA

1. Requirements

Devices A, B, C, and D are interconnected through the OSPFv3 routing protocol.

As ABRs, Devices A and B are responsible for the routing information transfer between OSPFv3 areas, and Device D functions as an ASBR to introduce the external static routes.

To reduce the number of LSAs in Area 2 and save the device performance, Area 2 is configured as an NSSA.

2. Topology

Figure 1-1 Topology for an NSSA

NSSA

3. Notes

- Configure IPv6 addresses on interfaces of all the devices.
- Configure the basic OSPFv3 functions for all the devices.
- Introduce an external static route to Device D.
- Configure Area 2 as an NSSA on Device B and Device D.

4. Procedure

- (1) Configure IPv6 addresses on interfaces of all the devices and enable basic OSPFv3 functions (omitted).
- (2) Introduce an external static route to Device D. Configure Area 2 as an NSSA.

```
Device D> enable
Device D# configure terminal
Device D(config)# ipv6 router ospf 1
Device D(config-router)# area 2 nssa
Device D(config-router)# redistribute static
```

- (3) Configure Area 2 as an NSSA on Device B.


```

Device B> enable
Device B# configure terminal
Device B(config)# ipv6 router ospf 1
Device B(config-router)# area 2 nssa

```

5. Verification

- (1) Run the **show ipv6 ospf database** command on Device D to display the database information and verify that Type 7 LSAs are generated.

```

Device D# show ipv6 ospf database nssa-external
          OSPFv3 Router with ID (1.1.1.1) (Process 1)
          NSSA-external-LSA (Area 0.0.0.1)
LS age: 1196
LS Type: NSSA-external-LSA
Link State ID: 0.0.0.3
Advertising Router: 1.1.1.1
LS Seq Number: 0x80000004
Checksum: 0x1F25
Length: 52
  Metric Type: 2 (Larger than any link state path)
  Metric: 20
Prefix: 2001:10::/64
Prefix Options: 8 (P|-|-|-)
Forwarding Address: 4000::1

```

- (2) Run the **show ipv6 route ospf** command on Device A to display the routing table and verify that an external static route is introduced by Router D.

```

Device A# show ipv6 route ospf

IPv6 routing table name - Default - 0 entries
Codes: C - Connected, L - Local, S - Static
       R - RIP, O - OSPFv3, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPFv3 NSSA external type 1, N2 - OSPFv3 NSSA external type 2
       E1 - OSPFv3 external type 1, E2 - OSPFv3 external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area

O N2 2001:10::/64 [110/20] via FE80::2D0:F8FF:FE22:4547, GigabitEthernet 0/1

```

6. Configuration Files

- Device B configuration file

```

!
ipv6 router ospf 1
area 2 nssa
!

```

- Device D configuration file

```

!
```

```

ipv6 router ospf 1
area 2 nssa
 redistribute static
!

```

7. Common Errors

- Configurations of the area type are inconsistent on devices in the same area.

1.21.5 Selecting an OSPFv3 DR

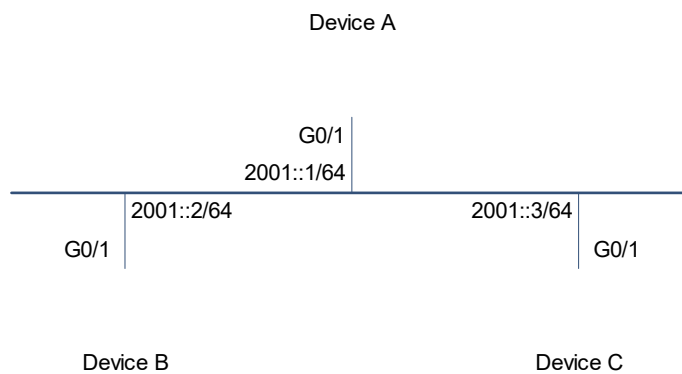
1. Requirements

Devices A, B, and C are in the same broadcast network.

The priority of Device A is set to 10 and Device A is configured as a DR. The priority of Device B is set to 5 and Device B is configured as a BDR. The priority of Device C is set to 0 and Device C does not participate in DR election.

2. Topology

Figure 1-1 Topology of OSPFv3 DR Configuration



3. Notes

- Configure IPv6 addresses on interfaces of all the devices.
- Configure the basic OSPFv3 functions for all the devices.
- Modify the DR election priority of all the devices.

4. Procedure

- Configure basic functions of OSPFv3.

Configure Device A.

```

Device A> enable
Device A# configure terminal
Device A(config)# ipv6 router ospf 1
Device A(config-router)# router-id 1.1.1.1
Device A(config-router)# exit

```

Configure Device B.

```
Device B> enable
Device B# configure terminal
Device B(config)# ipv6 router ospf 1
Device B(config-router)# router-id 2.2.2.2
Device B(config-router)# exit
```

Configure Device C.

```
Device C> enable
Device C# configure terminal
Device C(config)# ipv6 router ospf 1
Device C(config-router)# router-id 3.3.3.3
Device C(config-router)# exit
```

- (2) Configure IP addresses of interfaces, configure OSPFv3, and modify the DR election priority of all the devices.

Configure Device A.

```
Device A(config)# interface gigabitethernet 0/1
Device A(config-if-GigabitEthernet 0/1)# ipv6 address 2001::1/64
Device A(config-if-GigabitEthernet 0/1)# ipv6 ospf 1 area 0
Device A(config-if-GigabitEthernet 0/1)# ipv6 ospf priority 10
```

Configure Device B.

```
Device B(config)# interface gigabitethernet 0/1
Device B(config-if-GigabitEthernet 0/1)# ipv6 address 2001::2/64
Device B(config-if-GigabitEthernet 0/1)# ipv6 ospf 1 area 0
Device B(config-if-GigabitEthernet 0/1)# ipv6 ospf priority 5
```

Configure Device C.

```
Device C(config)# interface gigabitethernet 0/1
Device C(config-if-GigabitEthernet 0/1)# ipv6 address 2001::3/64
Device C(config-if-GigabitEthernet 0/1)# ipv6 ospf 1 area 0
Device C(config-if-GigabitEthernet 0/1)# ipv6 ospf priority 0
```

5. Verification

- Run the **show ipv6 ospf interface** command on Device C to display the DR and BDR.

```
Device C# show ipv6 ospf interface
GigabitEthernet 0/1 is up, line protocol is up
  Interface ID 4098
  IPv6 Prefixes
    fe80::250:56ff:feb5:820b/64 (Link-Local Address)
    2001::3/64
  OSPFv3 Process (1), Area 0.0.0.0, Instance ID 0
    Router ID 3.3.3.3, Network Type BROADCAST, Cost: 1
    Transmit Delay is 1 sec, State DROther, Priority 0
    Designated Router (ID) 1.1.1.1
      Interface Address fe80::250:56ff:feb5:694e
    Backup Designated Router (ID) 2.2.2.2
      Interface Address fe80::250:56ff:feb5:fdb4
```

```

Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Neighbor Count is 2, Adjacent neighbor count is 2
Hello received 73 sent 39, DD received 8 sent 7
LS-Req received 1 sent 2, LS-Upd received 9 sent 5
LS-Ack received 5 sent 5, Discarded 6

```

- Run the **show ipv6 ospf neighbor** command on Device A to display DROther of the broadcast network as Device C.

```

Device A# show ipv6 ospf neighbor

OSPFv3 Process (1), 2 Neighbors, 2 is Full:
Neighbor ID      Pri   State           BFD State  Dead Time   Instance ID
Interface
2.2.2.2          5    Full/BDR        -          00:00:36   0
GigabitEthernet 0/1
3.3.3.3          0    Full/DROther    -          00:00:38   0
GigabitEthernet 0/1

```

6. Configuration Files

- Device A configuration file

```

!
interface gigabitethernet 0/1
ipv6 address 2001::1/64
ipv6 ospf priority 10
ipv6 ospf 1 area 0
!
ipv6 router ospf 1
router-id 1.1.1.1
graceful-restart
!

```

- Device B configuration file

```

!
interface gigabitethernet 0/1
ipv6 address 2001::2/64
ipv6 ospf priority 5
ipv6 ospf 1 area 0
!
ipv6 router ospf 1
router-id 2.2.2.2
graceful-restart
!

```

- Device C configuration file

```

!
interface gigabitethernet 0/1
ipv6 address 2001::3/64

```

```

ipv6 ospf priority 0
ipv6 ospf 1 area 0
!
ipv6 router ospf 1
router-id 3.3.3.3
graceful-restart
!

```

1.21.6 Configuring BFD for OSPFv3

1. Requirements

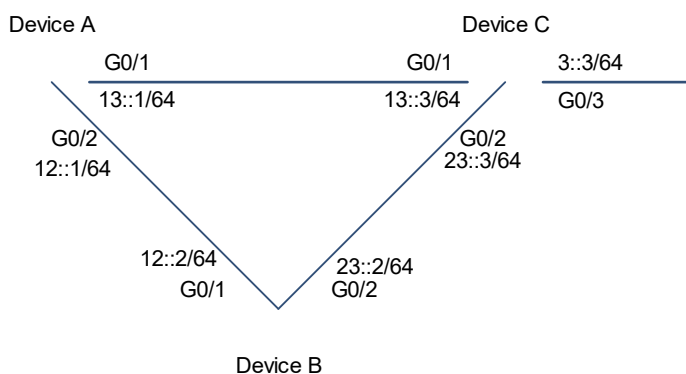
Devices A, B, and C are interconnected through OSPFv3.

The active link from Device A to 3::3 is Device A > Device C, and the standby link is Device A > Device B > Device C.

When the link from Device A to Device C fails, BFD can detect the failure and notify OSPFv3 of the failure, and quickly switch to the standby link.

2. Topology

Figure 1-1 Topology of BFD for OSPFv3



3. Notes

- Configure IPv6 addresses on interfaces of all the devices.
- Configure the basic OSPFv3 functions for all the devices.
- Enable the BFD function in the OSPFv3 routing process mode.

4. Procedure

- (1) Configure IP addresses for interfaces and configure basic OSPFv3 functions.

Configure Device A.

```

Device A> enable
Device A# configure terminal
Device A(config)# interface gigabitethernet 0/2
Device A(config-if-GigabitEthernet 0/2)# ipv6 address 12::1/64
Device A(config-if-GigabitEthernet 0/2)# ipv6 ospf 1 area 0

```

```

Device A(config-if-GigabitEthernet 0/2)# exit
Device A(config)# interface gigabitethernet 0/1
Device A(config-if-GigabitEthernet 0/1)# ipv6 address 13::1/64
Device A(config-if-GigabitEthernet 0/1)# exit
Device A(config)# ipv6 router ospf 1
Device A(config-router)# router-id 1.1.1.1

```

Configure Device B.

```

Device B> enable
Device B# configure terminal
Device B(config)# interface gigabitethernet 0/1
Device B(config-if-GigabitEthernet 0/1)# ipv6 address 12::2/64
Device B(config-if-GigabitEthernet 0/1)# ipv6 ospf 1 area 0
Device B(config-if-GigabitEthernet 0/1)# exit
Device B(config)# interface gigabitethernet 0/2
Device B(config-if-GigabitEthernet 0/2)# ipv6 address 23::2/64
Device B(config)# ipv6 router ospf 1
Device B(config-router)# router-id 2.2.2.2

```

Configure Device C.

```

Device C> enable
Device C# configure terminal
Device C(config)# interface gigabitethernet 0/1
Device C(config-if-GigabitEthernet 0/1)# ipv6 address 13::3/64
Device C(config-if-GigabitEthernet 0/1)# ipv6 ospf 1 area 0
Device C(config-if-GigabitEthernet 0/1)# exit
Device C(config)# interface gigabitethernet 0/2
Device C(config-if-GigabitEthernet 0/2)# ipv6 address 23::3/64
Device C(config-if-GigabitEthernet 0/2)# ipv6 ospf 1 area 0
Device C(config-if-GigabitEthernet 0/2)# exit
Device C(config)# ipv6 router ospf 1
Device C(config-router)# router-id 3.3.3.3

```

- (2) Enable the BFD function in the OSPFv3 routing process mode.

Configure Device A.

```
Device A(config-router)# bfd all-interfaces
```

Configure Device B.

```
Device B(config-router)# bfd all-interfaces
```

Configure Device C.

```
Device C(config-router)# bfd all-interfaces
```

5. Verification

- Normal network environment

Check the routing table of Device A.

```
Device A# show ipv6 route ospf
```

```

IPv6 routing table name - Default - 11 entries
Codes: C - Connected, L - Local, S - Static
       R - RIP, O - OSPFv3, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPFv3 NSSA external type 1, N2 - OSPFv3 NSSA external type 2
       E1 - OSPFv3 external type 1, E2 - OSPFv3 external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area, EV - BGP EVPN, N - Nd to host

O      3::3/128 [110/1] via FE80::2D0:F8FF:FE22:358D, GigabitEthernet 0/1
O      23::/64 [110/2] via FE80::2D0:F8FF:FE22:358D, GigabitEthernet 0/1
      [110/2] via FE80::274:9CFF:EEEE:53CB, GigabitEthernet 0/2

```

Run **traceroute 3::3** on Device A.

```

Device A# traceroute 3::3
  < press Ctrl+C to break >
Tracing the route to 3::3

 1                               3::3      5 msec    8 msec    10 msec

```

- Link from Device A to Device C fails

Check the routing table of Device A.

```

Device A# show ipv6 route ospf

IPv6 routing table name - Default - 7 entries
Codes: C - Connected, L - Local, S - Static
       R - RIP, O - OSPFv3, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPFv3 NSSA external type 1, N2 - OSPFv3 NSSA external type 2
       E1 - OSPFv3 external type 1, E2 - OSPFv3 external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area, EV - BGP EVPN, N - Nd to host

O      3::3/128 [110/2] via FE80::274:9CFF:EEEE:53CB, GigabitEthernet 0/2
O      23::/64 [110/2] via FE80::274:9CFF:EEEE:53CB, GigabitEthernet 0/2

```

Run **traceroute 3::3** on Device A.

```

Device A# traceroute 3::3
  < press Ctrl+C to break >
Tracing the route to 3::3

 1                               12::2      6 msec    9 msec    9 msec
 2                               3::3      7 msec    9 msec   10 msec

```

6. Configuration Files

- Device A configuration file

```

!
interface gigabitethernet 0/1
ipv6 address 13::1/64

```

```
ipv6 ospf 1 area 0
!
interface gigabitethernet 0/2
ipv6 address 12::1/64
ipv6 ospf 1 area 0
!
ipv6 router ospf 1
  router-id 1.1.1.1
  graceful-restart
  bfd all-interfaces
!
```

- Device B configuration file

```
!
interface gigabitethernet 0/1
ipv6 address 12::2/64
ipv6 ospf 1 area 0
!
interface gigabitethernet 0/2
ipv6 address 23::2/64
ipv6 ospf 1 area 0
!
ipv6 router ospf 1
  router-id 2.2.2.2
  graceful-restart
  bfd all-interfaces
!
```

- Device C configuration file

```
!
interface gigabitethernet 0/1
ipv6 address 13::3/64
ipv6 ospf 1 area 0
!
interface gigabitethernet 0/2
ipv6 address 23::3/64
ipv6 ospf 1 area 0
!
ipv6 router ospf 1
  router-id 3.3.3.3
  graceful-restart
  bfd all-interfaces
!
```

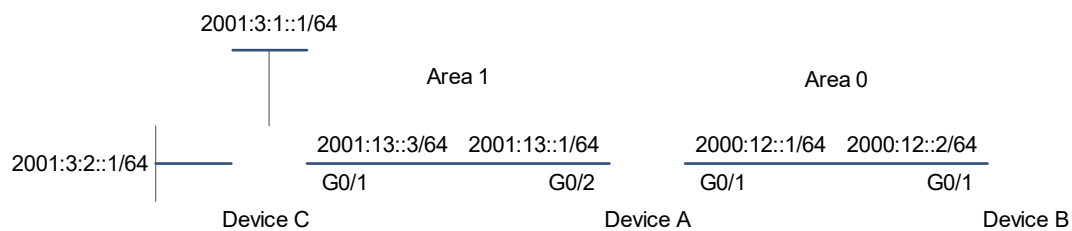

1.21.7 Configuring OSPFv3 Route Summarization

1. Requirements

Devices A and B reside in OSPFv3 Area 0, and Devices A and C reside in OSPFv3 Area 1. Two static routes are introduced to Device C. To reduce the number of routing entries, Device C summarizes introduced static routes as 2001:3::/32 and advertises the routes to the OSPFv3 domain. Device A summarizes routes in Area 1 as 2001:13::/32 and advertises the routes to the OSPFv3 neighbors.

2. Topology

Figure 1-1 Topology of OSPFv3 Route Summarization



3. Notes

- Configure IPv6 addresses on interfaces of all the devices.
- Configure the basic OSPFv3 functions for all the devices.
- Redistribute two static routes on Device C and configure external route summarization.
- Summarize routes in Area 1 on Device A.

4. Procedure

- (1) Configure basic functions of OSPFv3 (omitted).
- (2) Redistribute two static routes on Device C and summarize the redistributed routes as 2001:3::/32.

```
Device C> enable
Device C# configure terminal
Device C(config)# ipv6 router ospf 1
Device C(config-router)# redistribute static
Device C(config-router)# summary-prefix 2001:3::/32
```

- (3) Summarize routes in Area 1 as 2001:13::/32 on Device A.

```
Device A> enable
Device A# configure terminal
Device A(config)# ipv6 router ospf 1
Device A(config-router)# area 1 range 2001:13::/32
```

5. Verification

- Display OSPFv3 routes on Device A. Summarized static routes are displayed, and route details cannot be displayed.

```

Device A# show ipv6 route ospf

IPv6 routing table name - Default - 11 entries
Codes: C - Connected, L - Local, S - Static
        R - RIP, O - OSPFv3, B - BGP, I - IS-IS, V - Overflow route
        N1 - OSPFv3 NSSA external type 1, N2 - OSPFv3 NSSA external type 2
        E1 - OSPFv3 external type 1, E2 - OSPFv3 external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area, EV - BGP EVPN, N - Nd to host

O E2 2001:3::/32 [110/20] via FE80::250:56FF:FEB5:7BF5, GigabitEthernet 0/2
O    2001:13::/32 [110/0] via ::1, Null0

```

- Display OSPFv3 routes on Device B. Area 1 summarized routes are displayed, and route details cannot be displayed.

```

Device B# show ipv6 route ospf

IPv6 routing table name - Default - 7 entries
Codes: C - Connected, L - Local, S - Static
        R - RIP, O - OSPFv3, B - BGP, I - IS-IS, V - Overflow route
        N1 - OSPFv3 NSSA external type 1, N2 - OSPFv3 NSSA external type 2
        E1 - OSPFv3 external type 1, E2 - OSPFv3 external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area, EV - BGP EVPN, N - Nd to host

O E2 2001:3::/32 [110/20] via FE80::250:56FF:FEB5:694E, GigabitEthernet 0/1
O IA 2001:13::/32 [110/2] via FE80::250:56FF:FEB5:694E, GigabitEthernet 0/1

```

6. Configuration Files

- Device A configuration file

```

!
router-id 1.1.1.1
graceful-restart
area 1 range 2001:13::/32
!

```

- Device C configuration file

```

!
router-id 3.3.3.3
graceful-restart
redistribute static
summary-prefix 2001:3::/32
!

```