Contents

1 Configuring OSPF v2

1.1 Introduction

1.1.1 Overview

The open shortest path first (OSPF) 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.

In the early stage after dynamic routing emerges, Routing Information Protocol (RIP) was mainly used on the network. RIP is a distance vector routing protocol, facing some problems such as slow convergence, routing loop, poor scalability, and use for simple networks only. OSPF Version 2 (OSPFv2) is a link state routing protocol, which can effectively fix the above problems. Therefore, OSPFv2 is widely used on large and medium-sized networks.

Note

- OSPFv2 is applicable to IPv4, and OSPF Version 3 (OSPFv3) is applicable to IPv6. The protocol running mechanism and most configurations are the same.
- Unless otherwise specified, "OSPF" in the following descriptions refers to OSPFv2.

OSPF has the following characteristics:

- Wide scope of application: OSPF 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: OSPF supports equivalent routes.
- Authentication: OSPF 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 switches, routers, or firewalls.

1.1.2 Principles

1. Simple Principles

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

(1) Neighbor discovery → Bidirectional communication: An OSPF neighbor relationship is set up between adjacent routers, and bidirectional communication is maintained.

(2) Database synchronization → Full adjacency: A router uses link-state advertisements (LSAs) to advertise all its link states. LSAs are exchanged between neighbors and the link state database (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 OSPF routing table.

- Neighbor discovery → Bidirectional communication

  Routers send hello packets through all OSPF-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. Routers that are mutual neighbors find their own router IDs from hello packets sent from neighbors, and bidirectional communication is set up.

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

  - Router ID of the originating router.
  - Area ID of the originating router interface or virtual link.
  - Subnet mask of the originating router interface or virtual link.
  - Authentication information of the originating router interface or virtual link.
  - Hello interval of the originating router interface or virtual link.
  - Neighbor dead interval of the originating router interface or virtual link.
  - IP addresses of the designated router (DR) and backup designated router (BDR).
  - Priority of the originating router interface (used for DR/BDR election).
  - Router ID of the neighbor of the originating router.

- Database synchronization → Full adjacency

  After bidirectional communication is established between neighbor routers, database description (DD), link state request (LSR), link state update (LSU), and link state acknowledgment (LSAck) packets are used to exchange LSAs and establish an adjacency relationship. 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.

ℹ Note

OSPF will not generate LSDB updates and advertisements without changes in link costs or network addition/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 costs. OSPF generates a routing table based on the SPT.

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

ℹ Note

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

---

2. Basic Concepts

- 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 on which OSPF runs is also called OSPF routing domain, or OSPF domain for short.

- OSPF process

  OSPF supports multiple instances, and each instance corresponds to an OSPF process. One or more OSPF processes can be started on a router. Each OSPF process runs OSPF independently, and the processes are mutually isolated. The process ID takes effect only on the local router, and does not affect exchange of OSPF packets on adjacent interfaces.

- Router ID

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

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

  A router ID can be manually configured or automatically selected by the router. You are advised to select manual configuration. If no router ID is specified manually, the automatic selection rules are as follows:

  a The largest IP address from the lookback interface addresses is selected as the router ID;

b If no lookback interface is configured, the largest IP address from the physical interface addresses is selected as the router ID.

- Area

  OSPF supports multiple areas. An OSPF 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 OSPF-enabled interface must belong to a specified area.

  - Backbone area and normal area

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

  - Stub area (OSPF stubby area)

    Configuring a stub area can reduce the number of 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.

  - Not-so-stubby area (NSSA)

    An NSSA is similar to a stub area, but allows the autonomous system boundary router (ASBR). The route redistributed by ASBR will be transferred in the NSSA area in the form of Type-7 LSA, and the Type-7 LSA will be converted into Type-5 LSA on ABR and then transferred to other areas. The ABR also advertises the default route to the NSSA.

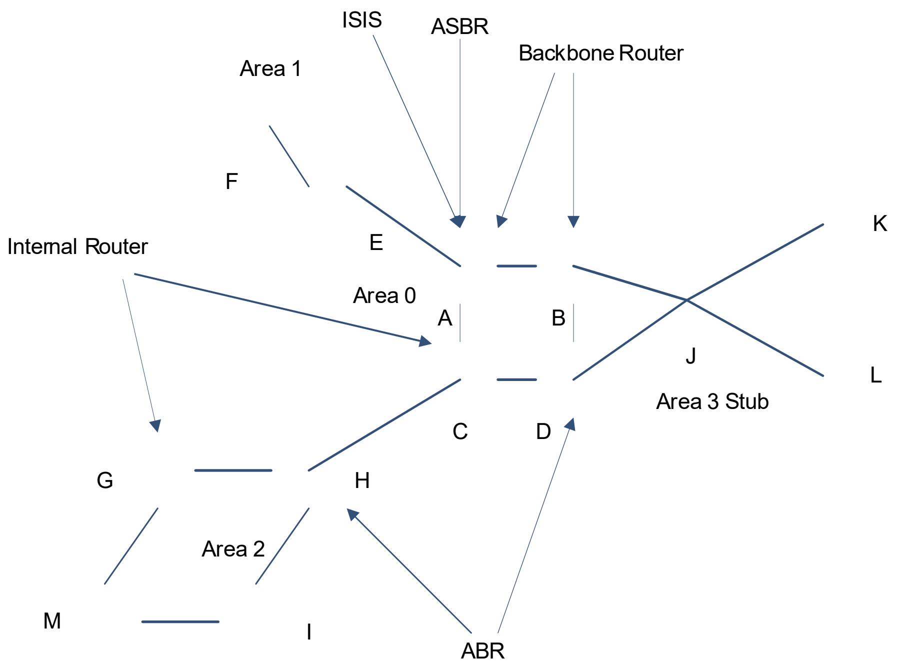
  - Totally NSSA

    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.

Note

- 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.

Figure 1-2 OSPF Areas



- OSPF routers

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

  - Internal router

    All interface of an interval router belong to the same OSPF area. See A, C, F, G, I, M, J, K, and L shown in Figure 1-2.

  - 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. See B, D, E, and H shown in Figure 1-2.

  - 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. See A, B, C, D, E, and H shown in Figure 1-2.

  - 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. See A shown in Figure 1-2.

- OSPF route types

  A mark is displayed in front of each OSPF route to indicate the type of the route. There are six types of OSPF 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.

- IA: 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.

- E1: 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.

- E2: 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.

- N1: 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 area. 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.

- N2: 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 E2 and N2 routes is poor. OSPF believes that the cost of the route from the ASBR to a destination 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 outside an AS is considered.

- OSPF packets

  OSPF packets are encapsulated in IP packets and transmitted in multicast or unicast mode. When the interfaces running the OSPF process on any network belong to this group, the router running the OSPF process receives all the multicast packets of 224.0.0.5; when the router is used as a DR/BDR on a multi-access network, 224.0.0.6 is used as the multicast receiving address. The OSPF data packet format is shown as follows:

Figure 1-3 OSPF Packet Format

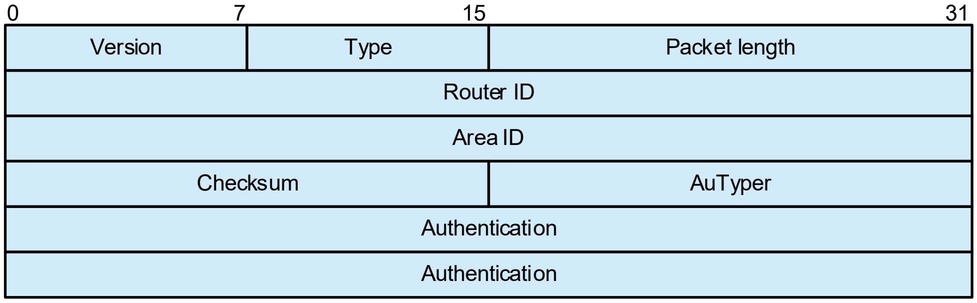


Table 1-1 Description of OSPF Packet Format Fields

Packet Field	Description
Version	Indicates the OSPF version No. The value of OSPFv2 is 2.
Type	Indicates the type of OSPF packet: 1: Indicates hello packet. 2: Indicates DD packet. 3: Indicates LSR packet. 4: Indicates LSU packet. 5: Indicates LSAck packet.
Packet length	Indicates the total length of the OSPF packet including the header, in bytes.
Router ID	Indicates the ID of the router sending the packet.
Area ID	Indicates the area of the router sending the packet.
Checksum	Indicates the checksum of the whole packet excluding the authentication field.
AuType	Indicates the authentication type: 0: Indicates no authentication. 1: Indicates simple authentication. 2: Indicates MD5 authentication.
Authentication	The meaning of this field varies with the authentication type: No authentication: This field is not defined. Simple authentication: This field indicates the password. MD5 authentication: This field includes the key ID, MD5 authentication data length, and sequence number information.

OSPF involves the following five types of packets:

Table 1-2 Types of OSPF Packets

Packet Type	Description
Hello	Hello packets are sent periodically to discover and maintain OSPF neighbor relationships.
DD	DD packets carry brief information about the local LSDB and are used to synchronize the LSDBs between OSPF neighbors.
LSR	LSR packets are used to request the required LSAs from neighbors. LSR packets are sent only after DD packets are exchanged successfully between OSPF neighbors.
LSU	LSU packets are used to send the required LSAs to peers.
LSAck	LSAck packets are used to acknowledge the received LSAs.

- LSA

OSPF describes the routing information by means of LSA.

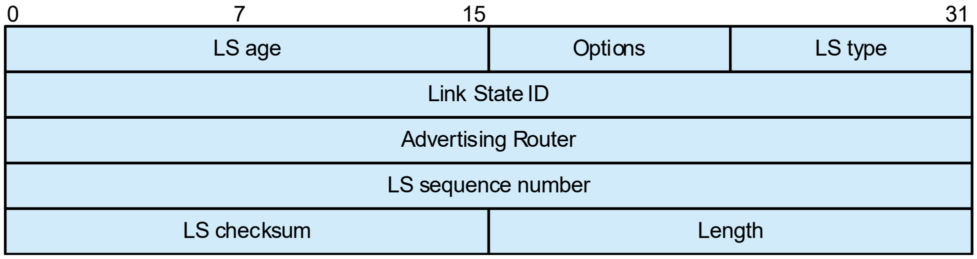
Table 1-3 Types of OSPF LSAs

LSA Type	Description
Router-LSA (Type 1)	This LSA is originated by each 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 (Type 2)	This LSA is originated by a DR on the non-broadcast multiple access (NBMA) network. It describes the link state in the current network segment, and is advertised only within the area where the DR is located.
Network-summary-LSA (Type 3)	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.
ASBR-summary-LSA (Type 4)	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 (Type 5)	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 (Type 7)	This LSA is originated by an ASBR. It describes a route to a destination outside the AS, and is advertised only within the NSSA.
Opaque LSA (Type 9/Type	Opaque LSAs provide a generalized mechanism to allow for the future

LSA Type	Description
10/Type 11)	extensibility of OSPF, wherein: ● Type-9 LSAs are advertised only within the network segment where interfaces are located. The grace LSA used to support graceful restart (GR) is one of Type-9 LSAs. ● Type-10 LSAs are advertised within an area. The LSA used to support traffic engineering (TE) is one of Type-10 LSAs. ● Type-11 LSAs are advertised within an AS. At present, there are no application examples of Type-11 LSAs.

Stub areas, NSSAs, totally stub areas, and totally NSSAs are special forms of normal areas and help reduce the number of LSAs transferred in an OSPF area, alleviate the load of routers, and enhance the stability of OSPF routes.

Figure 1-4 LSA Packet Header Format



- OSPF neighbor state

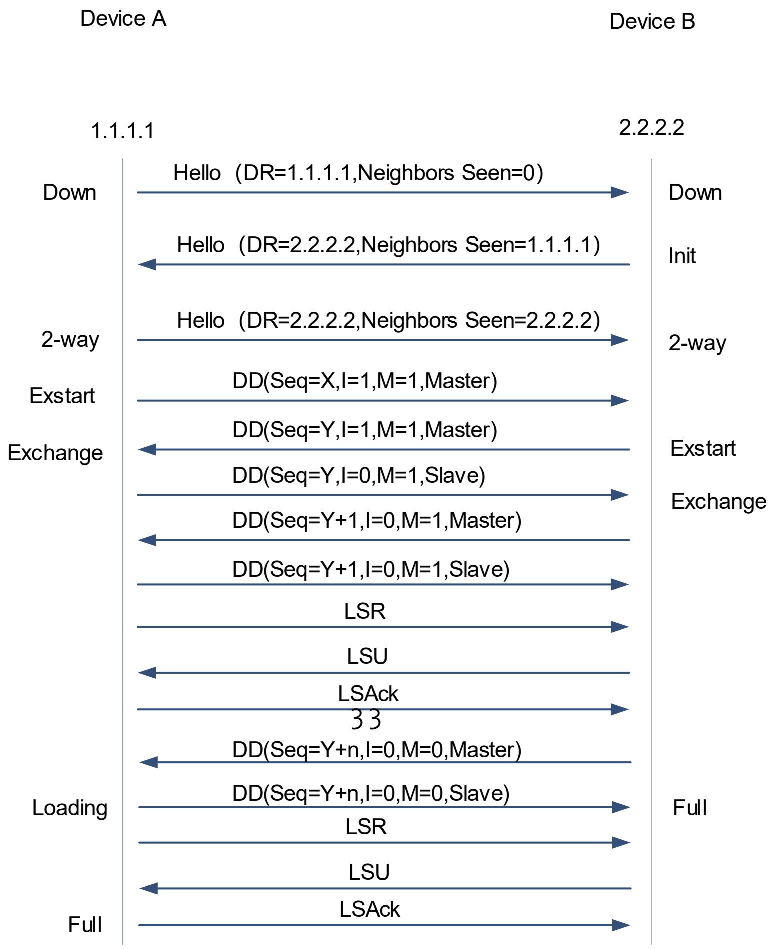
On the OSPF network, neighbor devices need to reach the adjacency state before exchanging link information. There are several OSPF neighbor states listed below. When a neighbor enters the full state, the adjacency relationship is established. Figure 1-5 shows the adjacency establishment process.

Table 1-1 OSPF Neighbor State Machine and Description

State	Description
Down	The state of the First OSPF 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

State	Description
	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 BDR will be selected for broadcast and non-broadcast multi-access.
Exstart	Indicates negotiation about the master/slave relationship. ● Selects the initial sequence number for forming an adjacency. ● 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.

Figure 1-5 OSPF Adjacency Establishment Process on Broadcast Network


Device A
Device B
1.1.1.1
2.2.2.2
Down
Hello (DR=1.1.1.1,Neighbors Seen=0)
Down
Hello (DR=2.2.2.2,Neighbors Seen=1.1.1.1)
Init
2-way
Hello (DR=2.2.2.2,Neighbors Seen=2.2.2.2)
2-way
Exstart
DD(Seq=X,I=1,M=1,Master)
Exchange
DD(Seq=Y,I=1,M=1,Master)
Exstart
DD(Seq=Y,I=0,M=1,Slave)
Exchange
DD(Seq=Y+1,I=0,M=1,Master)
DD(Seq=Y+1,I=0,M=1,Slave)
LSR
LSU
LSAck
33
DD(Seq=Y+n,I=0,M=0,Master)
Loading
DD(Seq=Y+n,I=0,M=0,Slave)
Full
LSR
LSU
Full
LSAck

- OSPF 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, OSPF 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 fiber distributed data interface (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 OSPF Network Types

Network Type	Link Layer Protocol	Neighbor Relationship and DR Election
Broadcast	Ethernet and FDDI belong to the broadcast network type by default.	● Neighbors are 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

Network Type	Link Layer Protocol	Neighbor Relationship and DR Election
		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.	● 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.	● 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.	● 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.	● 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.

- DR and BDR

  On 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*(n-1)/2 adjacency relationships will be set up, and n^2 LSAs will be generated on 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, OSPF 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 DR Other. DR Other 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, as shown in Figure 1-6 and Figure 1-7.

Figure 1-6 Number of Adjacency Relationships Before DR Election

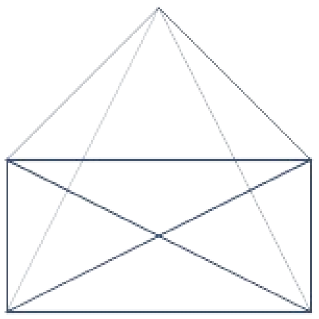
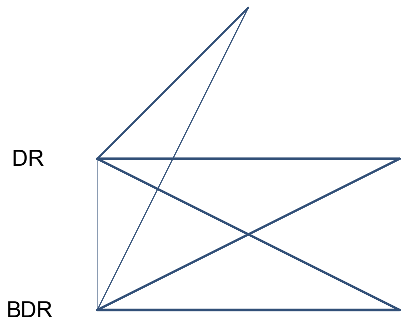


Figure 1-7 Number of Adjacency Relationships After DR Election

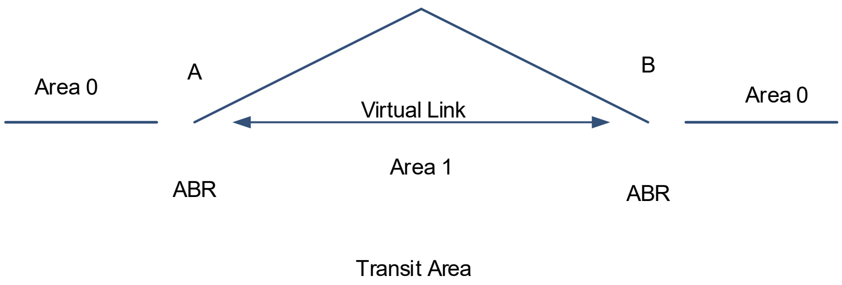


- Virtual link

  OSPF 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.

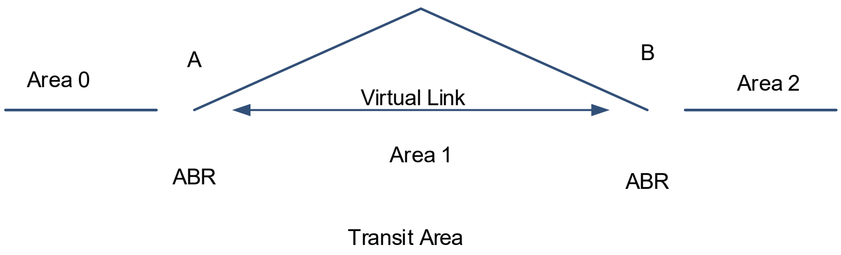
  A virtual link relies on an OSPF intra-domain route, making two ABRs adjacent. The OSPF packet information exchanged by ABRs is transparent to the intermediate device.

Figure 1-8 Discontinuous Backbone Area on the Physical Network



As shown in Figure 1-8, 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 1-9 Failure to Directly Connect a Normal Area to the Backbone Area on the Physical Network



As shown in Figure 1-9, 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.

3. OSPF Routing

- Route cost

  If redundancy links or devices exist on the network, multiple paths may exist from the local device to the destination network. OSPF selects the path with the minimum total cost to form an OSPF 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, OSPF selects this path to form a route.

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

  - Cost from an interface to a directly connected network segment and cost from the interface to a neighbor.
  - Cost from an ABR to the inter-area summarization network segment and cost from the ABR to the default network segment.

  - ○ Cost from an ASBR to an external network segment and cost from the ASBR to the default network segment.

Note

Cost value refers to the cost of a link and the link quality value after calculation. Metric is the cost of a complete path and the total cost of the links passed.

- OSPF management distance

  The management distance (AD) evaluates reliability of a route. Its value is an integer ranging from 0 to 255. A smaller AD value indicates that the route is more trustworthy. If multiples exist to the same destination, the route 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 Management Distances

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

4. OSPF Route Advertisement

- Route redistribution

  Route redistribution refers to the process of introducing routes of other routing protocols, routes of other OSPF processes, static routes, and direct routes that exist on the device to an OSPF 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 OSPF 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.

5. OSPF Route Summarization

Route summarization is a process of summarizing routing information with the same prefix into one route, and advertising the summarized route to neighbors by replacing a large number of individual routes. 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.

When configuring route summarization, the summarization range may exceed the actual network scope of routes. If the 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, ABR or ASBR will automatically add a discard route to the routing table. This route will not be advertised.

6. OSPF Route Filtering

OSPF allows filtering of 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 any LSAs or exchanging any LSAs with neighbors.
- Routing information advertised between areas: Only the Type-3 LSA that meets the filtering conditions can be advertised to another area.
- Routing information outside an AS: Only the Type-5 and Type-7 LSAs that meet the filtering conditions can be redistributed to the OSPF process.
- LSAs received by a router: In the OSPF routing table, only the routes that are computed based on the LSAs meeting the filtering conditions can be advertised.

7. 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	Types 1 and 2	Type 3	Type 4	Type 5	Type 7
Non-stub/totally stub area and non-NSSA/totally NSSA	Allowed	Allowed	Allowed	Allowed	Not allowed
Stub area	Allowed	Allowed (containing one	Not	Not	Not

Area	Types 1 and 2	Type 3	Type 4	Type 5	Type 7
		default route)	allowed	allowed	allowed
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 converts Type-7 LSAs in the NSSA/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 E1, E2, and IA 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 IA: a route to a destination network in another area E1 or E2: 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 IA: a route or a default route to a destination network in another area
Totally stub area	O: a route to a destination network in the local area IA: a default route
NSSA	O: a route to a destination network in the local area IA: a route or a default route to a destination network in another area N1 or N2: a route or default route to a destination network segment outside the AS (via an ASBR in the local area)

Area	Routes Available in the Routing Table of a Router Inside the Area
Totally NSSA	O: a route to a destination network in the local area IA: a default route N1 or N2: a route or default route to a destination network segment outside the AS (via an ASBR in the local area)

8. Enhanced Security and Reliability

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

- Authentication

  Authentication prevents routers that illegally access the network and hosts that forge OSPF packet from participating in the OSPF process. OSPF packets received on the OSPF interface or at both ends of the 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. On 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 type is configured in OSPF routing process mode.
  - Interface authentication: This neighbor-level authentication authenticates the packets transmitted on the related interface. This type is configured in interface mode.

- MTU verification

  Upon receiving a DD packet, OSPF 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.

- Source address verification

  Generally, the source address of a packet received by OSPF is in the same network segment as the receiving interface. The addresses at both ends of a P2P link are configured separately and are not necessarily in the same network segment. In this scenario, as the peer address information will be notified during the P2P link negotiation process, OSPF checks whether the source address of the packet is the address advertised by the peer during negotiation. If not, OSPF determines that the packet is invalid and discards this packet. In particular, OSPF never verifies the address of an interface not configured with an IP address.

In some scenarios, the source address of a packet received by OSPF may not be in the same network segment as the receiving interface, so the OSPF address verification fails. For example, the negotiated peer address cannot be obtained on a P2P link. In this scenario, source address verification must be disabled to ensure that the OSPF adjacency can be properly set up.

- Two-way maintenance

  OSPF routers periodically send hello packets to each other to maintain the adjacency. On 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 neighbor 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 OSPF process is restricted, the router can interact with neighbors by batches, which ensures data forwarding and other key services.

- Overflow

  OSPF requires that routers in the same area store the same LSDB. The number of routers keeps increasing on the network. Some routers, however, cannot store so much routing information due to the limited system resources. The large amount of routing information may exhaust the system resources of routers, causing failures of the routers.

  The overflow function limits the number of external routes in the LSDB to control the size of the LSDB.

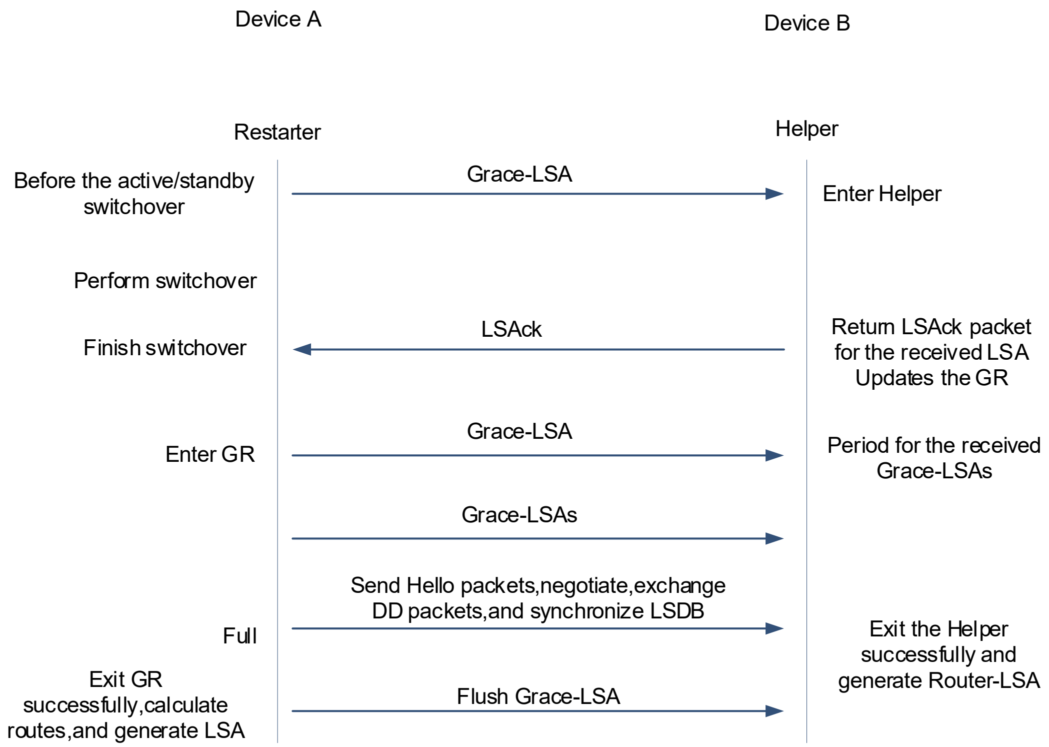
  When the number of external routes on a router exceeds the upper limit, the router enters the overflow state. The router deletes the external routes generated by itself from the LSDB, and does not generate new external routes. In addition, the router discards the newly received external routes. After the overflow state timer (5s) expires, if the number of external routes is lower than the upper limit, the normal state is restored.

- GR

  The control and forwarding separated technology is widely used among routers. On a relatively stable network topology, when a 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 OSPF GR Process


Device A
Device B
Restarter
Helper
Before the active/standby switchover
Grace-LSA
Enter Helper
Perform switchover
Finish switchover
LSAck
Return LSAck packet for the received LSA Updates the GR
Enter GR
Grace-LSA
Period for the received Grace-LSAs
Grace-LSAs
Send Hello packets,negotiate,exchange DD packets,and synchronize LSDB
Full
Exit the Helper successfully and generate Router-LSA
Exit GR successfully,calculate routes,and generate LSA
Flush Grace-LSA

- 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.

- NSR

  During nonstop routing (NSR), OSPF-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. The specific information of NSR active/standby synchronization includes configuration information backup, process information backup, interface information backup, neighbor information backup, and LSA information backup.

- Fast hello correlation with BFD and fast reroute

  After a link fails, it takes a period of time (about 40s) before OSPF can sense the failure of the neighbor. Then, OSPF 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), OSPF can sense the failure of the neighbor within 1s once a link is faulty. This greatly 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 OSPF is correlated with BFD, OSPF can sense the failure of a neighbor in as short as 150 ms once a link is faulty. This greatly accelerates route convergence and prevents traffic interruption.
  - Fast reroute prepares a backup route for OSPF. Once the OSPF senses the failure of a neighbor, the traffic is immediately switched over to the standby route, thus preventing traffic interruption.

- iSPF feature
  - The OSPF topology is area based. The SPF algorithm is run for independent computation in each area. The standard SPF algorithm re-computes the topology of the entire area each time even if only the leave nodes change in the area topology.
  - When computing the network topology, the incremental shortest path first (iSPF) method corrects only the nodes on the SPT that are affected by the topology changes, and does not re-build the entire SPT. This can effectively ease the pressure on the router processors on a large network, especially when the network is not stable.

- Fast convergence

  When a link or a router on the OSPF network fails, the packets that need to be transmitted through the faulty link or the faulty router to reach the destination will be lost or cause a routing loop, and the data traffic will be interrupted. The interrupted traffic cannot resume normal transmission until OSPF completes convergence according to the new topology network.

  To minimize the traffic interruption time caused by a network failure, the administrator can configure the OSPF fast reroute or fast hello function to speed up network convergence.

9. Network Management Functions

Functions such as management information base (MIB) and Syslog are used to facilitate OSPF 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 OSPF processes can be simultaneously started on a router, but the OSPF MIB can be bound to only one OSPF 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 that the OSPF adjacency is set up and maintained.

10. VPN Extended Feature of OSPF

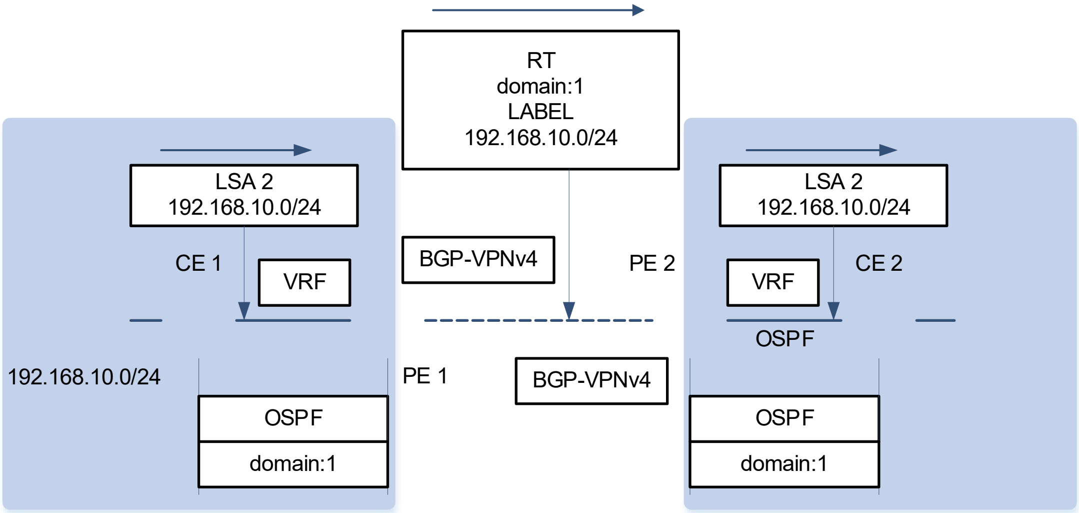
OSPF is a widely used IGP. In most of the existing application solutions, OSPF is generally selected as an internal routing protocol for VPN users. If OSPF is also used between PEs and CEs, other routing protocols are not needed, which simplifies the configuration and management of CEs.

- Domain ID

A domain ID refers to the ID of an OSPF domain to which a route belongs. When a CE learns an OSPF route in a VPN internal site, and this route is advertised to a PE as a Type-1/2/3 LSA, and is redistributed to the Border Gateway Protocol (BGP) domain and converted into a VPN route, the domain ID is also redistributed to the BGP domain along with the route. Then, this domain is also advertised as the extcommunity attribute of the VPN route. When another PE receives this VPN route and redistributes it to a VRF OSPF process, the domain ID is redistributed to the VRF OSPF process along with the route. If the VRF OSPF process confirms that the domain ID in the route is the same as that in the local VRF OSPF process, it advertises the route to the CE as an internal route. If the VRF OSPF process confirms that the domain ID in the route is different from that in the local VRF OSPF process, the VRF OSPF process advertises the route to the CE as an external route.

As shown in Figure 1-1, for internal routes belonging to the same OSPF domain, CE1 advertises the routes to PE1 as Type-2 LSAs, which are converted into VPN routes and advertised to PE2. After receiving the routes, PE2 redistributes them to the VRF OSPF process. The domain IDs in the VRF OSPF process are the same as those of the VPN routes, and therefore, the VPN routes are advertised to the VPN site as internal routes.

Figure 1-1 Diagram of Domain ID

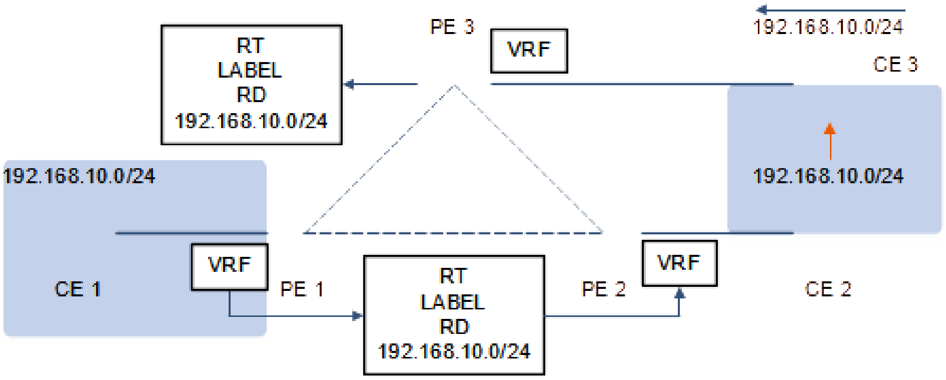


- DN bit technology

  The DN bit is a loop detection technology running the OSPF protocol between a PE and a CE. In some scenarios, loops may arise when OSPF runs between a PE and a CE, for example, multiple CEs are connected to one VPN site. If one PE advertises learned VPN routes to the VPN site, and the VPN site advertises the routes to another PE via OSPF, a loop may occur.

  As shown in Figure 1-2, PE1 advertises the 192.168.10.0/24 route to PE2 and PE3, CE2 advertises the route to CE3 via OSPF, and CE3 advertises the route to PE3, which redistributes the route to the BGP domain of PE3. PE3 selects the route that is redistributed via OSPF and converts this route into a VPNv4 route for advertisement. As a result, a loop may occur.

Figure 1-2 Diagram of DN Bit Technology



For this, when a PE advertises a Type-3/5/7 LSA to a CE, the DN bit is set to ON in the optional field of the LSA, to prevent possible loops. When an LSA received by another PE contains the DN bit in the optional field, the OSPF of the PE will not use this LSA for OSPF calculation.

- VPN router tag

  Router-tag is another loop detection technology running OSPF between a PE and a CE. When OSPF runs between a PE and a CE, the VRF OSPF process of the PE has a router tag by default, which is called VPN router tag. When a VPN route is imported into the VRF OSPF process of a PE and is converted into a Type-5/7 LSA and advertised to a CE, the LSA carries the VPN router-tag. When multiple PEs are connected to one VPN site, if the Type-5/7 LSA received by a PE contains the VPN router tag and the VPN router tag is the same as the VPN router tag of the OSPF process, the LSA will not be used for OSPF route calculation.

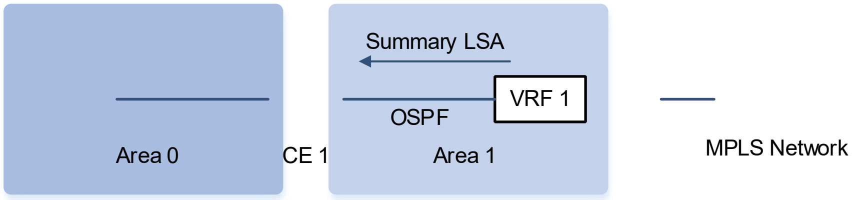
- Area deployment

  In normal cases, links between a PE and a CE may belong to any OSPF area. If links between a PE and a CE belong to a non-zero area, the PE is an ABR for the OSPF area where the CE resides. This may cause problems because the ABR running OSPF has the following features:

  - The ABR calculates Type-3 LSAs in the backbone area only.
  - The ABR forwards only Type-3 LSAs in the backbone area to a non-backbone area.

As shown in Figure 1-3, if the link between a PE and a CE belongs to a non-zero area, the PE redistributes the VPNv4 routes advertised by Multiprotocol Extensions for BGP (MP-BGP) to the OSPF domain, restores them to type-3 LSAs, and advertises them to CE1. CE1 does not calculate LSAs in non-backbone areas. Therefore, these LSAs are not advertised to routers in Area 0 and the VPN internal sites cannot learn routes of other sites. Therefore, exercise caution during the deployment when the links between a PE and a CE belong to a non-zero area.

Figure 1-3 Diagram of Area Deployment

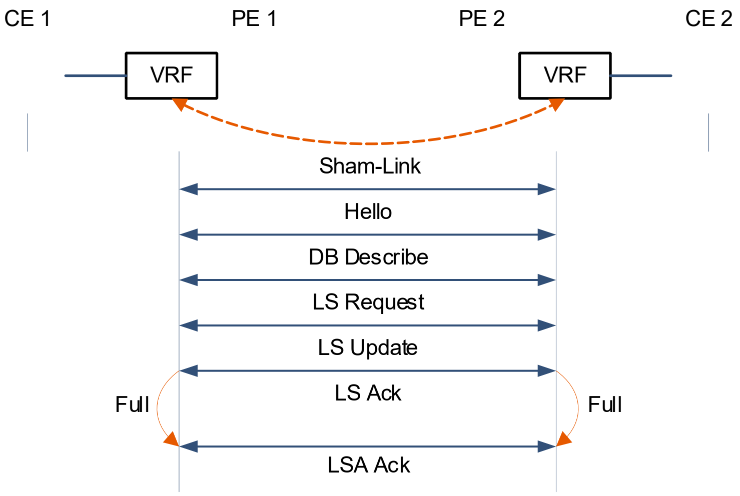


In L3VPN application, if OSPF is run between a PE and a CE to exchange VPN routes, do not deploy the backbone area at VPN internal sites if possible. If a router at a VPN internal site belongs to a backbone area in addition to a PE, at least one router series product at the VPN internal site must be connected to the PE and the links between the CE and PE must belong to Area 0. In this way, inter-area routes and external routes can be transmitted between the PE and the VPN site.

- Sham link

The sham link is not a real link but a virtual link established between VRF instances of two PEs. Like a normal OSPF link, a sham link has its OSPF interfaces, and is capable of sending OSPF protocol packets, establishing neighbor relationships, and sending LSAs. When LSAs are flooded on a sham link, no types of the OSPF routes will change, as shown in Figure 1-4.

Figure 1-4 Diagram of Sham Link



The purposes of establishing sham-links between VRF OSPF processes of different PEs are as follows:

- When the Multiprotocol Interior Border Gateway Protocol (MP-IBGP) is used to carry private routes, it only transfers routes; after the routes reach the peer PE and restored, MP-IBGP imports the original OSPF routes in a best-effort manner, and the OSPF topology information cannot be communicated properly. With sham-link, an OSPF link can be established to implement actual interworking between OSPF processes at each site and establish a complete topology.
- Different sites in the same VPN exchange information via the MPLS backbone network. One link is connected between these VPN sites. The purpose of this link is that VPN sites can communicate with each other through this link when the MPLS backbone network is unavailable. This link is called backdoor link.

If two VPN sites belong to the same OSPF area and one backdoor link is connected in between, routes inside the two sites are exchanged through both the MPLS backbone network and the backdoor link. Routes exchanged through the MPLS backbone network are inter-domain routes while routes exchanged through the backdoor link are intra-domain routes. The intra-domain routes advertised by the backdoor link are prior to the inter-domain routes advertised by the MPLS backbone network. Therefore, the forwarding of the routes inside the two sites takes the backdoor link first, which is against the intention of backdoor link connection for VPN users. In this case, a sham link is also required.

1.1.3 Protocols and Standards

- RFC2328: OSPF Version 2
- RFC2370: This memo defines enhancements to the OSPF protocol to support a new class of link-state advertisements (LSA) called Opaque LSAs. Opaque LSAs provide a generalized mechanism to allow for the future extensibility of OSPF.
- RFC3137: This memo describes a backward-compatible technique that may be used by OSPF (Open Shortest Path First) implementations to advertise unavailability to forward transit traffic or to lower the preference level for the paths through such a router.
- RFC3623: This memo documents an enhancement to the OSPF routing protocol, whereby an OSPF router can stay on the forwarding path even as its OSPF software is restarted.
- RFC3630: This document describes extensions to the OSPF protocol version 2 to support intra-area Traffic Engineering (TE), using Opaque Link State Advertisements.
- RFC3682: The use of a packet's Time to Live (TTL) (IPv4) or Hop Limit (IPv6) to protect a protocol stack from CPU-utilization based attacks has been proposed in many settings.
- RFC3906: This document describes how conventional hop-by-hop link-state routing protocols interact with new Traffic Engineering capabilities to create Interior Gateway Protocol (IGP) shortcuts.
- RFC4576: This document specifies the necessary procedure, using one of the options bits in the LSA (Link State Advertisements) to indicate that an LSA has already been forwarded by a PE and should be ignored by any other PEs that see it.
- RFC4577: This document extends that specification by allowing the routing protocol on the PE/CE interface to

be the Open Shortest Path First (OSPF) protocol.

- RFC4750: This memo defines a portion of the Management Information Base (MIB) for use with network management protocols in TCP/IP-based internets. In particular, it defines objects for managing version 2 of the Open Shortest Path First Routing Protocol. Version 2 of the OSPF protocol is specific to the IPv4 address family.

1.2 Configuration Task Summary

The OSPFv2 configuration includes the following tasks:

(1) Configuring Basic Features

a Configuring OSPF Process

b (Optional) Configuring Router ID

c Adding Interface IP to OSPF and Specifying Area ID

d Enabling OSPF on an Interface and Specifying an Area ID

e (Optional) Creating a Virtual Link

(2) Configuring OSPF Network Type

a Configuring the Interface Network Type

b (Optional) Configuring a Neighbor

c (Optional) Configuring the Interface Priority

d (Optional) Disabling Source Address Verification

(3) Adjusting OSPF Routing

o Configuring the AD

o Configuring the Reference Bandwidth

o Configuring the Cost of an Interface

o Configuring Cost Fallback Value for an AP

o Configuring the Cost of the Default Route in a Stub Area or an NSSA

o Configuring the Default Metric Value for Redistribution Value

o Configuring the Maximum Metric

o Configuring RFC1583 Compatibility

o Configuring Association of External Route Forwarding Addresses with Interface Configuration

(4) Configuring OSPF Route Advertisement

a Configuring External Route Redistribution

b Generating a Default Route

c (Optional) Configuring a Device as ASBR

1.3 Configuring Basic Features

1.3.1 Overview

Set up an OSPF routing domain on the network to provide IPv4 unicast routing service for users on the network.

1.3.2 Restrictions and Guidelines

- Ensure that the IP unitcast routing function is enabled, that is, **ip routing** is not disabled; otherwise, OSPF cannot be enabled.
- You are strongly advised to manually configure the router ID.
- After **ip ospf disable all** is configured, the interface neither sends or receives any OSPF packet, nor participates in OSPF computation even if the interface belongs to the advertisement range of the **network** command.

1.3.3 Configuration Tasks

The basic function configuration of OSPF includes the following tasks:

(1) Configuring OSPF Process

(2) (Optional) Configuring Router ID

(3) Adding Interface IP to OSPF and Specifying Area ID

(4) Enabling OSPF on an Interface and Specifying an Area ID

(5) (Optional) Creating a Virtual Link

1.3.4 Configuring OSPF Process

1. Overview

Configure and enable an RIP process.

2. Restrictions and Guidelines

- OSPF supports multiple instances, and each instance corresponds to an OSPF process. One or more OSPF processes can be started on a router. Each OSPF process runs OSPF independently, and the processes are mutually isolated.
- The process ID takes effect only on the local router, and does not affect exchange of OSPF packets on adjacent interfaces.
- This configuration must be performed on every router that requires OSPF.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create an OSPF process and enter OSPF configuration mode.

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

1.3.5 Configuring Router ID

1. Overview

Router ID is the unique identifier of a router in the OSPF domain, so the router ID must be unique on the entire network; otherwise it will lead to problems such as abnormality in neighbor relationship establishment and routing information error. Moreover, different OSPF processes in the same router need to use different router IDs.

2. Restrictions and Guidelines

- You are strongly advised to manually configure the router ID.
- When no router ID is configured, OSPF selects an interface IP address. If no IP address is configured for any interface, or the configured IP addresses have been used by other OSPF processes, you must manually configure the router ID.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

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

(4) Configure a router ID.

router-id *router-id*

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

1.3.6 Adding Interface IP to OSPF and Specifying Area ID

1. Overview

Add an interface to the OSPF area and associate it with the area. An interface can be associated with only one area and needs to be configured on all the OSPF-enabled routers.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

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

(4) Add an interface IP address to the OSPF area and specify an area ID.

network *ipv4-address wildcard* **area** *area-id*

No interface IP address is configured to join the OSPF area by default.

1.3.7 Enabling OSPF on an Interface and Specifying an Area ID

1. Overview

Running this command will add all IP addresses on the interface to the OSPF process.

2. Restrictions and Guidelines

- The configuration is mandatory for every OSPF-enabled router.
- You can also add an interface to OSPF process using the **network** command on the instance. If two commands are run at the same time, the configuration on the interface takes effect first.

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) Enable OSPF on an interface and specify an area ID.

ip ospf *process-id* **area** *area-id*

OSPF is disabled on an interface by default.

1.3.8 Creating a Virtual Link

1. Overview

In the OSPF routing domain, all the areas must be connected to the backbone area. If the backbone area is disconnected, a virtual link must be configured to connect to the backbone area; otherwise, network communication problems will occur. A virtual link must be created between two ABRs, and the area to which both ABRs belong is the transit area. A stub area or an NSSA cannot be used as a transit area. A virtual link can also be used to connect other non-backbone areas.

2. Restrictions and Guidelines

- Only the authentication key of the virtual link is defined in a virtual link. To enable OSPF packet authentication in the areas connected to the virtual link, run the **area authentication** command to enable the authentication.
- The virtual link supports the fast hello function.
  - If the fast hello function is configured for a virtual link, the hello interval field of the hello packet advertised on the virtual link is set to 0, and the hello interval field of the hello packet received on this virtual link is ignored.
  - No matter whether the fast hello function is enabled, the neighbor dead interval must be always consistent on the devices at both ends of the virtual link.
  - The **dead-interval**, **minimal hello-multiplier**, and **hello-interval** parameters introduced for the fast hello function cannot be configured simultaneously.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

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

(4) Configure a virtual link.

area *area-id* **virtual-link** *router-id* [**authentication** [**keychain** *kechain-name* | **message-digest** | **null**] | **dead-interval** { *dead-interval* | **minimal hello-multiplier** *multiplier-time* } | **hello-interval** *hello-interval* | **retransmit-interval** *retransmit-interval* | **transmit-delay** *transmit-delay*] * [**authentication-key** [**0** | **7**] *key* | **message-digest-key** *key-id* **md5** [**0** | **7**] *key*]

No virtual link is configured by default.

1.4 Configuring OSPF Network Type

1.4.1 Overview

If the physical network is X.25, frame relay, or ATM, set an OSPF network type so that the network can also run OSPF and provide IPv4 unicast routing service.

OSPF 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 OSPF basic functions must be configured.
- The network types must be consistent for the devices at both ends of the link. Otherwise, the neighbor relationship cannot be set up.
- The broadcast network sends multicast OSPF packets, automatically discovers neighbors, and elects a DR and a BDR.
- The P2P network sends multicast OSPF packets and automatically discovers neighbors.
- The NBMA network sends unicast OSPF 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 multicast OSPF packets. Neighbors are automatically discovered.
- The P2MP network (carrying the **non-broadcast** parameter) sends unicast OSPF packets. Neighbors must be manually specified.

1.4.3 Configuration Tasks

The OSPF network type configuration includes the following tasks:

(1) Configuring the Interface Network Type

(2) (Optional) Configuring a Neighbor

(3) (Optional) Configuring the Interface Priority

(4) (Optional) Disabling Source Address Verification

1.4.4 Configuring the Interface Network Type

1. Overview

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.

2. Restrictions and Guidelines

- The configuration is required on routers at both ends of the link.

- The broadcast type requires that the interface must have the broadcast capability.
- The P2P type requires that the interfaces are interconnected in one-to-one manner.
- The NBMA type requires full-meshed connections, and all interconnected routers can directly communicate with each other.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure a network type for the interface.

ip ospf network { **broadcast** | **non-broadcast** | **point-to-multipoint** [**non-broadcast**] | **point-to-point** }

By default, the network interface of OSPF is not configured, and no interface is set to P2MP type.

1.4.5 Configuring a Neighbor

1. Overview

On the NBMA network, routers cannot send or receive broadcast packets, and cannot discover neighbors through hello packets. You need to specify neighbors manually and send unicast hello packets.

If a neighbor router becomes inactive on the NBMA network, OSPF still sends hello packets to this neighbor even if no hello packet is received within the router failure time. The interval at which the hello packet is sent is called polling interval. When running for the first time, OSPF sends hello packets only to neighbors whose priorities are not 0. In this way, neighbors with priorities set to 0 do not participate in the DR/BDR election. After a DR/BDR is elected, the DR/BDR sends the hello packets to all neighbors to set up a neighbor relationship.

2. Restrictions and Guidelines

- If the network type of an interface is set to NBMA or P2MP (carrying the **non-broadcast** parameter), neighbors must be configured.
- Neighbors are configured on routers at both ends of the NBMA or P2MP (carrying the **non-broadcast** parameter) network.
- The neighbor IP address must be the primary IP address of this neighbor interface.
- The P2MP (non-broadcast) network cannot dynamically discover neighbors because it does not have the broadcast capability. Therefore, you must run this command to manually configure neighbors for the P2MP (non-broadcast) network.

- You can use the **cost** parameter to specify the cost to reach each neighbor on the P2MP network.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

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

(4) Configure a neighbor.

neighbor *ipv4-address* [**cost** *cost* | [**poll-interval** *poll-interval* | **priority** *priority*] *]

No neighbor is configured by default. Neighbors must be specified for the NBMA or P2MP (non-broadcast) interfaces. The neighbor IP address must be the primary IP address of this neighbor interface. In addition, you can use the **cost** parameter to specify the cost to reach each neighbor on the P2MP network.

1.4.6 Configuring the Interface Priority

1. Overview

When the DR/BDR election occurs on the OSPF broadcast network, the router with the highest priority becomes the DR or BDR. If the priorities are the same, the router with the largest router ID becomes the DR or BDR. A router with the priority set to 0 does not participate in the DR/BDR election. The priority value of an OSPF interface is contained in the hello packet.

2. Restrictions and Guidelines

- This command is applicable only to the OSPF broadcast and NBMA interfaces.
- You must configure the interface priority if a router must be specified as a DR, or a router cannot be specified as a DR.
- Configure the interface priority on a router that must be specified as a DR, or cannot be specified as a DR.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the interface priority.

ip ospf priority *priority*

The priority value is 1 by default.

1.4.7 Disabling Source Address Verification

1. Overview

Generally, the source address of a packet received by OSPF is in the same network segment as the receiving interface. The addresses at both ends of a P2P link are configured separately and are not necessarily in the same network segment. In this scenario, as the peer address information is notified during the P2P link negotiation, OSPF checks whether the source address of the packet is the address advertised by the peer end during negotiation. If not, OSPF determines that the packet is invalid and discards it. Besides, OSPF does not verify the address of an unnumbered interface.

In some scenarios, the source address of a packet received by OSPF may not be in the same network segment as the receiving interface, so the OSPF address verification fails. For example, the negotiated peer address cannot be obtained on a P2P link. In this scenario, source address verification must be disabled to ensure that the OSPF adjacency can be properly set up.

2. Restrictions and Guidelines

- The OSPF basic functions must be configured.
- Source address verification cannot be disabled on a broadcast or NBMA network.

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 source address verification.

ip ospf source-check-ignore

The source address verification on a P2P link is enabled by default.

1.5 Adjusting OSPF Routing

1.5.1 Overview

Change the OSPF routes so that the traffic passes through specified nodes or bypasses specified nodes. Change the sequence that a router selects routes so as to change the priorities of OSPF routes.

1.5.2 Restrictions and Guidelines

- The OSPF basic functions must be configured.
- If you run the **ip ospf cost** command to configure the cost of an interface, the configured cost will automatically overwrite the cost that is computed based on the auto cost.

1.5.3 Configuration Tasks

The configuration for adjusting OSPF routing includes the following tasks, which are optional. Select tasks for configuration according to actual condition.

- Configuring the AD
- Configuring the Reference Bandwidth
- Configuring the Cost of an Interface
- Configuring Cost Fallback Value for an AP
- Configuring the Cost of the Default Route in a Stub Area or an NSSA
- Configuring the Default Metric Value for Redistribution value
- Configuring the Maximum Metric
- Configuring RFC1583 Compatibility
- Configuring Association of External Route Forwarding Addresses with Interface Configuration

1.5.4 Configuring the AD

1. Overview

AD is used to select the best path when multiple routing protocols are used to reach the same target. AD defines the reliability of routing protocol. A smaller AD indicates higher reliability and higher routing priority. The default AD values of OSPF intra-domain routes, inter-domain routes, and external routes are all 110. Different ADs can be set to control routing.

2. Restrictions and Guidelines

- Perform this configuration if you hope to change the priorities of OSPF routes on a router that runs multiple unicast routing protocols.
- Run this command to specify different ADs for different types of OSPF routes.
- Configure the **route-map** parameter and set an AD for the specific route through a policy. If the route map is configured with **set distance**, then:
  - Through the matched route: the AD is set by the **set distance** command.
  - Not through the matched route: the AD is set by the **distance** command.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

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

(4) Configure an AD.

distance { *distance* [**route-map** *map-name*] | **ospf** { [**intra-area** *distance* [**route-map** *map-name*]] [**inter-area** *distance* [**route-map** *map-name*]] [**external** *distance* [**route-map** *map-name*]] } }

By default, the management distance is **110** for all the OSPF routes.

1.5.5 Configuring the Reference Bandwidth

1. Overview

The default value of OSPF 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 calculated 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.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

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

(4) Configure the reference bandwidth.

auto-cost reference-bandwidth *ref-bw*

By default, the reference bandwidth value of interface metric calculation is 100 Mbps.

1.5.6 Configuring the Cost of an Interface

1. Overview

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

2. Restrictions and Guidelines

- By default, the cost of an OSPF interface is equal to the reference value of the auto cost divided by the interface bandwidth.
- A router is connected with multiple lines. This configuration is recommended if you wish to manually specify a preferential line.
- Run the **auto-cost** command to obtain the reference value of the auto cost. The default value is 100 Mbps.
- Run the **bandwidth** command to set the interface bandwidth.
- The default costs of OSPF interfaces on several typical lines are as follows:
  - 64 Kbps serial line: The cost is 1562.
  - E1 line: The cost is 48.
  - 10M Ethernet: The cost is 10.
  - 100M Ethernet: The cost is 1.
- If you run the **ip ospf cost** command to configure the cost of an interface, the configured cost will automatically overwrite the cost that is computed based on the auto cost.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the cost of an interface.

ip ospf cost *cost*

By default, the cost of an OSPF interface is equal to the reference value of the auto cost divided by the interface bandwidth (the reference bandwidth is 100 Mbps by default).

1.5.7 Configuring Cost Fallback Value for an AP

1. **Overview**

The bandwidth of an AP is equal to the sum of the bandwidths of all the valid member ports. When a member port fails, the bandwidth of the AP will be reduced. You can set a cost fallback value for the AP to enable OSPF to select other paths preferably. When the failed member port of the AP recovers, the cost fallback value becomes invalid, and the metric of the AP returns to normal.

2. **Procedure**

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the cost fallback value for an AP.

ip ospf cost-fallback *cost* **threshold** *bandwidth*

The cost fallback function is disabled on an AP by default.

1.5.8 Configuring the Cost of the Default Route in a Stub Area or an NSSA

1. **Overview**

After an area is set to a stub area/NSSA, 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 of a default route is 1. This function can adjust the cost of the default route and flexibly control the routes of the stub area and NSSA.

2. **Restrictions and Guidelines**

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

3. **Procedure**

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

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

(4) Configure the cost of the default route in a stub area or an NSSA.

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

By default, the cost of a route is 1.

1.5.9 Configuring the Default Metric Value for Redistribution

1. Overview

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

2. Restrictions and Guidelines

- This configuration is mandatory if the cost of external routes of the OSPF domain should be specified when external routes are introduced to an ASBR.
- The **default-metric** command must be used together with the **redistribute** command in routing process configuration mode to modify the initial metrics of all redistributed routes.
- The **default-metric** command does not take effect on external routes that are injected to the OSPF routing domain using the **default-information originate** command.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

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

(4) Configure the default metric for redistribution.

default-metric *metric*

By default, the metric of a redistributed route is 20.

1.5.10 Configuring the Maximum Metric

1. Overview

In the scenarios of restarting a device and using a device as a candidate path, the OSPF information advertised by the current device can be configured with the maximum metric value so that the data traffic will not pass through the current device.

2. Restrictions and Guidelines

- A router may be unstable in the restart process or a period of time after the router is restarted, and users do not want to forward data traffic through this router. In this case, this configuration is recommended.

- After the **max-metric router-lsa** command is configured, the metrics of the non-stub links in the router LSAs generated by the router will be set to the maximum value (0xFFFF). If you cancel this configuration or the timer expires, the normal metrics of the links are restored.
- By default, if the **max-metric router-lsa** command is configured, the stub links still advertise common metrics, that is, the costs of outbound interfaces. If the **include-stub** parameter is configured, the stub links will advertise the maximum metric.
- If an ABR is not intended to transfer inter-area traffic, use the **summary-lsa** parameter to set the metric of the summary LSA to the maximum value.
- If an ASBR does not wish to transfer external traffic, use the **external-lsa** parameter to set the metric of the external LSA to the maximum value.
- The **max-metric router-lsa** command is generally used in the following scenarios:
  - Restart a device. After the device is restarted, IGP generally converges faster, and other devices attempt to forward traffic through the restarted device. If the current device is still building the BGP routing table and some BGP routes are not learned yet, packets sent to these networks are discarded. In this case, you can use the **on-startup** parameter to set a delay after which the restarted device acts as the transmission mode.
  - Add a device to the network but the device is not used to transfer traffic. The device is added to the network. If a candidate path exists, the current device is not used to transfer traffic. If a candidate path does not exist, the current device is still used to transfer traffic.
  - Delete a device gracefully from the network. After the **max-metric router-lsa** command is configured, the current device advertises the maximum metric among all the routes. In this way, other devices on the network can select the backup path for data transmission before the device is shut down.
  - In the earlier OSPF version (RFC1247 or earlier), the links with the maximum metric (0xFFFF) in the LSAs do not participate in the SPF computation, that is, no traffic is sent to routers that generate these LSAs.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

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

(4) Configure the maximum metric.

max-metric router-lsa [**external-lsa** [*max-metric-value*] | **include-stub** | **on-neighborup** [*full-interval-time*] | **on-startup** [*startup-interval-time*] | **summary-lsa** [*max-metric-value*]] *

By default, the LSAs of normal metric are advertised.

1.5.11 Configuring RFC1583 Compatibility

1. Overview

When there are multiple paths to an ASBR or the forwarding address of an external route, RFC1583 and RFC2328 define different routing rules. If RFC1583 compatibility is configured, a path in the backbone area or an inter-area path is preferentially selected. If RFC1583 compatibility is not configured, a path in a non-backbone area is preferentially selected.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

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

(4) Configure compatible RFC1583.

compatible rfc1583

The RFC1583 rule function is enabled by default.

1.5.12 Configuring Association of External Route Forwarding Addresses with Interface Configuration

1. Overview

Setting the forwarding address (FA) of relevant flag bit can associate the interface configuration with the external route forwarding address to calculate the reachability and metric.

2. Restrictions and Guidelines

- In the case of interconnection with a Cisco device, the FA configuration compatible with the Cisco device must be enabled.
- When the FA of an external route is 0, external route computation of OSPF will compute the reachability and metric to the advertiser. When the FA is not 0, the reachability and metric to the forwarding address will be computed.
- When the following conditions are met simultaneously in default configuration, the ASBR of OSPF fills the forwarding address field of the external route with digits other than 0:
  - OSPF is enabled on the next hop interface for connecting the ASBR to external network.

  - The next hop interface for connecting the ASBR to the external network is in the network scope advertised in the OSPF protocol.

- When the following conditions are met simultaneously after association of forwarding address rules with interface configuration is configured, the ASBR of OSPF fills the forwarding address field of the external route with digits other than 0:
  - OSPF is enabled on the next hop interface for connecting the ASBR to external network.
  - The next hop interface for connecting the ASBR to the external network is in the network scope advertised in the OSPF protocol.
  - The next hop interface for connecting the ASBR to the external network is not configured as a passive interface.
  - The next hop interface for connecting the ASBR to the external network is not P2P or P2MP type of OSPF.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

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

1.6 Configuring OSPF Route Advertisement

1.6.1 Overview

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

OSPF 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, the **show ip route** command displays only the Type-1 route.

1.6.2 Restrictions and Guidelines

The OSPF basic functions must be configured.

1.6.3 Configuration Tasks

The configuration of OSPF route advertisement includes the following tasks:

(1) Configuring External Route Redistribution

(2) Generating a Default Route

(3) (Optional) Configuring a Device as ASBR

1.6.4 Configuring External Route Redistribution

1. Overview

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

2. Restrictions and Guidelines

- Perform this configuration on an ASBR.
- After this command is configured, the router becomes an ASBR, imports related routing information to the OSPF domain, and advertises the routing information as Type-5 LSAs to other OSPF routers in the domain.
- If the **level** parameter is not carried when IS-IS route redistribution is configured, only Level-2 routes can be redistributed by default. The **level** parameter is carried during initial configuration of redistribution, the routes configured with the **level** parameter can be redistributed. If both **level 1** and **level 2** are configured, the two levels are combined and saved as **level-1-2**.
- If you configure redistribution of OSPF routes without specifying the **match** parameter, OSPF routes of all sub-types can be distributed by default. The latest setting of the **match** parameter is used as the initial **match** parameter. Only routes that match the sub-types can be redistributed. You can run the **no** form of the command to restore the default value of **match**.
- If **route-map** is specified, the **match** filtering rules specified in **route-map** are applicable to the original parameters of redistribution. For redistribution of OSPF or IS-IS routes, **route-map** is used for filtering only when the redistributed routes meet the criteria specified by **match** or **level**.
- The **set metric** value range of the associated **route-map** is from 0 to 16777214. If the value exceeds this range, routes cannot be introduced.
- The configuration rules for the **no** form of the **redistribute** command are as follows:
    - If some parameters are specified in the **no** form of this command, default values of these parameters will be restored.
    - If no parameter is specified in the **no** form of this command, the entire command will be deleted.
- For example, if **redistribute isis 112 level-2** is configured, you can run the **no redistribute isis 112 level-2** command to restore the default value of level-2. As **level-2** itself is the default value of the parameter, the configuration saved is still **redistribute isis 112 level-2** after the preceding **no** form of the command is executed. To delete the entire command, run the **no redistribute isis 112** command.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

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

(4) Configure external route redistribution.

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

The route redistribution function is not configured by default.

1.6.5 Generating a Default Route

1. Overview

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

2. Restrictions and Guidelines

- When the **redistribute** or **default-information** command is executed, the OSPF router automatically becomes an ASBR. The ASBR, however, does not automatically generate or advertise a default route to all routers in the OSPF routing domain. To enable an ASBR to generate a default route, configure the **default-information originate** command.
- The metric of the external default route can only be defined in the **default-information originate** command, instead of the **default-metric** command.
- A router in a stub area cannot generate an external default route.
- The **set metric** value range of the associated **route-map** is from 0 to 16777214. If the value exceeds this range, routes cannot be introduced.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

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

(4) Generate a default route.

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

No default route is generated by default.

If the **always** parameter is specified, the OSPF routing process advertises an external default route to neighbors regardless of whether a default route exists. This default route, however, is not displayed on the local router. To confirm whether the default route is generated, run the **show ip ospf database** command to display the OSPF LSDB. The external link with the ID 0.0.0.0 describes the default route. On an OSPF neighbor, you can run the **show ip route** command to see the default route.

1.6.6 Configuring a Device as ASBR

1. Overview

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

2. Restrictions and Guidelines

After the **redistribute** or **default-information** command is executed, the OSPF router automatically becomes an ASBR. If you want the device to become an ASBR without configuring the above command, configure the **asbr enable** command. If the **asbr enable** command is deleted, but the **redistribute** or **default-information** command is still configured, the device is still an ASBR.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

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

(4) Configure a device as ASBR.

asbr enable

ASBR is disabled by default.

1.7 Configuring OSPF 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. Shield or filter routes.

1.7.2 Restrictions and Guidelines

- The OSPF basic functions must be configured.
- The address range of the route 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.

1.7.3 Configuration Tasks

The configuration of OSPF route summarization includes the following tasks, which are optional. Select tasks for configuration according to actual condition.

- Configuring Inter-Area Route Summarization
- Configuring External Route Summarization
- Configuring a Discard Route

1.7.4 Configuring Inter-Area Route Summarization

1. Overview

On a large-scale OSPF network, configuring route summarization can reduce the size of a routing table and the LSA information, thus reducing the system loss.

2. Restrictions and Guidelines

- Perform this configuration when routes of the OSPF area need to be summarized.
- Unless otherwise required, perform this configuration on an ABR in the area where routes to be summarized are located.
- This command can be executed only on the ABR. It is used to combine or summarize multiple routes of an area into one route, and then advertise the route to other areas. Combination of the routing information occurs only on the boundary of an area. Routers inside the area can learn specific routing information, whereas routers in other areas can learn only one summarized route. You can set **advertise** or **not-advertise** to determine whether to advertise this summarized route to shield and filter routes. By default, the summarized route is advertised. You can use the **cost** parameter to set the metric of the summarized route.
- You can configure the route summarization command for multiple areas. This simplifies routes in the entire OSPF routing domain, and improves the network forwarding performance, especially for a large-sized network.
- When multiple routes for summarization are configured and have an inclusive relationship with each other, the range of routes to be summarized is determined based on the longest match principle.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

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

(4) Configure inter-area route summarization.

area *area-id* **range** *ipv4-address mask* [**advertise** | **not-advertise**] [**cost** *cost* | **inherit-minimum**]

The inter-area route summarization function is disabled by default.

1.7.5 Configuring External Route Summarization

1. Overview

When a lot of OSPF domain routes need to be introduced, configuring route summarization can reduce the size of a routing table and the LSA information, thus reducing the system loss.

2. Restrictions and Guidelines

- Perform this configuration when routes outside the OSPF domain need to be summarized.
- Unless otherwise required, perform this configuration on an ASBR, to which routes that need to be summarized are introduced.
- When routes are redistributed from other routing processes and injected to the OSPF routing process, every route is advertised to the OSPF routers using an external LSA respectively. If the injected routes are in a continuous address space, the ASBR can advertise only one summarized route to significantly reduce the size of the routing table.
- The **area range** command summarizes the routes between OSPF areas, whereas **summary-address** summarizes external routes of the OSPF routing domain.
- When configured on the NSSA ABR translator, **summary-address** summarizes redistributed routes and routes obtained based on the LSAs that are converted from Type 7 to Type 5. When configured on the ASBR (not an NSSA ABR translator), **summary-address** summarizes only redistributed routes.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

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

(4) Configure external route summarization.

summary-address *ipv4-address mask* [[**cost** *cost* | **distribute-delay** *interval* | **nssa-only** | **tag** *tag-value*] * | **not-advertise**]

The route summarization function is disabled by default.

1.7.6 Configuring a Discard Route

1. Overview

The address range of summarized routes 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 on the ABR or ASBR. This route is automatically generated, and is not advertised.

The discard route means adding a route whose egress is Null 0 to the routing table, and it will not generate the corresponding LSA, so it will not be received by neighbors. The packets matching the route are discarded.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

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

(4) Configure a discard route.

discard-route { **internal** | **external** }

The discard route adding function is enabled by default.

1.8 Configuring OSPF Route Filtering

1.8.1 Overview

Routes that do not meet filtering conditions cannot be loaded to the routing table, or advertised to neighbors. Network users cannot access specified destination network.

1.8.2 Restrictions and Guidelines

The OSPF basic functions must be configured.

1.8.3 Configuration Tasks

The configuration of OSPF route filtering includes the following tasks, which are optional. Select tasks for configuration according to actual condition.

- Configuring a Passive Interface
- Configuring LSA Update Packet Filtering
- Configuring Inter-area Route Filtering
- Configuring Redistributed Route Filtering
- Configuring Learned Route Filtering

1.8.4 Configuring a Passive Interface

1. Overview

To prevent other routers on the network from learning the routing information of the local router, you can configure a specified network interface of the local router as the passive interface, or a specified IP address of a network interface as the passive address.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

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

(4) Configure a passive interface.

passive-interface { **default** | *interface-type interface-number* | *interface-type interface-number ipv4-address* }

By default, the passive modes of all interfaces are disabled, and all interfaces are allowed to send and receive OSPF packets.

1.8.5 Configuring LSA Update Packet Filtering

1. Overview

Enable this function on an interface to prevent sending the LSA update packet from this interface. After this function is enabled, the local router does not advertise the LSA update packet to neighbors, but still sets up an adjacency with neighbors and receives LSAs from neighbors.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure LSA update packet filtering.

ip ospf database-filter all out

By default, the function of not diffusing LSA packets to the outside is disabled on an interface, that is, any LSA update packet can be sent from the interface.

1.8.6 Configuring Inter-area Route Filtering

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.

Routers are filtered using the following three methods.

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

2. Restrictions and Guidelines

- This command can be configured only on an ABR.
- Run this command when it is required to configure filtering conditions for inter-area routes on the ABR.
- This configuration is recommended if users need to be prevented from accessing the network in a certain OSPF area.
- Unless otherwise required, perform this configuration on an ABR in the area where filtered routes are located.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an ACL or prefix list. Please configure only one task.

- Configure an ACL.

  access-list *acl-number* { **deny** | **permit** } { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } [**time-range** *tm-range-name*] [**log**]

- Configure a prefix list.

  ip prefix-list *prefix-list-name* [**seq** *seq-number*] { **deny** | **permit** } *ipv4-prefix* [**ge** *minimum-prefix-length*] [**le** *maximum-prefix-length*]

(4) Enter the OSPF configuration mode.

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

(5) Configure inter-area route filtering.

area *area-id* **filter-list** { **access** *acl-number* | **prefix** *prefix-list-name* } { **in** | **out** }

By default, the filtering list function is not configured on an ABR.

1.8.7 Configuring Redistributed Route Filtering

1. Overview

Similar to the **redistribute route-map** command, the **distribute-list out** command is used to filter routes that are redistributed from other protocols to OSPF. The command itself does not redistribute routes, and is generally used together with the **redistribute** command.

2. Restrictions and Guidelines

- Perform this configuration if external routes introduced by the ASBR need to be filtered.
- Unless otherwise required, perform this configuration on an ASBR to which filtered routes are introduced.
- The ACL and prefix list filtering rules are mutually exclusive in the configuration. In other words, if the ACL is used for filtering routes coming from a certain a source, the prefix list cannot be configured to filter the same routes.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an ACL or prefix list. Please configure only one task.

- Configure an ACL.

  access-list *acl-number* { **deny** | **permit** } { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } [**time-range** *tm-range-name*] [**log**]

- Configure a prefix list.

ip prefix-list *prefix-list-name* [**seq** *seq-number*] { **deny** | **permit** } *ipv4-prefix* [**ge** *minimum-prefix-length*] [**le** *maximum-prefix-length*]

(4) Enter the OSPF configuration mode.

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

(5) Configure redistributed route filtering.

distribute-list { *acl-number* | *acl-name* | **prefix** *prefix-list-nam*e } **out** [**arp-host** | **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 get past.

1.8.8 Configuring Learned Route Filtering

1. Overview

This function filters the routes that are computed based on received LSAs. Only the routes meeting the filtering conditions can be forwarded.

2. Restrictions and Guidelines

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.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an ACL or prefix list. Please configure only one task.

- Configure an ACL.

  istribute-list { *acl-name* | *acl-number* | **gateway** *prefix-list-name* | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*] | **route-map** *route-map-name* } **in** [*interface-type interface-number*]

- Configure a prefix list.

  ip prefix-list *prefix-list-name* [**seq** *seq-number*] { **deny** | **permit** } *ipv4-prefix* [**ge** *minimum-prefix-length*] [**le** *maximum-prefix-length*]

(4) Enter the OSPF configuration mode.

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

(5) Configure learned route filtering.

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

By default, the filtering function of the routes calculated based on the received LSA is disabled, that is, all these routes get past.

1.9 Adjusting OSPF Network Convergence Speed

1.9.1 Overview

This function aims to modify protocol control parameters to change the protocol running status, thus adjusting the convergence speed of OSPF network.

1.9.2 Restrictions and Guidelines

- The OSPF basic functions must be configured.
- The neighbor relationship maintenance time cannot be shorter than the hello interval.

1.9.3 Configuration Tasks

The configuration for adjusting the convergence speed of OSPF network includes the following tasks, which are optional. Select tasks for configuration according to actual condition.

- Configuring the Hello Interval
- Configuring the Dead Interval
- Configuring LSU Transmission Delay
- Configuring LSU Retransmission Interval
- Configuring LSU Generation Time
- Configuring LSA Group Refresh Time
- Configuring LSA Group Refresh Interval
- Configuring Duplicate LSA Receiving Delay
- Configuring Inter-Area Route Computation Delay
- Configuring External Route Computation Delay
- Configuring SPF Computation Delay
- Enabling Two-Way Maintenance

1.9.4 Configuring the Hello Interval

1. Overview

The hello packet interval is contained in the hello packet. A shorter hello interval indicates that OSPF can detect topology changes more quickly, but the network traffic increases.

2. Restrictions and Guidelines

- This configuration is performed on routers at both ends of a link.
- The hello packet interval must be the same on all routers in the same network segment. If you want to manually modify the neighbor dead interval, ensure that the neighbor dead interval is longer than the hello packet interval.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the hello interval.

ip ospf hello-interval *hello-interval*

By default, the hello packet interval is 10s for Ethernet, PPP, HDLC encapsulation interfaces, and frame relay point-to-point sub-interfaces; the hello packet interval is 30s for non-frame relay point-to-point sub-interfaces and X.25 interfaces.

1.9.5 Configuring the Dead Interval

1. Overview

This configuration can be adjusted if you wish to accelerate OSPF convergence when a link fails. The failure determining interval of an OSPF neighbor is contained in the hello packet. If OSPF does not receive a hello packet from a neighbor within the neighbor dead interval, it declares that the neighbor is invalid and deletes this neighbor record from the neighbor list.

2. Restrictions and Guidelines

- This configuration is performed on routers at both ends of a link.
- By default, the dead interval is four times the hello packet interval. If the hello packet interval is modified, the dead interval is modified automatically.

- Be sure to run this command to manually modify the interval for OSPF to judge failure of a neighbor with caution. Pay attention to the following two issues:
  - The neighbor dead interval cannot be smaller than the hello packet sending interval;
  - The neighbor dead interval must be the same on all routers in the same network segment.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the **dead** interval.

ip ospf dead-interval { *dead-interval* | **minimal hello-multiplier** *multiplier* }

By default, the fast hello function is disabled, and the neighbor dead interval is four times the sending interval of hello packet.

1.9.6 Configuring LSU Transmission Delay

1. Overview

On a low speed network, a device can be configured with the delay before sending LSU packets.

2. Restrictions and Guidelines

- Before an LSU packet is transmitted, the **Age** fields in all LSAs in this packet will increase based on the amount specified by the LSU transmission delay. Considering the transmission delay and line propagation delay on the interface, you need to set the LSU transmission delay to a greater value for a low-speed line or interface. The LSU packet transmission delay of a virtual link is defined by the **transmit-delay** parameter in the **area virtual-link** command.
- If the value of the **Age** field of an LSA reaches 3600, the packet will be retransmitted or a retransmission request will be sent. If the LSA is not updated in time, the expired LSA will be deleted from the LSDB.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the LSU transmission delay.

ip ospf transmit-delay *transmit-delay*

The LSU packet transmission delay is 1s by default.

1.9.7 Configuring LSU Retransmission Interval

1. Overview

When a network is congested, frequent LSU retransmission will aggravate the congestion. The retransmission delay can be set to a greater value on a serial line or virtual link to prevent unwanted retransmission. The LSU retransmission interval of a virtual link is defined by the **retransmit-interval** parameter in the **area virtual-link** command.

After a router finishes sending an LSU packet, this packet is still kept in the transmit buffer queue. If an acknowledgment from the neighbor is not received within the LSU retransmission interval, the router retransmits the LSU packet.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the LSU retransmission interval.

ip ospf retransmit-interval *retransmit-interval*

By default, the LSU retransmission interval is 5s.

1.9.8 Configuring LSU Generation Time

1. Overview

The LSU generation time can be adjusted according to different requirements for network performance and convergence speed.

2. Restrictions and Guidelines

- If a high convergence requirement is raised when a link changes, 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.

- When configuring this command, 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*.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

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

(4) Configure the exponential backoff algorithm for generating LSAs.

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

By default, the 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.

1.9.9 Configuring LSA Group Refresh Time

1. Overview

Every LSA has its time to live (LSA age). When the LSA age reaches 3600s, a refreshment is needed to prevent normal 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. Allocate the LSAs received within a certain time (pacing interval) to the same group. The device will maintain a refresh timer for this group. After the timer expires, the LSAs in the group will be refreshed uniformly.

2. Restrictions and Guidelines

If the total number of LSAs does not change, a larger group pacing interval indicates that more LSAs need to be processed after timeout, which will lead to a high load of the CPU in a certain period of time. For CPU stability, the number of LSAs 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.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

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

(4) Configure the LSA group refresh time.

timers pacing lsa-group *pacing-interval*

The group pacing interval of LSA is 30s by default.

1.9.10 Configuring LSA Group Refresh Interval

1. Overview

If a router has a large number of routing entries, synchronizing LSDB will send a large number of LSU packets, easily causing network congestion. The LSU packets can be grouped and sent at an interval to ensure stability of the network.

2. Restrictions and Guidelines

- If the number of LSAs is large and the device load is heavy in an environment, properly configuring *transimit-time* and *transimit-count* can limit the number of LS-UPD packets flooded on the network.
- If the CPU usage is not high and the network bandwidth load is not heavy, reducing the value of *transimit-time* and increasing the value of *transimit-count* can accelerate the environment convergence.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

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

(4) Configure the LSA group refresh interval.

timers pacing lsa-transmit *transmit-interval transmit-count*

By default, the interval for sending LSU group is 40 ms, and the number of LS-UPD packets in each group is 1.

1.9.11 Configuring Duplicate LSA Receiving Delay

1. Overview

According to the network connection and equipment resources of the current network, you can configure that no processing is performed if the same LSA is received within the specified time. This prevents excessive usage of network bandwidth and equipment resources caused by network connection or frequent route flapping.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

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

(4) Configure duplicate LSA receiving delay.

timers lsa arrival *arrival-time*

By default, the delay for receiving a duplicate LSA is 1000 ms.

1.9.12 Configuring Inter-Area Route Computation Delay

1. Overview

In case of route flapping, frequent inter-area route computation will consume a lot of device performance, and delaying the process of inter-area route computation can reduce the device load.

2. Restrictions and Guidelines

- This delay cannot be modified if strict requirements are raised for the network convergence time.
- If a lot of inter-area or external routes exist on the network and the network is not stable, you can adjust the corresponding delays.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

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

(4) Configure inter-area route computation delay.

timers throttle route inter-area *ia-delay*

By default, the waiting time for inter-area route computation is 0 ms.

1.9.13 Configuring External Route Computation Delay

1. Overview

In case of route flapping, frequent external route computation will consume a lot of device performance, and delaying the process of external route computation can reduce the device load.

2. Restrictions and Guidelines

- This delay cannot be modified if strict requirements are raised for the network convergence time.
- If a lot of inter-area or external routes exist on the network and the network is not stable, you can adjust the corresponding delays.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

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

(4) Configure the external route computation delay.

timers throttle route ase *ase-delay*

By default, the waiting time for external route computation is 0 ms.

1.9.14 Configuring SPF Computation Delay

1. Overview

Changes to LSDB will trigger SPF computation. Frequent network jitter will consume a lot of CPU resources. Setting a reasonable delay for SPF computation can avoid occupying excessive router memory and bandwidth resources.

2. Restrictions and Guidelines

- Compared with the **timers spf** command, this command supports more flexible settings to accelerate the convergence speed of SPF computation and further reduce the system resources consumed by SPF computation when the topology continuously changes. Therefore, you are advised to run the **timers throttle spf** command to adjust the SPF computation time.
- The value of *spf-holdtime* cannot be smaller than that of *spf-delay*; otherwise, *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.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

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

(4) Configure the SPF computation delay.

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

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

1.9.15 Enabling Two-Way Maintenance

1. Overview

On a large network, a lot of packets may be sent or received, occupying too much CPU and memory. As a result, some packets are delayed or discarded. If the time required for processing hello packets exceeds the neighbor dead interval, the corresponding adjacency times out and is removed. 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 when a large number of packets exist on the network. This prevents termination of the adjacency caused by delayed or discarded hello packets. The function is enabled by default. You are advised to retain the default configuration.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

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

(4) Enable two-way maintenance.

two-way-maintain

By default, the two-way maintenance function is enabled for an OSPF process.

1.10 Configuring Stub Area and NSSA

1.10.1 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.

1.10.2 Restrictions and Guidelines

- The OSPF basic functions must be configured.
- A backbone or transit area cannot be configured as a stub or an NSSA area.
- A router in the stub area cannot introduce external routes, but a router in the NSSA area can introduce external routes.

1.10.3 Configuration Tasks

The configuration of stub area and NSSA includes the following tasks, which are optional. Select tasks for configuration according to actual condition.

- Configuring a Stub Area
- Configuring an NSSA

1.10.4 Configuring a Stub Area

1. Overview

The stub area is an OSPF stubby area. Configuring a stub area can reduce the number of LSAs in the stub area. The ABR in the stub area will not transfer the Type-5 LSA (external route), and the default route will be advertised to the 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 the default route will be advertised to the stub area.

2. Restrictions and Guidelines

- To configure a totally stub area, add the **no-summary** keyword when running the **area stub** command on the ABR. A router in the totally stub area can learn only the internal routes of the local area, including the internal default route generated by an ABR.
- Perform this configuration if you want to reduce the size of the routing table on routers in the area.
- The area must be configured as a stub area on all routers in this area.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

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

(4) Configure a stub area.

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

The stub area function is disabled by default.

1.10.5 Configuring an NSSA

1. Overview

An NSSA is similar to a stub area, but allows ASBR. The route redistributed by ASBR will be transferred in the NSSA in the form of Type-7 LSA, and the Type-7 LSA will be converted into Type-5 LSA on ABR and then transferred to other areas. This ABR is also called a translator. The ABR also advertises the default route to the NSSA.

2. Restrictions and Guidelines

- The **default-information-originate** parameter is used to generate a default Type-7 LSA. This parameter has different functions on the ABR and the ASBR in an NSSA. On the ABR, a Type-7 LSA default route is generated regardless of whether the default route exists in the routing table. On the ASBR (not an ABR), a Type-7 LSA default route is generated only when the default route exists in the routing table.
- Configuring a totally NSSA can further reduce the number of LSAs sent to the 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.
- In the same NSSA, it is recommended that only one ABR serve as a translator.
- Perform this configuration if you want to reduce the size of the routing table on routers in the area and the number of LSAs in the area, and also introduce external routes of the OSPF domain to this area.
- The area must be configured as an NSSA on all routers in this area.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

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

(4) Configuring an NSSA Area

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

The NSSA function is disabled by default.

1.11 Configuring OSPF Authentication

1.11.1 Overview

Authentication prevents routers that illegally access the network and hosts that forge OSPF packet from participating in the OSPF process. All routers connected to the OSPF network must be authenticated to ensure stability of OSPF and protect OSPF against intrusions.

1.11.2 Restrictions and Guidelines

- The OSPF basic functions must be configured.
- If authentication is configured for an area, the configuration takes effect on all interfaces that belong to this area.
- If authentication is configured for both an interface and the area to which the interface belongs, the configuration for the interface takes effect preferentially.

1.11.3 Configuration Tasks

The OSPF authentication configuration includes the following tasks:

- Configuring the Authentication Type of an Area
- Configuring the Authentication Type of an Interface
- (Optional) Configuring a Plain Text Authentication Key for an Interface
- (Optional) Configuring an MD5 Authentication Key for an Interface

1.11.4 Configuring the Authentication Type of an Area

1. Overview

OSPF area authentication can improve the security of an OSPF area. The consistency in the authentication type and password is a requisite for establishing a neighbor relationship.

2. Restrictions and Guidelines

- This configuration is recommended if the same authentication type should be enabled on all the interfaces in the same area.
- Perform this configuration if a router accesses a network that requires authentication.
- The device supports three authentication types:

- Type 0: No authentication is required. When the OSPF authentication command is not run to enable OSPF authentication, the authentication type carried in OSPF data packets is type 0.
- Type 1: The authentication type is plain text authentication if this command is configured but does not contain the **message-digest** parameter.
- Type 2: The authentication type is MD5 authentication if this command is configured and contains the **message-digest** parameter.

- All routers in the same OSPF area must use the same authentication type. If authentication is enabled, the authentication key must be configured on interfaces that are connected to neighbors.
- If keychain authentication is configured, the key and authentication type configured for keychain are used. Currently, keychain supports plain text authentication, Message-Digest 5 (MD5) authentication, and SM3 authentication.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

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

(4) Configure the authentication type of an area.

area *area-id* **authentication** [**message-digest** | **keychain** *name*]

The OSPF area authentication function is disabled by default.

1.11.5 Configuring the Authentication Type of an Interface

1. Overview

OSPF interface authentication can improve the communication security of neighbors. The consistency in the authentication type and password is a requisite for establishing a neighbor relationship.

2. Restrictions and Guidelines

- This configuration is mandatory if different authentication types should be used on different interfaces in the same area.
- Perform this configuration if a router accesses a network that requires authentication.
- If the **ip ospf authentication** command does not contain any option, plain text authentication is enabled. If you run the **no** form of the command to restore the default authentication mode, whether authentication is enabled is determined by the authentication type that is configured in the area to which the interface belongs. If the authentication type is set to **null**, authentication is disabled forcibly. When authentication is configured for both

an interface and the area to which the interface belongs, the authentication type configured for the interface is used preferentially.

- If keychain authentication is configured, the key and authentication type configured for keychain are used. Currently, keychain supports plain text authentication, MD5 authentication, and SM3 authentication.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the authentication type of an interface.

ip ospf authentication [**message-digest** | **null** | **keychain** *kc-name*]

By default, no authentication mode is set on an interface. In this case, the authentication type of the related area is used on the interface.

1.11.6 Configuring a Plain Text Authentication Key for an Interface

1. Overview

This configuration is required when a router accesses a network that requires plain text authentication. The key information will be inserted to the headers of all OSPF packets. If the keys are inconsistent, two directly connected devices cannot set up an OSPF neighbor relationship and cannot exchange routing information.

2. Restrictions and Guidelines

- Different keys can be configured for different interfaces, but all the routers connected to the same physical network segment must be configured with the same key.
- You must set the authentication type to plain text authentication on the related interface or in the area in advance.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure plain text authentication for an interface.

ip ospf authentication

(5) Configure a plain text authentication key for an interface.

ip ospf authentication-key [**0** | **7**] *key*

The authentication key is disabled by default.

1.11.7 Configuring an MD5 Authentication Key for an Interface

1. Overview

The MD5 cipher text authentication mode can be used to enhance security to a certain extent.

2. Restrictions and Guidelines

- MD5 authentication features high security, and therefore is recommended. You must configure either plain text authentication or MD5 authentication. The HMAC-SHA256 algorithm features the highest security and consumes the maximum performance, while the MD5 algorithm features the lowest security and consumes the minimum performance. Select one according to the actual situation.
- This configuration is required if a router accesses a network that requires MD5 authentication.
- You must set the authentication type to cipher text authentication on the related interface or in the area in advance.
- Authentication succeeds only when both *key-id* and key are matched.
- Multiple *key-id* values are configured for the same interface, and the last *key-id* configured takes effect when packets are sent, but all *key-id* values can participate in the authentication when packets are received.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure cipher text authentication for an interface.

ip ospf authentication message-digest

(5) Configure an MD5 authentication key for an interface.

ip ospf message-digest-key *key-id* **md5** [**0** | **7**] *key*

The cipher text key function is disabled by default.

1.12 Enabling Fast Reroute

1.12.1 Overview

Once OSPF detects a route failure, the router can immediately switch to the second-best route. This configuration helps shorten the traffic interruption time.

1.12.2 Restrictions and Guidelines

- The OSPF basic functions must be configured.
- The LAF configuration for fast reroute is mutually exclusive with the virtual link configuration.
- The **carrier-delay** value must be set to **0** for an interface.

1.12.3 Configuration Tasks

The configuration for enabling fast reroute includes the following tasks:

- Configuring Fast Reroute
- (Optional) Configuring Interface LFA Protection
- (Optional) Preventing an Interface From Becoming a Backup Interface

1.12.4 Configuring Fast Reroute

1. Overview

This configuration is required if you want to increase the OSPF network convergence speed to the millisecond level.

2. Restrictions and Guidelines

- This configuration is performed on a router that has multiple paths to a destination network.
- It is recommended that automatic computation of loop-free alternate (LFA) for the backup path be disabled if any of the following cases exists on the network:
    - Virtual links exist.
    - Alternative ABRs exist.
    - An ASBR is also an ABR.
    - Multiple ABSRs advertise the same external route.
- When the OSPF fast reroute function is used, it is recommended that BFD be enabled at the same time so that the device can quickly detect any link failure and therefore shorten the forwarding interruption time. If the interface is Up or Down, to shorten the forwarding interruption time during OSPF fast reroute, you can configure

carrier-delay 0 in Layer-3 interface configuration mode to achieve the fastest switchover speed.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

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

(4) Configure fast reroute.

fast-reroute { **lfa** [**downstream-paths**] | **route-map** *route-map-name* }

The fast reroute function is disabled by default.

1.12.5 Configuring Interface LFA Protection

1. Overview

A backup route is generated for the primary route based on the LFA protection mode specified in interface configuration mode. By default, LFA protection is enabled on each OSPF interface, and a failure of the primary link does not affect data forwarding on the backup route.

2. Restrictions and Guidelines

This command does not take effect if **fast-rerotue route-map** is configured.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure interface LFA protection.

ip ospf fast-reroute protection { **node | link-node | disable** }

The LFA link protection function is enabled by default.

1.12.6 Preventing an Interface From Becoming a Backup Interface

1. Overview

This configuration is mandatory if you hope that data traffic is not switched over to a specified path after the best path fails. After the best path fails, the traffic will be switched over to another second-best path, but a new best path will be selected based on the interface costs after OSPF converges again.

2. Restrictions and Guidelines

- If the remaining bandwidth of an interface is small or if the interface and its primary interface may fail at the same time, the interface cannot be used as a backup interface. Therefore, you need to run this command in interface configuration mode to prevent this interface from becoming a backup interface during OSPF fast reroute computation. After this command is executed, a backup interface will be selected from the other interfaces.
- This command does not take effect if **fast-rerotue route-map** is configured.

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) Prevent an interface from becoming a backup interface.

ip ospf fast-reroute no-eligible-backup

By default, an interface can be used as a backup interface of OSPF fast reroute.

1.13 Modifying the Maximum Number of Concurrent Neighbors

1.13.1 Overview

This function can control the maximum number of concurrent neighbors on the OSPF process to ease the pressure on the device.

1.13.2 Restrictions and Guidelines

The OSPF basic functions must be configured.

1.13.3 Configuration Tasks

The configuration of modifying the maximum number of concurrent neighbors includes the following tasks, which are optional. Select tasks for configuration according to actual condition.

- Configuring the Maximum Number of Concurrent Neighbors on the Current Process
- Configuring the Maximum Number of Concurrent Neighbors on All Processes

1.13.4 Configuring the Maximum Number of Concurrent Neighbors on the Current Process

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 of neighbors with which each OSPF process can concurrently initiate or accept interaction.

2. Restrictions and Guidelines

This configuration is recommended if you want to set up an OSPF adjacency more quickly when a router is connected to a lot of other routers.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

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

(4) Configure the maximum number of concurrent neighbors on the current process.

max-concurrent-dd *neighbor-num*

The maximum number of neighbors of a single OSPF routing process is 5 by default.

1.13.5 Configuring the Maximum Number of Concurrent Neighbors on All Processes

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 of neighbors with which all OSPF processes can concurrently initiate or accept interaction.

2. Restrictions and Guidelines

This configuration is recommended if you want to set up an OSPF adjacency more quickly when a router is connected to a lot of other routers.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

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

router ospf max-concurrent-dd *max-neighbor*

The maximum number of neighbors of all OSPF routing processes is 10 by default.

1.14 Configuring 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.

1.14.2 Restrictions and Guidelines

- The OSPF basic functions must be configured.
- 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 Configuration Tasks

The configuration for enabling the GR function includes the following tasks:

(1) Enabling the GR Function

(2) (Optional) Configuring the OSPF GR Helper Function

1.14.4 Enabling the GR Function

1. Overview

The GR function is configured based on the OSPF process. You can configure different parameters for different OSPF processes based on the actual conditions. This command is used to configure the GR restarter capability of a device. The grace period is the maximum time of the entire GR process, during which link state is rebuilt so that the original state of the OSPF process is restored. After the GR period expires, OSPF exits the GR state and performs common OSPF operations.

2. Restrictions and Guidelines

- You are advised to retain the default configuration.
- The precondition for successful execution of GR and uninterrupted forwarding is that the topology remains stable. If the topology changes, OSPF quickly converges without waiting for further execution of GR, thus avoiding long-time forwarding black-hole.
- Disabling topology detection: If OSPF cannot converge in time when the topology changes during the hot standby process, forwarding black-hole may appear in a long time.
- Configuring topology detection: Forwarding may be interrupted when topology detection is enabled, but the interruption time is far shorter than that when topology detection is disabled.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

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

(4) Enable the opaque LSA processing capability.

capability opaque

The opaque LSA processing capability is enabled by default.

(5) Enable the GR function.

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

The GR capability is enabled by default.

1.14.5 Configuring the OSPF GR Helper Function

1. Overview

When a neighbor router implements GR, it 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 to complete GR. The **disable** option indicates that the GR helper is not provided for any device that implements GR.

2. Restrictions and Guidelines

- You are advised to retain the default configuration.
- After a device becomes a GR helper, the network changes are not detected by default. If any change takes place on the network, the network topology converges after GR is completed. If you hope that network changes can be quickly detected during the GR process, you can configure **strict-lsa-checking** to check Type-1 to Type-5 and Type-7 LSAs that indicate the network information or **internal-lsa-checking** to check Type-1 to Type-3 LSAs that indicate internal routes of the AS domain. When the network scale is large, it is recommended that you disable the LSA checking options (strict-lsa-checking and internal-lsa-checking) because regional network changes may trigger termination of GR and consequently reduce the convergence of the entire network.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

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

(4) Configure the OSPF GR helper function.

graceful-restart helper { **disable** | **strict-lsa-checking** | **internal-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 Correlating OSPF with BFD

1.15.1 Overview

Once a link is faulty, OSPF can quickly detect the failure of the route. This configuration helps shorten the traffic interruption time.

1.15.2 Restrictions and Guidelines

- The OSPF basic functions must be configured.
- 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.
- The configuration must be performed on routers at both ends of the link.

1.15.3 Configuration Tasks

The configuration for correlating OSPF with BFD includes the following tasks, which are optional. Select tasks for configuration according to actual condition.

- Configuring BFD Correlation with OSPF on an Interface
- Configuring BFD Correlation with OSPF Globally

1.15.4 Configuring BFD Correlation with OSPF on an Interface

1. Overview

Correlating OSPF with BFD on a specified interface can quickly detect the interface fault and accelerate OSPF convergence.

2. Restrictions and Guidelines

- The BFD configured on an interface takes precedence over that configured in OSPF process configuration mode.
- Based on the actual environment, you can run the **ip ospf bfd** command to enable BFD on a specified interface for link detection, or run the **bfd all-interfaces** command in OSPF process configuration mode to enable BFD on all interfaces of the OSPF process, or run the **ip ospf bfd disable** command to disable BFD on a specified interface.

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) Correlate OSPF with BFD on an interface.

ip ospf bfd [**disable**]

By default, the BFD function is disabled on an interface, and the BFD configuration is subject to that configured in RIP process configuration mode.

1.15.5 Configuring BFD Correlation with OSPF Globally

1. Overview

OSPF dynamically discovers neighbors through the hello packets. After OSPF enables the BFD function, a BFD session will be set up to achieve the full adjacency, and the BFD mechanism is used to detect the neighbor state. Once a neighbor failure is detected through BFD, OSPF performs network convergence immediately.

2. Restrictions and Guidelines

You can also run the **ip ospf bfd** [**disable**] command in interface configuration mode to enable or disable the BFD function on a specified interface, and this configuration takes precedence over the **bfd all-interfaces** command used in OSPF process configuration mode.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

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

(4) Enter correlation with BFD in OSPF configuration mode.

bfd all-interfaces

By default, the BFD function is disabled on all the interfaces.

1.16 Enabling Overflow

1.16.1 Overview

New routes are not loaded to routers when the router memory is insufficient or the usage of the database space reaches the upper limit.

1.16.2 Restrictions and Guidelines

- The OSPF basic functions must be configured.
- After a router enters the overflow state, you can run the **clear ip ospf process** command, or stop and then restart the OSPF protocol to exit the overflow state.

1.16.3 Configuration Tasks

The configuration of enabling overflow includes the following tasks, which are optional. Select tasks for configuration according to actual condition.

- Configuring the Memory Overflow Function
- Configuring the Database Overflow Function
- Configuring the External LSA Database Overflow Function

1.16.4 Configuring the Memory Overflow Function

1. Overview

The OSPF process enters the overflow state to discard newly-learned external routes. This behavior can effectively prevent the memory usage from increasing.

2. Restrictions and Guidelines

- This configuration is recommended if a large number of routes exist in the domain and may cause insufficiency of the router memory.
- After the overflow function is enabled, the OSPF process enters the overflow state and discards newly-learned external routes, which may cause a routing loop on the entire network. To reduce the occurrence probability of this problem, OSPF generates a default route to the null interface, and this route always exists in the overflow state.
- You can run the **clear ip ospf process** command to reset the OSPF process so that the OSPF process can exit the overflow state. You can run the **no** form of the command to prevent the OSPF process from entering the overflow state when the memory is insufficient. This, however, may lead to over-consumption of the memory resource, after which the OSPF process will stop and delete all the learned routes.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

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

(4) Configure the memory overflow function.

overflow memory-lack

By default, the OSPF process is allowed to enter the overflow state when the memory is insufficient.

1.16.5 Configuring the Database Overflow Function

1. **Overview**

This function controls the maximum number of routes in LSDB to avoid abnormal operation of a router due to insufficient memory.

2. **Restrictions and Guidelines**

This configuration is recommended if a large number of routes exist in the domain and may cause insufficiency of the router memory.

3. **Procedure**

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

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

(4) Configure the database overflow function.

overflow database *max-lsa* [**hard** | **soft**]

The maximum number of LSAs is not configured by default.

1.16.6 Configuring the External LSA Database Overflow Function

1. **Overview**

This function controls the maximum number of external routes in LSDB to avoid abnormal operation of a router due to insufficient memory.

2. **Restrictions and Guidelines**

- This configuration is recommended if the ASBR introduces a large number of external routes and the router memory may be insufficient.
- When using the overflow function, ensure that the same *max-dbsize* is configured on all routers in the OSPF backbone area and common areas; otherwise, the following problems may occur:
  - The LSDBs throughout the network are inconsistent, and the neighbor relationship fails to reach the full state.
  - Routes are incorrect, including routing loops.
  - AS external LSAs are frequently retransmitted.

- If the maximum number of external LSAs is set, when the number of external LSAs exceeds the maximum, the normal state will not be restored.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

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

(4) Configure the external LSA database overflow function.

overflow database external *max-dbsize wait-time*

The maximum number of external LSAs is not configured by default.

1.17 Configuring VPN Extended Feature of OSPF

1.17.1 Overview

When OSPF is enabled on a VPN client network, OSPF runs between the PE and CE to simplify the configuration and management of CE.

1.17.2 Restrictions and Guidelines

The router ID of Label Distribution Protocol (LDP) must consist of 32 bits.

1.17.3 Configuration Tasks

The configuration of VPN extended feature of OSPF includes the following tasks:

- (Optional) Configuring Domain ID
- (Optional) Configuring a Sham Link
- (Optional) Configuring a Domain Label
- (Optional) Disabling Loop Detection for a VRF OSPF ProcessDisabling Loop Detection for a VRF OSPF Process
- (Optional) Configuring Extcommunity Attribute for a VPN Route
- Disabling Loop Detection Using the DN Bit of LSA
- Disabling Loop Detection Using the Route Tag of LSA

1.17.4 Configuring Domain ID

1. Overview

Domain ID is used to indicate the domain information of an OSPF process.

A VRF OSPF process can be configured with multiple domain IDs, but only one is the primary domain ID, and the remaining ones are secondary domain IDs. An OSPF route is converted into a VPN route for advertising, and only the primary domain ID is included in a VPN route.

2. Restrictions and Guidelines

- This function takes effect only for the OSPF process associated with VRF.
- The domain IDs of different VRF OSPF processes do not influence each other, and can be configured the same. However, the VRF OSPF processes that belong to the same VPN must be configured with the same domain ID to ensure the correctness of route advertising.
- You are advised to configure all the VRF OSPF processes that belong to the same VPN with the same domain ID.

3. Prerequisites

Before configuring the VPN feature, complete the VRF configuration.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *ospf-id* **vrf** *vrf-name*

(4) Configure a domain ID.

domain-id { *ipv4-address* [**secondary**] | **null** | **type** { **0005** | **0105** | **0205** | **8005** } **value** *hex-value* [**secondary**] }

By default, the domain ID value of an OSPF process is **null**, and the type value is 0x0005.

1.17.5 Configuring a Domain Label

1. Overview

If a VPN site is connected to multiple PEs, the VPN route is learned from the PE through MP-BGP. If the route is advertised to the VPN site through a Type-5 or Type-7 LSA, it may be learned and advertised by other PE routers connected to the VPN site, which may cause a loop. To prevent the preceding loop, the VRF OSPF processes connected to the same VPN site on the PEs are configured with the same VPN route tag. When a VRF OSPF process sends a Type-5 or Type-7 LSA to a VPN site, the VPN route tag information will also be attached to the LSA. When other PE sites receive such a Type-5 or Type-7 LSA, if they detect that the VPN route tag in the LSA is consistent with that of the local OSPF process, the LSA will not participate in the OSPF computation. Generally, the OSPF processes belonging to the same VPN site are configured with the same tag value.

The VPN route tag occupies four bytes in an OSPF packet. If a VRF OSPF process is not configured with this command, when the OSPF process advertises a Type-5 or Type-7 LSA, the first two bytes of the VPN route tag are set to 0xD000 by default, and the last two bytes are the AS number of local BGP. For example, if the AS number of the local BGP is 1, the hexadecimal form of the VPN route tag is 0xD0000001.

2. Restrictions and Guidelines

This function takes effect only for the OSPF process associated with VRF and BGP redistributed routes.

3. Prerequisites

Before configuring the VPN feature, complete the VRF configuration.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *ospf-id* **vrf** *vrf-name*

(4) Configure a VPN route tag.

domain-tag *tag*

By default, the default value of a VRF OSPF process is the AS number of the local BGP protocol.

1.17.6 Configuring a Sham Link

1. Overview

A sham link is used in an environment with backdoor links between VPN sites. If you still want VPN data to be transmitted through the MPLS backbone network in this case, you can establish a sham link between the VRF OSPF processes of two PEs. The VRF OSPF processes of two PEs can set up an OSPF neighbor relationship through the sham link and distribute LSA packets on the sham link.

2. Restrictions and Guidelines

- The area ID of sham link configured for the two PEs must be consistent.
- The combination of source address and destination address of a sham link configured on one PE must be equal

to the combination of destination address and source address of a sham link configured on the other PE.

- Both the source address and destination address used to establish a sham link on the PEs must be a 32-bit loopback address bound to the corresponding VRF.
- Since the OSPF route advertised through a sham link has no VPN label, the route cannot be used for forwarding. Actually packets are still forwarded through the BGP VPNv4 route. Therefore, in the actual configuration, you must ensure that the route advertised through the sham link will also be learned through MP-BGP.
- The source address for establishing the sham link must participate in the BGP VPNv4 route advertisement, but cannot join the calculation of VRF OSPF process.

3. Prerequisites

Before configuring the VPN feature, complete the VRF configuration.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *ospf-id* **vrf** *vrf-name*

(4) Configure a sham link.

area *area-id* **sham-link** *source-ipv4-address destination-ipv4-address* [[**authentication** [**keychain** *kechain-name* | **message-digest** | **null**] | **cost** *number* | **dead-interval** ***dead-interval*** | **hello-interval** *hello-interval* | **retransmit-interval** *retransmit-interval* | **transmit-delay** *transmit-delay*] * | **authentication-key [0** | **7]** *key* | **message-digest-key** *key-id* **md5** [**0** | **7**] *key*]

No sham link is configured by default.

1.17.7 Disabling Loop Detection for a VRF OSPF Process

1. Overview

Loop detection of OSPF processes aims to prevent possible loop of VPN routes in propagation.

2. Restrictions and Guidelines

- By default, the VRF OSPF process supports the PE-CE OSPF features (that is, conversion from domain ID to LSA, to DN bits, and to VPN route tag). If you do not want a VRF OSPF process to support the PE-CE OSPF features, disable the PE-CE OSPF features by running the **capability vrf-lite** command.
- This command takes effect only for the OSPF process associated with VRF.

- In some application scenarios, you may need to disable the loop detection function of VRF OSPF processes. For example, VPN users use MCE devices to exchange VPN routes with PEs, if the OSPF protocol runs between MCEs and PEs to exchange VPN routes, to enable the VPN site to learn the routes of other VPN sites, you need to run the **capability vrf-lite** command to disable the loop detection function of VRF OSPF processes on the MCE device.

3. Prerequisites

Before configuring the VPN feature, complete the VRF configuration.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *ospf-id* **vrf** *vrf-name*

(4) Configure capability vrf-lite.

capability vrf-lite [**auto**]

By default, the automatic judging function of support to loop detection is enabled for the OSPF processes associated with VRF.

1.17.8 Configuring Extcommunity Attribute for a VPN Route

1. Overview

When an OSPF route of VRF forms a VPN route, the Router-ID and Router-Type of the OSPF process will also be carried in the extcommunity attribute of the VPN route. To ensure compatibility with the implementations of different vendors, you can manually modify the Router-ID and Router-Type.

2. Restrictions and Guidelines

- When OSPF routes are redistributed to BGP to form VPN routes, the extcommunity attributes of OSPF routes, including the extcommunity attributes of **router-id** and **route-type**, will also be attached. By default, the extcommunity attribute type of **router-id** is 0x0107, and the extcommunity attribute of **route-type** is 0x0306. You can also use commands to manually configure the extcommunity attributes of **router-id** and **route-type**.
- This function takes effect only for the OSPF process associated with VRF.
- Configuring the type of **router-id** aims to ensure compatibility with the implementations of different vendors. For example, some vendors support the **router-id** type “0x0107” only. In the case of interconnection with the devices of these vendors, you need to set the type of **router-id** to 0x0107 by using the **extcommunity-type** command.

- Configuring the type of **router-type** aims to ensure compatibility with the implementations of different vendors. For example, some vendors support the **route-type** “0x8000” only. In the case of interconnection with the devices of these vendors, you need to set **route-type** to 0x8000 by using the **extcommunity-type** command.

3. Prerequisites

Before configuring the VPN feature, complete the VRF configuration.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *ospf-id* **vrf** *vrf-name*

(4) Configure **extcommunity-type**.

extcommunity-type { **router-id** { **0107 | 8001** } | **route-type** { **0306** | **8000** } }

By default, the type of **router-id** is 0107, and the type of **route-type** is 0306.

1.17.9 Disabling Loop Detection Using the DN Bit of LSA

1. Overview

In the CE dual-homing scenario of L3VPN, loop is avoided by suppressing the route computation of DN bit between PEs. However, in a specific scenario, PEs may be allowed to learn routes from each other without generating any loops. In this case, check of the DN bit can be cancelled by configuring this command. When a PE device is connected to an MCE device, the MCE device needs to calculate the route advertised by the PE and the DN bit will not be checked. Type-3, Type-5, and Type-7 LSAs of OSPF can all carry a DN bit.

2. Restrictions and Guidelines

This function takes effect only for the OSPF process associated with VRF.

3. Prerequisites

Before configuring the VPN feature, complete the VRF configuration.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *ospf-id* **vrf** *vrf-name*

(4) Disable loop detection using the DN bit of LSA.

disable-dn-bit-check [**summary | ase | nssa**]

The DN bit loop detection function of LSA is enabled by default.

1.17.10 Disabling Loop Detection Using the Route Tag of LSA

1. Overview

In the CE dual-homing scenario of L3VPN, when the LSA route tag received by a PE is the same as its route tag, the route is not calculated, thus avoiding a loop. In a specific scenario, PEs are allowed to learn routes from each other without generating any loops. In this case, you can set different route tags for multiple PEs, or set to disable route tag check. When a PE device is connected to an MCE device, the MCE device needs to calculate the route advertised by the PE and the route tag will not be checked. Type-5 and Type-7 LSAs of OSPF can carry a route tag.

2. Restrictions and Guidelines

This command takes effect only for the OSPF process associated with VRF.

3. Prerequisites

Before configuring the VPN feature, complete the VRF configuration.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *ospf-id* **vrf** *vrf-name*

(4) Disable loop detection using the route tag of LSA.

disable-tag-check

The loop detection function using the route tag of LSA is enabled by default.

1.18 Configuring Network Management Functions

1.18.1 Overview

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

1.18.2 Restrictions and Guidelines

- The OSPF basic functions must be configured.
- You must enable the MIB function of the SNMP-Server before enabling the OSPF MIB function.
- You must enable the Trap function of the SNMP-Server before enabling the OSPF Trap function.
- You must enable the logging function of the device before outputting the OSPF logs.

1.18.3 Configuration Tasks

The configuration of network management functions includes the following tasks:

- Binding the MIB with an OSPF Process
- Configuring the Trap Function
- Configuring the Logging Function

1.18.4 Binding the MIB with an OSPF Process

1. Overview

This configuration is required if you want to use the network management software to manage parameters of a specified OSPF process.

2. Restrictions and Guidelines

- The OSPFv2 MIB does not have the OSPFv2 process information. Therefore, you must perform operations on a single OSPFv2 process through SNMP. By default, the OSPFv2 MIB is bound with the OSPFv2 process with the smallest process ID, and all user operations take effect on this process.
- If you hope to perform operations on a specified OSPFv2 process through SNMP, run this command to bind the MIB to the process.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

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

(4) Bind the MIB with an OSPF process.

enable mib-binding

By default, the MIB is bound to the OSPFv2 process with the minimum process ID.

1.18.5 Configuring the Trap Function

1. Overview

This configuration is required if you want to use the network management software to monitor the OSPF running status.

2. Restrictions and Guidelines

- The function configured by this command is restricted by the **snmp-server** command. You need to configure the **snmp-server enable traps ospf** command and then the **enable traps** command before the corresponding OSPF trap can be correctly sent out.
- This command is not restricted by the MIB bound to the process. The trap switch can be enabled concurrently for different processes.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

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

(4) Configure the trap function.

enable traps [**error** [**IfAuthFailure** | **IfConfigError** | **IfRxBadPacket** | **VirtIfAuthFailure** | **VirtIfConfigError** | **VirtIfRxBadPacket**] | **lsa** [**LsdbApproachOverflow** | **LsdbOverflow** | **MaxAgeLsa** | **OriginateLsa**] | **retransmit** [**IfTxRetransmit** | **VirtIfTxRetransmit**] | **state-change** [**IfStateChange** | **NbrRestartHelperStatusChange** | **NbrStateChange** | **NssaTranslatorStatusChange** | **RestartStatusChange** | **VirtIfStateChange** | **VirtNbrRestartHelperStatusChange** | **VirtNbrStateChange**]]

The trap message sending function is disabled by default.

1.18.6 Configuring the Logging Function

1. Overview

This function outputs the relevant log records so that the related information can be analyzed and found easily.

2. Restrictions and Guidelines

You are advised to retain the default configuration. If you want to reduce the log output, disable this function.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

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

(4) 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.

1.19 Enabling NSR

1.19.1 Overview

During an active/standby switchover of devices in distributed (with the independent active/standby modular engine) or VSU mode, data forwarding continues and is not interrupted.

1.19.2 Restrictions and Guidelines

- The OSPF basic functions must be configured.
- You are advised to retain the default configuration.
- This command is used to enable the NSR function. For the same OSPF 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 a distributed or VSU mode takes a period of time. If the OSPF neighbor keepalive duration is shorter than the switchover duration, the OSPF neighbor relationship with the neighbor device is removed, and services are interrupted during the switchover. Therefore, it is recommended that the OSPF neighbor keepalive duration be no smaller than the default value when the NSR function is enabled. It is recommended that the fast hello function be disabled because when it is enabled, the OSPF neighbor keepalive duration is less than 1s.

1.19.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

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

(4) Enable the NSR function.

nsr

The NSR function is disabled by default.

1.20 Enabling the iSPF Feature

1.20.1 Overview

OSPF adopts the iSPF algorithm to compute a network topology. The iSPF function is generally used on a large-sized network to ease the pressure on router processors.

1.20.2 Restrictions and Guidelines

- The OSPF basic functions must be configured.
- This configuration is recommended if you hope to accelerate route convergence in a single area with more than 100 routers.
- This configuration is performed on all routers in the area.
- After iSPF is enabled, OSPF will use the iSPF algorithm to compute the network topology. That is, after the network topology changes, OSPF corrects only the nodes affected by the topological change, instead of re-building the entire SPT.

1.20.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

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

(4) Configure the **i**SPF feature.

ispf enable

The iSPF feature is disabled by default.

1.21 Configuring to Disable MTU Verification

1.21.1 Overview

On receiving the database description packet, OSPF checks whether the MTU of the interface on the neighbor is the same as the MTU of its own interface. If the interface MTU specified in the received database description packet is greater than the MTU of the local interface, the adjacency cannot be set up. To resolve this problem, you can disable MTU verification.

1.21.2 Restrictions and Guidelines

- The OSPF basic functions must be configured.
- You are advised to retain the default configuration.
- This configuration is performed on two routers with different interface MTUs.

1.21.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure to disable MTU verification.

ip ospf mtu-ignore

The MTU verification function is disabled by default.

1.22 Configuring a Super VLAN to Enable OSPF

1.22.1 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 OSPF multicast packets are sent over a super VLAN containing multiple sub VLANs, the OSPF 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 certain application scenarios in which OSPF packets need to be sent over a super VLAN, the packets only need to be sent over a sub VLAN of the super VLAN. In this case, you can run the command to specify a sub VLAN to avoid the neighbor flapping caused by a device processing bottleneck.

1.22.2 Restrictions and Guidelines

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

1.22.3 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 the **subvlan** feature.

ip ospf subvlan *vlan-id*

The OSPF function is not configured for a super VLAN by default.

1.23 Monitoring

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

You can run the **clear** commands to clear information.

⚠ Caution

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

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

⚠ Caution

When the **debug** command is used to output debugging information, system resources are occupied. Therefore, disable the debugging function immediately after use.

Table 1-1 OSPF Monitoring

Command	Purpose
show ip ospf [*process-id*]	Displays the OSPF process configuration

Command	Purpose
	information.
show ip ospf [*process-id*] **border-routers**	Displays the OSPF internal routing table (the routes to ABRs and ASBRs).
show ip ospf [*process-id area-id*] **database** [{ **asbr-summary** | **external** | **network** | **nssa-external** | **opaque-area** | **opaque-as** | **opaque-link** | **router** | **summary** }] [{ **adv-router** *ip-address* | **self-originate** } | *link-state-id* | **brief**] [**database-summary** | **max-age** | **detail**]	Displays the information of the OSPF LSDB.
show ip ospf [*process-id*] **interface** [*interface-type interface-number* | **brief**]	Displays the OSPF-enabled interface.
show ipv6 ospf [*process- id*] **keepalive** [**process** | **area** [*area-id*] | **interface** [*interface-type interface-number*] [**with-clear** | **nbr**] | [**virtual-link** | **send-queue** | **recv-queue**] [**with-clear**]]	Displays the OSPFv3 keepalive thread information.
show ip ospf [*process-id*] **neighbor** [[*interface-type interface-number* | *neighbor-id*] * [**detail**] | **statistics**]	Displays the neighbor list of an OSPF process.
show ip ospf [*process-id*] **route** [**count**]	Displays the OSPF routing table.
show ip ospf [*process-id*] **sham-links** [**area** *area-id*]	Displays the sham link information of an OSPF process.
show ip ospf [*process-id*] **spf**	Displays the number of times SPT is computed in the OSPF area.
show ip ospf [*process-id*] **summary-address**	Displays the summarized route of OSPF redistributed routes.
show ip ospf [*process-id* [*area-id*]] **topology** [**adv-router** *adv-router-id* [*router-id*] | **self-originate** [*router-id*]]	Displays the OSPF network topology information.
show ip ospf [*process-id*] **virtual-links** [*ip-address*]	Displays OSPF virtual links.
show running-config router ospf	Displays the OSPF configuration.
clear ip ospf [*process-id*] **process**	Clears and resets an OSPF process.

Command	Purpose
debug ip ospf events [**abr** | **asbr** | **lsa** | **nssa** | **os** | **restart** | **router** | **slink** | **vlink**]	Debugs OSPF events.
debug ip ospf ifsm [**events** | **status** | **timers**]	Debugs OSPF interfaces.
debug ip ospf nfsm [**events** | **status** | **timers**]	Debugs OSPF neighbors.
debug ip ospf nsm [**interface** | **redistribute** | **route**]	Debugs the OSPF NSM.
debug ip ospf lsa [**flooding** | **generate** | **install** | **maxage** | **refresh**]	Debugs OSPF LSAs.
debug ip ospf packet [**dd | detail** | **hello** | **ls-ack** | **ls-request** | **ls-update** | **recv** | **send**]	Debugs OSPF packets.
debug ip ospf route [**ase** | **ia** | **install** | **spf** | **time**]	Debugs OSPF routes.

1.24 Configuration Examples

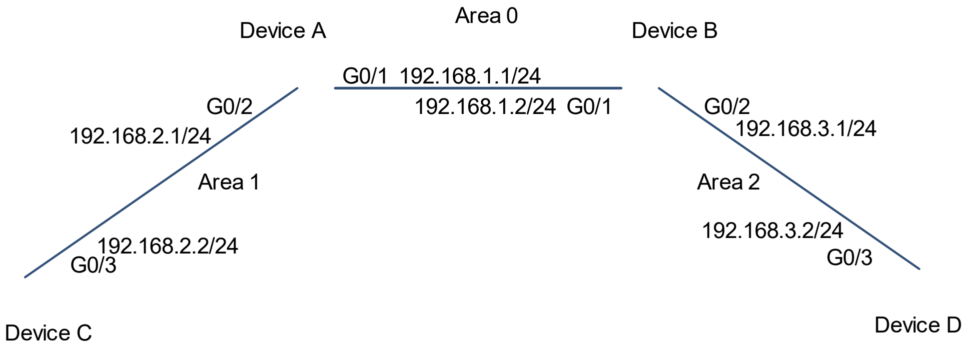
1.24.1 Configuring Basic Functions of OSPF

1. Requirements

OSPF is enabled on all the devices, and three areas are defined in total. Device A and device B are used as ABR forwarding inter-area routes so as to implement the interworking between all networks. After configuration, all devices can learn the routing of all network segments in the AS, and the neighbor relationships are correct.

2. Topology

Figure 1-1 Topology for Configuring Basic Functions of OSPF



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 the OSPF processes and router IDs on all the devices.
- Configure interface configuration OSPF on all the devices.

4. Procedure

(1) Configure interface IP addresses on all the devices.

Configure Device A.

```
Device A> enable
Device A# configure terminal
Device A(config)# interface GigabitEthernet 0/1
Device A(config-if-GigabitEthernet 0/1)# ip address 192.168.1.1 255.255.255.0
Device A(config-if-GigabitEthernet 0/1)# exit
Device A(config)# interface GigabitEthernet 0/2
Device A(config-if-GigabitEthernet 0/2)# ip address 192.168.2.1 255.255.255.0
Device A(config-if-GigabitEthernet 0/2)# exit
```

Configure Device B.

```
Device B> enable
Device B# configure terminal
Device B(config)# interface GigabitEthernet 0/1
Device B(config-if-GigabitEthernet 0/1)# ip address 192.168.1.2 255.255.255.0
Device B(config-if-GigabitEthernet 0/1)# exit
Device B(config)# interface GigabitEthernet 0/2
Device B(config-if-GigabitEthernet 0/2)# ip address 192.168.3.1 255.255.255.0
Device B(config-if-GigabitEthernet 0/2)# exit
```

Configure Device C.

```
Device C> enable
Device C# configure terminal
Device C(config)# interface GigabitEthernet 0/3
Device C(config-if-GigabitEthernet 0/3)# ip address 192.168.2.2 255.255.255.0
Device C(config-if-GigabitEthernet 0/3)# exit
```

Configure Device D.

```
Device D> enable
Device D# configure terminal
Device D(config)# interface GigabitEthernet 0/3
Device D(config-if-GigabitEthernet 0/3)# ip address 192.168.3.2 255.255.255.0
Device D(config-if-GigabitEthernet 0/3)# exit
```

(2) Configure the OSPF process, router ID, and the interface configuration OSPF.

Configure Device A.

```
Device A(config)# router ospf 1
Device A(config-router)# router-id 192.168.1.1
Device A(config-router)# network 192.168.1.0 0.0.0.255 area 0
Device A(config-router)# network 192.168.2.0 0.0.0.255 area 1
```

Configure Device B.

```
Device B(config)# router ospf 1
Device B(config-router)# router-id 192.168.1.2
Device B(config-router)# network 192.168.1.0 0.0.0.255 area 0
Device B(config-router)# network 192.168.3.0 0.0.0.255 area 2
```

Configure Device C.

```
Device C(config)# router ospf 1
Device C(config-router)# router-id 192.168.2.2
Device C(config-router)# network 192.168.2.0 0.0.0.255 area 1
```

Configure Device D.

```
Device D(config)# router ospf 1
Device D(config-router)# router-id 192.168.3.2
Device D(config-router)# network 192.168.3.0 0.0.0.255 area 2
```

5. Verification

(1) Check the OSPF neighbor and route of Device A.

Check the OSPF route of Device A.

```
Device A# show ip route ospf
O IA 192.168.3.0/24 [110/2] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1
```

Check the neighbor information of Device A.

```
Device A# show ip ospf neighbor
OSPF process 1, 2 Neighbors, 2 is Full:
Neighbor ID   Pri   State      Dead Time   Address       Interface
192.168.1.2   1     Full/DR    00:00:40    192.168.1.2   GigabitEthernet 0/1
192.168.2.2   1     Full/BDR   00:00:34    192.168.2.2   GigabitEthernet 0/2
```

(2) Check the OSPF neighbor and route of Device B.

Check the OSPF route of Device B.

```
Device B# show ip route ospf
O IA 192.168.2.0/24 [110/2] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1
```

Check the neighbor information of Device B.

```
Device B# show ip ospf neighbor
OSPF process 1, 2 Neighbors, 2 is Full:
Neighbor ID   Pri   State      Dead Time   Address       Interface
192.168.1.1   1     Full/BDR   00:00:32    192.168.1.1   GigabitEthernet 0/1
192.168.3.2   1     Full/BDR   00:00:30    192.168.3.2   GigabitEthernet 0/2
```

(3) Check the OSPF neighbor and route of Device C.

Check the OSPF route of Device C.

```
Device C# show ip route ospf
O IA 192.168.1.0/24 [110/2] via 192.168.2.1, 00:19:05, GigabitEthernet 0/3
O IA 192.168.3.0/24 [110/3] via 192.168.2.1, 00:19:05, GigabitEthernet 0/3
```

Check the neighbor information of Device C.

```
Device C# show ip ospf neighbor
OSPF process 1, 1 Neighbors, 1 is Full:
Neighbor ID   Pri   State      Dead Time   Address       Interface
192.168.1.1   1     Full/BDR   00:00:32    192.168.2.1   GigabitEthernet 0/3
```

(4) Check the OSPF neighbor and route of Device D.

Check the OSPF route of Device D.

```
Device D# show ip route ospf
O IA 192.168.1.0/24 [110/2] via 192.168.3.1, 00:19:05, GigabitEthernet 0/3
O IA 192.168.2.0/24 [110/3] via 192.168.3.1, 00:19:05, GigabitEthernet 0/3
```

Check the neighbor information of Device D.

```
Device D# show ip ospf neighbor
OSPF process 1, 1 Neighbors, 1 is Full:
```

```
Neighbor ID   Pri   State      Dead Time   Address       Interface
192.168.1.2   1     Full/BDR   00:00:30    192.168.3.1   GigabitEthernet 0/3
```

(5) Ping 192.168.2.2 on Device D. The network is reachable.

```
Device D# ping 192.168.2.2
Sending 5, 100-byte ICMP Echoes to 192.168.2.2, timeout is 2 seconds:
< press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms.
```

6. Configuration Files

- Device A configuration file

```
!
interface GigabitEthernet 0/1
 ip address 192.168.1.1 255.255.255.0
!
interface GigabitEthernet 0/2
 ip address 192.168.2.1 255.255.255.0
!
router ospf 1
 router-id 192.168.1.1
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.2.0 0.0.0.255 area 1
!
```

- Device B configuration file

```
!
interface GigabitEthernet 0/1
 ip address 192.168.1.2 255.255.255.0
!
interface GigabitEthernet 0/2
ip address 192.168.3.1 255.255.255.0
!
router ospf 1
 router-id 192.168.1.2
 network 192.168.1.0 0.0.0.255 area 0
! network 192.168.3.0 0.0.0.255 area 2
```

- Device C configuration file

```
!
interface GigabitEthernet 0/3
 ip address 192.168.2.2 255.255.255.0
!
```

```
router ospf 1
 router-id 192.168.2.2
 network 192.168.2.0 0.0.0.255 area 1
!
```

- Device D configuration file

```
!
interface GigabitEthernet 0/3
 ip address 192.168.3.2 255.255.255.0
!
router ospf 1
 router-id 192.168.3.2
 network 192.168.3.0 0.0.0.255 area 2
!
```

7. Common Errors

- OSPF cannot be enabled because the IP unicast routing function is disabled.
- The network segment configured by the **network** command does not include the interface IP addresses.
- The area IDs configured for adjacent interfaces are inconsistent.
- The same router ID is configured on multiple devices, resulting in a router ID conflict.
- The same interface IP address is configured on multiple devices, resulting in a running error of the OSPF network.

1.24.2 Configuring a Stub Area

1. Requirements

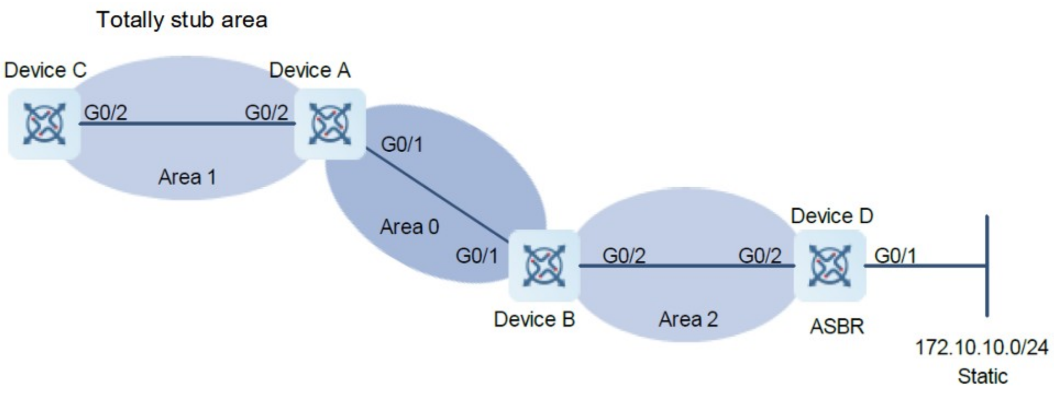
Device A, Device B, Device C, and Device D are interconnected through the OSPF routing protocol.

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

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



3. Notes

- Configure interface IP addresses for all devices (omitted).
- Configure OSPF basic functions on all devices (omitted).
- Introduce an external static route to Device D.
- Configure Area 1 as a stub area on Device A and Device C.

4. Procedure

(1) Introduce an external static route to Device D.

```
Device D> enable
Device D# configure terminal
Device D(config)# router ospf 1
Device D(config-router)# redistribute static subnets
```

(2) Configure Area 1 as a stub area on Device A and Device C.

Configure Device A.

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

Configure Device C.

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

5. Verification

On Device C, run the **show ip route ospf** command 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 ip route ospf
O*IA 0.0.0.0/0 [110/2] via 192.168.2.1, 00:30:53, GigabitEthernet 0/2
```

6. Configuration Files

- Device A configuration file

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

- Device C configuration file

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

- Device D configuration file

```
!
router ospf 1
 redistribute static subnets
!
```

1.24.3 Configuring an NSSA

1. Requirements

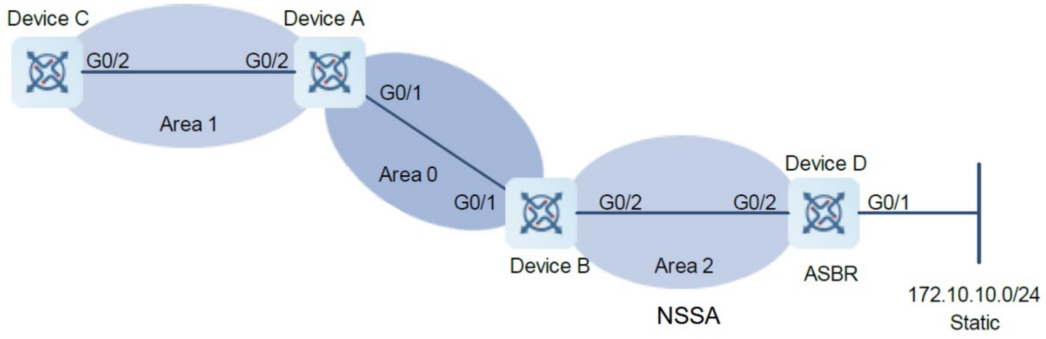
Device A, Device B, Device C, and Device D are interconnected through the OSPF routing protocol.

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

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



3. Notes

- Configure interface IP addresses for all devices (omitted).
- Configure OSPF basic functions on all devices (omitted).
- Introduce an external static route to Device D.
- Configure Area 2 as NSSA on Device B and Device D.

4. Procedure

(1) Configure a static route for Device D.

```
Device D> enable
Device D# configure terminal
Device D(config)# ip route 172.10.10.0 255.255.255.0 192.168.6.2
```

(2) Introduce an external static route to Device D.

```
Device D(config)# router ospf 1
Device D(config-router)# redistribute static subnets
```

(3) Configure Area 2 as NSSA on Device B and Device D.

Configure Device B.

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

Configure Device D.

```
Device D(config-router)# area 2 nssa
```

5. Verification

On Device D, check the Type-7 LSAs generated from 172.10.10.0/24.

```
Device D# show ip ospf database nssa-external
            OSPF Router with ID (192.168.6.2) (Process ID 1)
                NSSA-external Link States (Area 0.0.0.1 [NSSA])
  LS age: 61
  Options: 0x8 (-|-|-|-|N/P|-|-|-)
  LS Type: AS-NSSA-LSA
  Link State ID: 172.10.10.0 (External Network Number For NSSA)
  Advertising Router: 192.168.6.2
  LS Seq Number: 80000001
  Checksum: 0xc8f8
  Length: 36
  Network Mask: /24
        Metric Type: 2 (Larger than any link state path)
        TOS: 0
        Metric: 20
        NSSA: Forward Address: 192.168.6.2
        External Route Tag: 0
```

On Device B, verify that Type-5 and Type-7 LSAs are generated from 172.10.10.0/24.

```
Device B# show ip ospf database nssa-external
            OSPF Router with ID (192.168.3.1) (Process ID 1)
                NSSA-external Link States (Area 0.0.0.1 [NSSA])
  LS age: 314
  Options: 0x8 (-|-|-|-|N/P|-|-|-)
  LS Type: AS-NSSA-LSA
  Link State ID: 172.10.10.0 (External Network Number For NSSA)
  Advertising Router: 192.168.6.2
  LS Seq Number: 80000001
  Checksum: 0xc8f8
  Length: 36
  Network Mask: /24
        Metric Type: 2 (Larger than any link state path)
        TOS: 0
        Metric: 20
        NSSA: Forward Address: 192.168.6.2
        External Route Tag: 0
```

On Device B, check the Type-N2 routes generated from 172.10.10.0/24.

```
Device B# show ip ospf database external
            OSPF Router with ID (192.168.3.1) (Process ID 1)
```

```
                AS External Link States
LS age: 875
Options: 0x2 (-|-|-|-|-|-|E|-)
LS Type: AS-external-LSA
Link State ID: 172.10.10.0 (External Network Number)
Advertising Router: 192.168.3.1
LS Seq Number: 80000001
Checksum: 0xd0d3
Length: 36
Network Mask: /24
      Metric Type: 2 (Larger than any link state path)
      TOS: 0
      Metric: 20
      Forward Address: 192.168.6.2
      External Route Tag: 0
```

6. Configuration Files

- Device B configuration file

```
!
router ospf 1
 area 2 nssa
!
```

- Device D configuration file

```
!
ip route 172.10.10.0 255.255.255.0 192.168.6.2
!
router ospf 1
 redistribute static subnets
 area 2 nssa
!
```

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.

1.24.4 Correlating OSPF Process with BFD

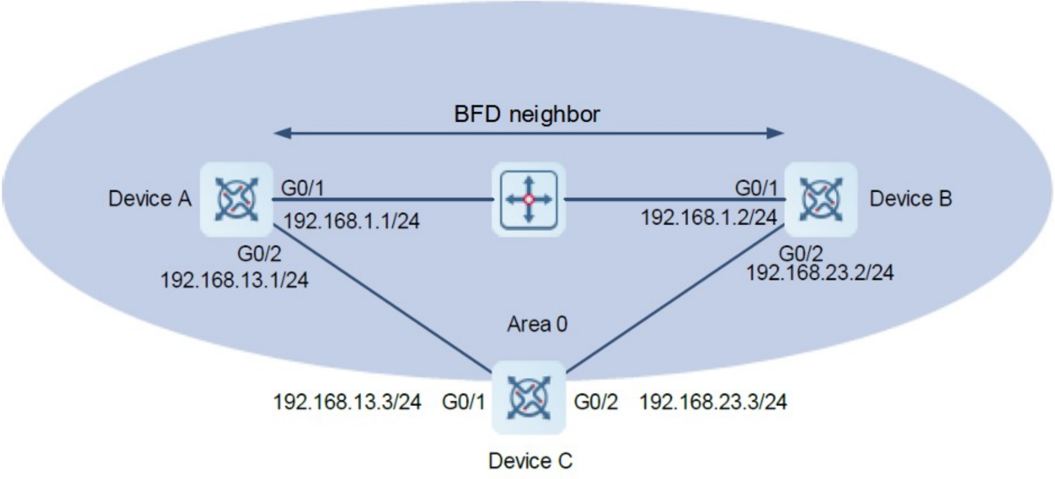
1. Requirements

Device A, Device B, and Device C implement internetworking by running OSPFv2.

Device A and Device B use a switch as the primary link. When the switch or the link connected to it fails, BFD can quickly detect the failure and switch to Device C for communication.

2. Topology

Figure 1-1 Topology for Correlating an OSPF Process with BFD



3. Notes

- Configure interface IP addresses for all devices (omitted).
- Configure OSPF basic functions on all devices (omitted).
- Configure the BFD parameters for the interfaces of all devices.
- Correlate OSPF with BFD on all the devices.

4. Procedure

(1) Configure BFD parameters for the interfaces of all devices.

Configure Device A.

```
Device A> enable
Device A# configure terminal
Device A(config)# interface GigabitEthernet 0/1
Device A(config-if-GigabitEthernet 0/1)# bfd interval 200 min_rx 200 multiplier
5
Device A(config-if-GigabitEthernet 0/1)# exit
Device A(config)# interface GigabitEthernet 0/2
Device A(config-if-GigabitEthernet 0/2)# bfd interval 200 min_rx 200 multiplier
5
Device A(config-if-GigabitEthernet 0/2)# exit
```

Configure Device B.

```
Device B> enable
Device B# configure terminal
Device B(config)# interface GigabitEthernet 0/1
Device B(config-if-GigabitEthernet 0/1)# bfd interval 200 min_rx 200 multiplier
5
Device B(config-if-GigabitEthernet 0/1)# exit
Device B(config)# interface GigabitEthernet 0/2
Device B(config-if-GigabitEthernet 0/2)# bfd interval 200 min_rx 200 multiplier
5
Device B(config-if-GigabitEthernet 0/2)# exit
```

(2) Correlate OSPF with BFD on all the devices.

Configure Device A.

```
Device A(config)# router ospf 1
Device A(config-router)# bfd all-interfaces
```

Configure Device B.

```
Device B(config)# router ospf 1
Device B(config-router)# bfd all-interfaces
```

5. Verification

On Device A, verify that correlating OSPF with BFD is up.

```
Device A# show ip ospf neighbor
OSPF process 1, 1 Neighbors, 1 is Full:
Neighbor ID     Pri   State          BFD State  Dead Time   Address
Interface
192.168.1.2       1   Full/BDR       Up         00:00:40    192.168.1.2
GigabitEthernet 0/1
192.168.13.3       1   Full/BDR       Up         00:00:40    192.168.13.3
GigabitEthernet 0/2
```

On Device B, verify that correlating OSPF with BFD is up.

```
Device B# show ip ospf neighbor
OSPF process 1, 1 Neighbors, 1 is Full:
Neighbor ID     Pri   State          BFD State  Dead Time   Address
Interface
192.168.1.1       1   Full/BDR       Up         00:00:40    192.168.1.1
GigabitEthernet 0/1
192.168.13.3       1   Full/BDR       Up         00:00:40    192.168.23.3
GigabitEthernet 0/2
```

6. Configuration Files

- Device A configuration file

```
!
interface GigabitEthernet 0/1
 bfd interval 200 min_rx 200 multiplier 5
!
interface GigabitEthernet 0/2
 bfd interval 200 min_rx 200 multiplier 5
!
router ospf 1
 bfd all-interfaces
!
```

- Device B configuration file

```
!
interface GigabitEthernet 0/1
 bfd interval 200 min_rx 200 multiplier 5
!
interface GigabitEthernet 0/2
 bfd interval 200 min_rx 200 multiplier 5
!
router ospf 1
 bfd all-interfaces
!
```

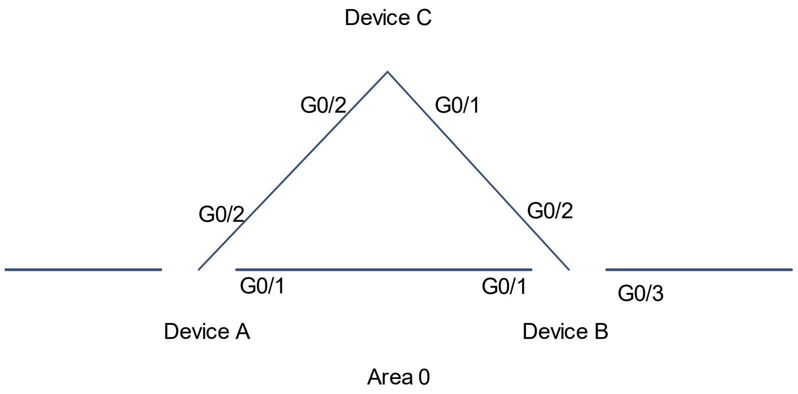
1.24.5 Configuring Fast Reroute

1. Requirements

Devices A, B, and C belong to the same OSPF area, and any two of them implement internetworking through the OSPF protocol. When a link of Device A fails, the service can be quickly switched to the backup link. The handover delay should be reduced as much as possible.

2. Topology

Figure 1-1 Topology for Fast Reroute



3. Notes

- Configure fast reroute on Device A.
- Configure **carrier-delay 0** on the interfaces on Device A.

4. Procedure

(1) Configure interface IP addresses for all devices (omitted).

(2) Configure OSPF basic functions on all devices (omitted).

(3) Configure fast reroute on Device A.

```
Device A> enable
Device A# configure terminal
Device A(config)# router ospf 1
Device A(config-router)# fast-reroute lfa
Device A(config-router)# exit
```

(4) Configure carrier-delay 0 on all the interfaces of Device A.

```
Device A(config)# interface GigabitEthernet 0/1
Device A(config-if-GigabitEthernet 0/1)# carrier-delay 0
Device A(config-if-GigabitEthernet 0/1)# exit
Device A(config)# interface GigabitEthernet 0/2
Device A(config-if-GigabitEthernet 0/2)# carrier-delay 0
```

5. Verification

On Device A, check the routing table to verify that a backup route exists for the entry 192.168.4.0/24.

```
Device A# show ip route fast-reroute  | begin 192.168.4.0
```

```
O  192.168.4.0/24 [ma] via 192.168.1.2, 00:39:28, GigabitEthernet 0/1
                   [b] via 192.168.2.2, 00:39:28, GigabitEthernet 0/2
```

6. Configuration Files

Device A configuration file

```
!
router ospf 1
fast-reroute lfa
!
interface GigabitEthernet 0/1
carrier-delay 0
!
interface GigabitEthernet 0/2
 carrier-delay 0
!
```

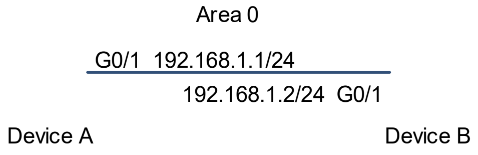
1.24.6 Configuring Network Management Functions

1. Requirements

Configure network management functions on Device A to realize information management interaction from the NMS to the agent through SNMP. The NMS server IP address is 192.168.2.2.

2. Topology

Figure 1-1 Topology of Network Management Functions



3. Notes

- Bind MIB to the OSPF process on Device A.
- Configure the trap function on Device A.

4. Procedure

(1) Configure interface IP addresses for all devices (omitted).

(2) Configure OSPF basic functions on all devices (omitted).

(3) Bind MIB to the OSPF process on Device A.

```
Device A> enable
Device A# configure terminal
Device A(config)# snmp-server host 192.168.2.2 traps version 2c public
Device A(config)# snmp-server community public rw
Device A(config)# snmp-server enable traps
```

(4) Configure the trap function in OSPF process 10.

```
Device A(config)# router ospf 10
Device A(config-router)# enable mib-binding
Device A(config-router)# enable traps
```

5. Verification

Verify the SNMP information before the trap function is configured for the OSPF process.

```
Device A# show snmp
Chassis: 60FF60
0 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  0 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
  0 Get-next PDUs
  0 Set-request PDUs
  0 Drop PDUs
  0 UDP parse errors
0 SNMP packets output
  0 Too big errors (Maximum packet size 1472)
  0 No such name errors
  0 Bad values errors
  0 General errors
  0 Response PDUs
  0 Trap PDUs
SNMP global trap: disabled
SNMP logging: disabled
SNMP trap logging: disabled
SNMP agent: enabled
SNMP v1:  enabled
SNMP v2c: enabled
SNMP v3:  enabled
```

Verify the SNMP information after the trap function is configured for the OSPF process.

```
Device A# show snmp
Chassis: 60FF60
0 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  8 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
  0 Get-next PDUs
  0 Set-request PDUs
  0 Drop PDUs
  0 UDP parse errors
2 SNMP packets output
  0 Too big errors (Maximum packet size 1472)
  0 No such name errors
  0 Bad values errors
  0 General errors
  0 Response PDUs
  2 Trap PDUs
```

6. Configuration Files

- Device A configuration file

```
!
snmp-server host 192.168.2.2 traps version 2c public
snmp-server community public rw
snmp-server enable traps
!
router ospf 10
enable mib-binding
enable traps
!
```

7. Common Errors

- Configurations on the SNMP server are incorrect. For example, the MIB or trap function is not enabled.

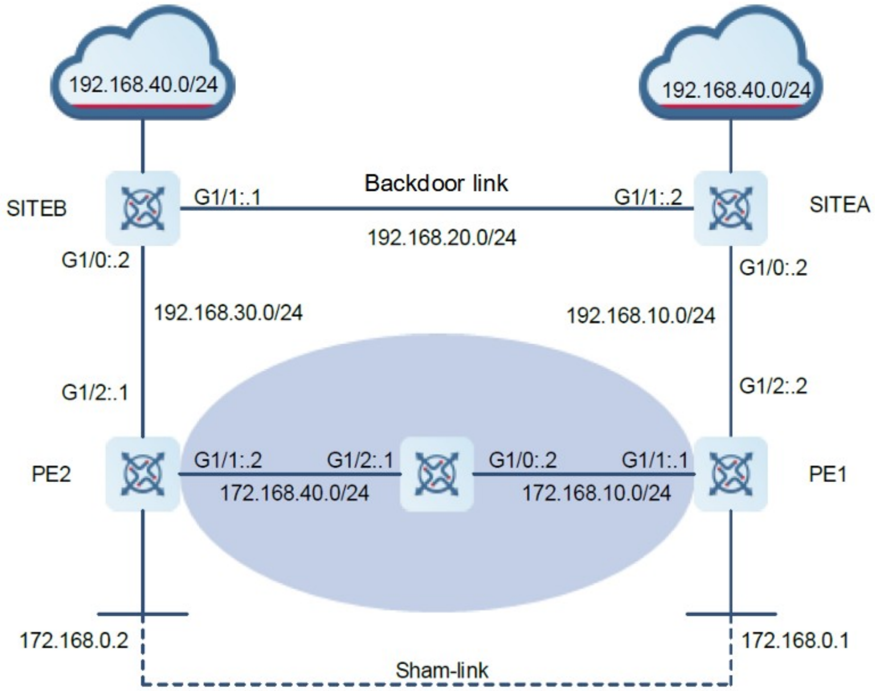
1.24.7 Configuring the Sham Link Function

1. Requirements

Two different sites of the client interact VPN routes through the MPLS backbone network. At the same time, a "backdoor link" is assumed between the two sites, and aims to ensure that, when the MPLS backbone network fails, information interaction between the two sites can be still implemented normally through this backup link.

2. Topology

Figure 1-1 Topology for Sham Link Function



3. Notes

- Configure on Site A to run the OSPF protocol with PE 1 and Site B, where the OSPF protocol runs with Site B through the backdoor link. Configure the OSPF cost for the interface.
- Configure on Site B to run the OSPF protocol with PE 2 and Site A, where the OSPF protocol runs with Site A through the backup link. Configure the OSPF cost for the interface.
- Configure a loopback interface on PE 1, create a VRF: VPN A, define the RD value and RT value, associate VRF with the corresponding interface, and associate the interface connecting to the CE with VRF; configure a loopback interface of VRF to establish a sham link, configure BGP, establish an MP-IBGP session with PE 2, implement route interaction with CE through the OSPF protocol, establish a sham link with the OSPF process on PE 2, configure MPLS signaling of the backbone network, enable the MPLS capability of public network interface, and configure the backbone network routing protocol.

- Configure a loopback interface on PE 2, create a VRF: VPN A, define the RD value and RT value, associate VRF with the corresponding interface, and associate the interface connecting to the CE with VRF; configure a loopback interface of VRF to establish a sham link, configure BGP, establish an MP-IBGP session with PE 1, implement VPN route interaction with CE through the OSPF protocol, and configure to establish a sham link with PE 1; configure MPLS signaling of the backbone network, enable the MPLS capability of public network interface, and configure the backbone network routing protocol.
- Configure backbone network MPLS signaling on P 1, enable the MPLS capability of interface, and configure the backbone network routing protocol.

4. Procedure

(1) Make configuration on Site A.

Configure an IP address for the interface.

```
SITEA> enable
SITEA# configure terminal
SITEA(config)# interface GigabitEthernet 1/0
SITEA(config-GigabitEthernet 1/0)# ip address 192.168.10.2 255.255.255.0
SITEA(config-GigabitEthernet 1/0)# ip ospf cost 1
SITEA(config-GigabitEthernet 1/0)# exit
SITEA(config)# interface GigabitEthernet 1/1
SITEA(config-GigabitEthernet 1/1)# ip address 192.168.20.1 255.255.255.0
SITEA(config-GigabitEthernet 1/1)# ip ospf cost 200
SITEA(config-GigabitEthernet 1/1)# exit
```

Advertise the interface network to the OSPF process.

```
SITEA(config)# router ospf 10
SITEA(config-router)# network 192.168.10.0 255.255.255.0 area 0
SITEA(config-router)# network 192.168.20.0 255.255.255.0 area 0
```

(2) Make configuration on Site B.

Configure an IP address for the interface.

```
SITEB> enable
SITEB# configure terminal
SITEB(config)# interface GigabitEthernet 1/0
SITEB(config-GigabitEthernet 1/0)# ip address 192.168.30.2 255.255.255.0
SITEB(config-GigabitEthernet 1/0)# ip ospf cost 1
SITEB(config-GigabitEthernet 1/0)# exit
SITEB(config)# interface GigabitEthernet 1/1
SITEB(config-GigabitEthernet 1/1)# ip address 192.168.20.2 255.255.255.0
SITEB(config-GigabitEthernet 1/1)# ip ospf cost 200
SITEB(config-GigabitEthernet 1/1)# exit
```

Advertise the interface network to the OSPF process.

```
SITEB(config)# router ospf 10
SITEB(config-router)# network 192.168.30.0 255.255.255.0 area 0
SITEB(config-router)# network 192.168.20.0 255.255.255.0 area 0
```

(3) Make configuration on PE 1.

Configure loopback interface 0.

```
PE1> enable
PE1# configure terminal
PE1(config)# interface loopback 0
PE1(config-Loopback 0)# ip address 172.168.0.1 255.255.255.255
PE1(config-Loopback 0)# exit
```

Create a VRF VPNA and define its RD and RT attribute values.

```
PE1(config)# ip vrf VPNA
PE1(config-vrf)# rd 1:100
PE1(config-vrf)# route-target both 1:100
PE1(config-vrf)# exit
```

Configure an interface IP address and associate VRF with the corresponding interface.

```
PE1(config)# interface GigabitEthernet 1/2
PE1(config-GigabitEthernet 1/2)# ip vrf forwarding VPNA
PE1(config-GigabitEthernet 1/2)# ip address 192.168.10.1 255.255.255.0
PE1(config-GigabitEthernet 1/2)# exit
PE1(config)# interface loopback 10
PE1(config-Loopback 10)# ip vrf forwarding VPNA
PE1(config-Loopback 10)# ip address 192.168.0.1 255.255.255.255
PE1(config-Loopback 10)# exit
```

Configure BGP and establish an MP-IBGP session with PE 2.

```
PE1(config)# router bgp 1
PE1(config-router)# neighbor 172.168.0.2 remote-as 1
PE1(config-router)# neighbor 172.168.0.2 update-source loopback 0
PE1(config-router)# address-family vpnv4
PE1(config-router-af)# neighbor 172.168.0.2 activate
PE1(config-router-af)# exit
PE1(config-router)# exit
```

Configure to establish a sham link with the OSPF process on PE 2.

```
PE1(config)# router ospf 10 vrf VPNA
PE1(config-router)# network 192.168.10.0 255.255.255.0 area 0
PE1(config-router)# redistribute bgp subnets
PE1(config-router)# area 0 sham-link 192.168.0.1 192.168.0.2
PE1(config-router)# exit
```

Configure OSPF and direct route redistribution by BGP.

```
PE1(config)# router bgp 1
PE1(config-router)# address-family ipv4 vrf VPNA
PE1(config-router-af)# redistribute ospf 10
PE1(config-router-af)# redistribute connected
PE1(config-router-af)# exit
PE1(config-router)# exit
```

Configure backbone network MPLS signaling, and enable the MPLS capability of public network interface.

```
PE1(config)# mpls ip
PE1(config)# mpls router ldp
PE1(config-mpls-router)# ldp router-id interface loopback 0 force
PE1(config-mpls-router)# exit
PE1(config)# interface GigabitEthernet 1/1
PE1(config-GigabitEthernet 1/1)# ip address 172.168.10.1 255.255.255.0
PE1(config-GigabitEthernet 1/1)# label-switching
PE1(config-GigabitEthernet 1/1)# mpls ip
PE1(config-GigabitEthernet 1/1)# exit
```

Advertise the interface network to the OSPF process.

```
PE1(config)# router ospf 1
PE1(config-router)# network 172.168.10.0 0.0.0.255 area 0
PE1(config-router)# network 172.168.0.1 0.0.0.0 area 0
```

(4) Make configuration on PE 2

Configure loopback interface 0.

```
PE2> enable
PE2# configure terminal
PE2(config)# interface loopback 0
PE2(config-Loopback 0)# ip address 172.168.0.2 255.255.255.255
PE2(config-Loopback 0)# exit
```

Create a VRF VPNA and define its RD and RT attribute values.

```
PE2(config)# ip vrf VPNA
PE2(config-vrf)# rd 1:100
PE2(config-vrf)# route-target both 1:100
PE2(config-vrf)# exit
```

Configure an interface IP address and associate VRF with the corresponding interface.

```
PE2(config)# interface GigabitEthernet 1/2
PE2(config-GigabitEthernet 1/2)# ip vrf forwarding VPNA
PE2(config-GigabitEthernet 1/2)# ip address 192.168.30.1 255.255.255.0
PE2(config-GigabitEthernet 1/2)# exit
PE2(config)# interface loopback 10
PE2(config-Loopback 10)# ip vrf forwarding VPNA
```

```
PE2(config-Loopback 10)# ip address 192.168.0.2 255.255.255.255
PE2(config-Loopback 10)# exit
```

Configure BGP and establish an MP-IBGP session with PE 2.

```
PE2(config)# router bgp 1
PE2(config-router)# neighbor 172.168.0.1 remote-as 1
PE2(config-router)# neighbor 172.168.0.1 update-source loopback 0
PE2(config-router)# address-family vpnv4
PE2(config-router-af)# neighbor 172.168.0.1 activate
PE2(config-router-af)# exit
PE2(config-router)# exit
```

Configure to establish a sham link with the OSPF process on PE 2.

```
PE2(config)# router ospf 10 vrf VPNA
PE2(config-router)# network 192.168.30.0 255.255.255.0 area 0
PE2(config-router)# redistribute bgp subnets
PE2(config-router)# area 0 sham-link 192.168.0.2 192.168.0.1
PE2(config-router)# exit
```

Configure OSPF and direct route redistribution by BGP.

```
PE2(config)# router bgp 1
PE2(config-router)# address-family ipv4 vrf VPNA
PE2(config-router-af)# redistribute ospf 10
PE2(config-router-af)# redistribute connected
PE2(config-router-af)# exit
```

Configure backbone network MPLS signaling, and enable the MPLS capability of public network interface.

```
PE2(config)# mpls ip
PE2(config)# mpls router ldp
PE2(config-mpls-router)# ldp router-id interface loopback 0 force
PE2(config-mpls-router)# exit
PE2(config)# interface GigabitEthernet 1/1
PE2(config-GigabitEthernet 1/1)# ip address 172.168.40.2 255.255.255.0
PE2(config-GigabitEthernet 1/1)# label-switching
PE2(config-GigabitEthernet 1/1)# mpls ip
PE2(config-GigabitEthernet 1/1)# exit
```

Advertise the interface network to the OSPF process.

```
PE2(config)# router ospf 1
PE2(config-router)# network 172.168.40.0 0.0.0.255 area 0
PE2(config-router)# network 172.168.0.2 0.0.0.0 area 0
```

(5) Make configuration on P 1.

Configure loopback interface 0 on P 1.

```
P1> enable
```

```
P1# configure terminal
P1(config)# interface loopback 0
P1(config-Loopback 0)# ip address 172.168.0.3 255.255.255.255
P1(config-Loopback 0)# exit
```

Make basic configuration of OSPF.

```
P1(config)# router ospf 1
P1(config-router)# network 172.168.40.0 0.0.0.255 area 0
P1(config-router)# network 172.168.10.0 0.0.0.255 area 0
P1(config-router)# network 172.168.0.3 0.0.0.0 area 0
P1(config-router)# exit
```

Configure backbone network MPLS signaling on P 1, and enable the MPLS capability of interface.

```
P1(config)# interface GigabitEthernet 1/0
P1(config-GigabitEthernet 1/0)# ip address 172.168.10.2 255.255.255.0
P1(config-GigabitEthernet 1/0)# mpls ip
P1(config-GigabitEthernet 1/0)# label-switch
P1(config-GigabitEthernet 1/0)# exit
P1(config)# interface GigabitEthernet 1/1
P1(config-GigabitEthernet 1/1)# ip address 172.168.40.1 255.255.255.0
P1(config-GigabitEthernet 1/1)# mpls ip
P1(config-GigabitEthernet 1/1)# label-switch
P1(config-GigabitEthernet 1/1)# exit
P1(config)# mpls ip
P1(config)# mpls router ldp
PE2(config-mpls-router)# ldp router-id interface loopback 0 force
PE2(config-mpls-router)# exit
```

5. Verification

(1) Verify the configuration on PE 1.

Verify that an OSPF sham link route exists on PE 1.

```
PE1# show ip ospf 10 sham-links
Sham Link SLINK0 to address 192.168.0.2 is up
  Area 0.0.0.0 source address 192.168.0.1, Cost: 1
  Output interface is GigabitEthernet 1/1
  Nexthop address 172.16.40.2
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
    Adjacency state Full
```

Check the OSPF neighbor of PE 1.

```
PE1# show ip ospf 10 neighbor
```

```

OSPF process 10, 1 Neighbors, 1 is Full:
Neighbor ID     Pri   State               BFD State  Dead Time   Address
Interface
192.168.0.2        1   Full/ -              -          00:00:34    192.168.0.2
SLINK0
```

Check the VRF route of PE 1.

```
PE1# show ip route vrf VPNA
Routing Table: VPNA

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C       192.168.10.0/24 is directly connected, GigabitEthernet 1/2
O       192.168.20.0/24 [110/101] via 192.168.1.2, 00:56:23, GigabitEthernet 1/2
O       192.168.30.0/24 [110/2] via 172.168.0.2, 00:00:36
O       192.168.40.0/24 [110/2] via 172.168.0.2, 00:00:36
```

(2) Verify the configuration on PE 2.

Verify that an OSPF sham link route exists on PE 2.

```
PE2# show ip ospf 10 sham-links
Sham Link SLINK0 to address 192.168.0.1 is up
  Area 0.0.0.0 source address 192.168.0.2, Cost: 1
  Output interface is GigabitEthernet 1/1
  Nexthop address 172.16.10.1
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
    Adjacency state Full
```

Check the OSPF neighbor of PE 2.

```
PE2# show ip ospf 10 neighbor

OSPF process 10, 1 Neighbors, 1 is Full:
Neighbor ID     Pri   State               BFD State  Dead Time   Address
Interface
```

```
192.168.0.1        1   Full/ -              -          00:00:34    192.168.0.1
SLINK0
```

Check the VRF route of PE 2.

```
PE2# show ip route vrf VPNA
Routing Table: VPNA

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
O       192.168.10.0/24 [110/2] via 172.168.0.1, 00:00:36
O       192.168.20.0/24 [110/2] via 172.168.0.1, 00:00:36
C       192.168.30.0/24 is directly connected, GigabitEthernet 1/2
O       192.168.40.0/24 [110/101] via 192.168.30.2, 00:56:23, GigabitEthernet
1/2
```

6. Configuration Files

- Site A configuration file

```
!
interface GigabitEthernet 1/0
 ip address 192.168.10.2 255.255.255.0
 ip ospf cost 1
!
interface GigabitEthernet 1/1
 ip address 192.168.20.1 255.255.255.0
 ip ospf cost 200
!
router ospf 10
 network 192.168.10.0 255.255.255.0 area 0
 network 192.168.20.0 255.255.255.0 area 0
!
```

- Site B configuration file

```
!
interface GigabitEthernet 1/0
 ip address 192.168.30.2 255.255.255.0
 ip ospf cost 1
```

```
!
interface GigabitEthernet 1/1
 ip address 192.168.20.2 255.255.255.0
 ip ospf cost 200
!
router ospf 10
 network 192.168.30.0 255.255.255.0 area 0
 network 192.168.20.0 255.255.255.0 area 0
!
```

- PE 1 configuration file

```
!
ip vrf VPNA
 rd 1:100
 route-target both 1:100
!
interface GigabitEthernet 1/1
 ip address 172.168.10.1 255.255.255.0
 label-switching
 mpls ip
!
interface GigabitEthernet 1/2
 ip vrf forwarding VPNA
 ip address 192.168.10.1 255.255.255.0
interface loopback 0
 ip address 172.168.0.1 255.255.255.255
!
interface loopback 10
 ip vrf forwarding VPNA
 ip address 192.168.0.1 255.255.255.255
!
router bgp 1
 neighbor 172.168.0.2 remote-as 1
 neighbor 172.168.0.2 update-source loopback 0
 address-family vpnv4
  neighbor 172.168.0.2 activate
 address-family ipv4 vrf VPNA
  redistribute ospf 10
  redistribute connected
!
router ospf 1
 network 172.168.10.0 0.0.0.255 area 0
 network 172.168.0.1 0.0.0.0 area 0
```

```
!
router ospf 10 vrf VPNA
 network 192.168.10.0 255.255.255.0 area 0
 redistribute bgp subnets
 area 0 sham-link 192.168.0.1 192.168.0.2
!
mpls ip
mpls router ldp
 ldp router-id interface loopback 0 force
!
```

- PE 2 configuration file

```
!
ip vrf VPNA
 rd 1:100
 route-target both 1:100
!
interface GigabitEthernet 1/1
 ip address 172.168.40.2 255.255.255.0
 label-switching
 mpls ip
!
interface GigabitEthernet 1/2
 ip vrf forwarding VPNA
 ip address 192.168.30.1 255.255.255.0
!
interface loopback 0
 ip address 172.168.0.2 255.255.255.255
!
interface loopback 10
 ip vrf forwarding VPNA
 ip address 192.168.0.2 255.255.255.255
!
router bgp 1
 neighbor 172.168.0.1 remote-as 1
 neighbor 172.168.0.1 update-source loopback 0
 address-family vpnv4
  neighbor 172.168.0.1 activate
 address-family ipv4 vrf VPNA
  redistribute ospf 10
  redistribute connected
!
router ospf 1
```

```
 network 172.168.40.0 0.0.0.255 area 0
 network 172.168.0.2 0.0.0.0 area 0
!
router ospf 10 vrf VPNA
 network 192.168.30.0 255.255.255.0 area 0
 redistribute bgp subnets
 area 0 sham-link 192.168.0.2 192.168.0.1
!
mpls ip
mpls router ldp
 ldp router-id interface loopback 0 force
!
```

- P 1 configuration file

```
!
interface GigabitEthernet 1/0
 ip address 172.168.10.2 255.255.255.0
 mpls ip
 label-switch
!
interface GigabitEthernet 1/1
 ip address 172.168.40.1 255.255.255.0
 mpls ip
 label-switch
!
interface loopback 0
 ip address 172.168.0.3 255.255.255.255
!
router ospf 1
 network 172.168.40.0 0.0.0.255 area 0
 network 172.168.10.0 0.0.0.255 area 0
 network 172.168.0.3 0.0.0.0 area 0
!
mpls ip
mpls router ldp
 ldp router-id interface loopback 0 force
!
```

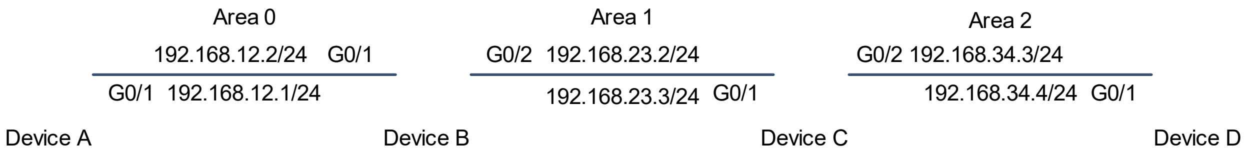
1.24.8 Configuring a Virtual Link

1. Requirements

Area 2 is not directly connected to Area 0. To ensure the normal operation of OSPF on the network, a virtual link is configured between Device B and Device C.

2. Topology

Figure 1-1 Topology for Configuring a Virtual Link



3. Notes

- Configure interface IP addresses for all devices (omitted).
- Configure OSPF basic functions on all devices (omitted).
- Configure a virtual link on Devices B and C.

4. Procedure

(1) Configure an IP address for each interface and the OSPF routing protocol (omitted).

(2) Configure a virtual link on Devices B and C.

Configure Device B.

```
Device B> enable
Device B# configure terminal
Device B(config)# router ospf 1
Device B(config-router)# area 1 virtual-link 192.168.23.3
```

Configure Device C.

```
Device C> enable
Device C# configure terminal
Device C(config)# router ospf 1
Device C(config-router)# area 1 virtual-link 192.168.12.2
```

5. Verification

Verify that the route of Area 2 can be learned by running the **show ip ospf database** command on Device A.

```
Device A# show ip ospf database
            OSPF Router with ID (192.168.12.1) (Process ID 1)
                Router Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum Link count
192.168.12.1    192.168.12.1    1025        0x80000002 0x00292E 1
192.168.12.2    192.168.12.2    3           0x80000004 0x00DA5E 2
192.168.23.3    192.168.23.3    7     (DNA) 0x80000001 0x001328 0
```

```
                Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
192.168.12.2    192.168.12.2    1031        0x80000001 0x00CE8E
                Summary Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
192.168.23.0    192.168.12.2    820         0x80000001 0x0077CC
192.168.23.0    192.168.23.3    7     (DNA) 0x80000001 0x002414
192.168.34.0    192.168.23.3    7     (DNA) 0x80000001 0x00AA82
```

6. Configuration Files

- Device B configuration file

```
!
router ospf 1
area 1 virtual-link 192.168.23.3
!
```

- Device C configuration file

```
!
router ospf 1
 area 1 virtual-link 192.168.12.2
!
```

1.24.9 Selecting a DR of OSPF

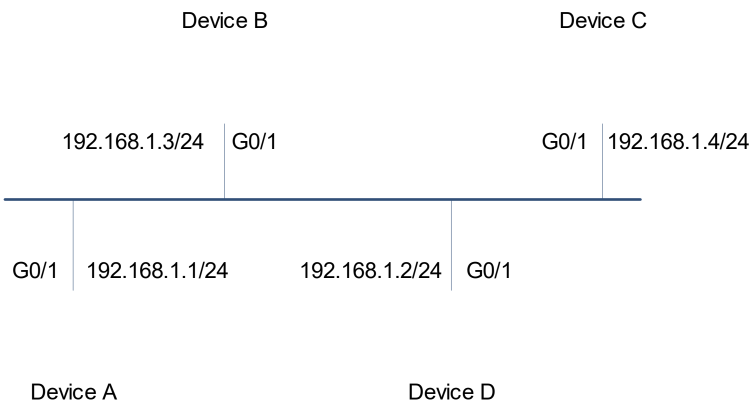
1. Requirements

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

Configure the priority of Device A as 10 to turn it into a DR, and the priority of Device B as 5 to turn it into a BDR, set the default priority for Device C, and set the priority of Device D to 0 to avoid participating in DR election.

2. Topology

Figure 1-1 Topology for Selecting a DR



3. Notes

Set the priorities to 10, 5, and 0 on Devices A, B, and D respectively.

4. Procedure

(1) Configure an IP address for each interface and the OSPF routing protocol (omitted).

(2) Set the priorities on Devices A, B, and D.

Configure Device A.

```
Device A> enable
Device A# configure terminal
Device A(config)# interface GigabitEthernet 0/1
Device A(config-if-GigabitEthernet 0/1)# ip ospf priority 10
```

Configure Device B.

```
Device B> enable
Device B# configure terminal
Device B(config)# interface GigabitEthernet 0/1
Device B(config-if-GigabitEthernet 0/1)# ip ospf priority 5
```

Configure Device D.

```
Device D> enable
Device D# configure terminal
Device D(config)# interface GigabitEthernet 0/1
Device D(config-if-GigabitEthernet 0/1)# ip ospf priority 0
```

5. Verification

Verify that the displayed neighbor is correct when the **show ip ospf neighbor** command is run on Device D.

```
Device D# show ip ospf neighbor
Neighbor ID     Pri   State            Dead Time   Address         Interface
192.168.1.1      10   FULL/DR         00:00:38    192.168.1.1    GigabitEthernet0/1
192.168.1.2      5   FULL/BDR         00:00:30    192.168.1.2    GigabitEthernet0/1
```

6. Configuration Files

- Device A configuration file

```
!
interface GigabitEthernet 0/1
ip ospf priority 10
!
```

- Device B configuration file

```
!
interface GigabitEthernet 0/1
ip ospf priority 5
!
```

- Device D configuration file

```
!
interface GigabitEthernet 0/1
ip ospf priority 0
!
```