Contents

1 Configuring IS-IS

1.1 Overview

1.1.1 Overview

Intermediate System to Intermediate System (IS-IS) is an extensible, robust, and easy-to-use Interior Gateway Protocol (IGP) for route selection and applicable to an IP and ISO (connectionless network service) CLNS dual environment network.

IS-IS was designed for the Connection-Less Network Protocol (CLNP) at the very start. After TCP/IP became mainstream protocols, IETF modified IS-IS so that this protocol could apply to TCP/IP environment. The modified IS-IS is referred to as Integrated IS-IS or Dual IS-IS.

IS-IS has the common characteristics of a link state protocol. It sends Hello packets to discover and maintain neighbor relationships, and sends Link State Protocol Data Units (LSPs) to neighbors to advertise its link state. IS-IS supports Level-1 routing and Level-2 routing. All devices at the same level maintain the same link state database (LSDB), which stores the LSPs generated by the devices to notify each other of the network topology at this level. Each device uses the Dijkstra shortest path first (SPF) algorithm to perform best-route computation, path selection, and fast convergence.

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. Basic Concepts

- IS-IS network hierarchy

  As shown in Figure 1-1, an IS-IS network is divided into Level-1 and Level-2. The nodes on which devices exchange information in the same area form one level (Level-1).

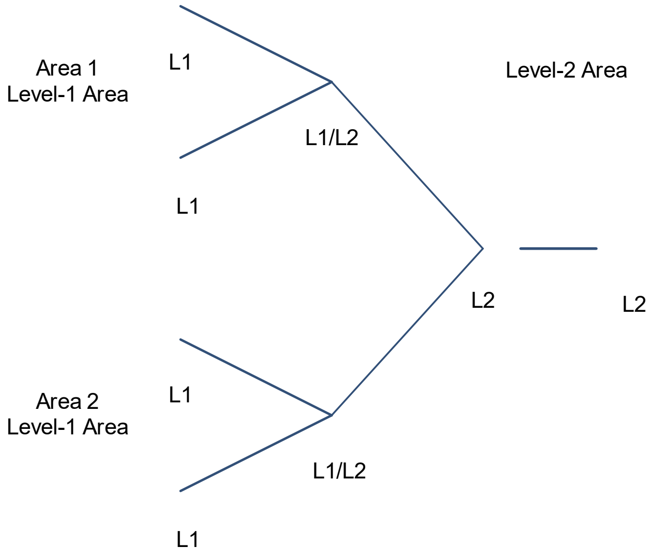
  - Level-1 routers perform routing in the local area and they can form neighbor relationship with local Level-1 routers and Level-1/Level-2 routers and maintain Level-1 LSDB. This LSDB includes routing information of local area and packets destined for another area are forwarded to the closest Level-1/Level-2 router.
  - Level-2 routers perform inter-area routing and they can form neighbor relationship with Level-2 routers in the same area or another area and Level-1/Level-2 routers and maintain Level-2 LSDB. This LSDB includes inter-area routing information. All Level-2 routers and Level-1/Level-2 routers form a backbone network of a routing domain and take charge of communication between different areas. The backbone network must be physically connected. Only Level-2 routers can exchange data packets and routing information with routers outside the routing domain.
  - Level-1/Level-2 routers, belonging to Level-1 and Level-2 areas, can form Level-1 neighbor relationship

with Level-1 routers in the same area and Level-1/Level-2 routers and form Level-2 neighbor relationship with Level-2 routers in the same or another area and Level-1/Level-2 routers. Level-1 routers must be connected to another area through Level-1/Level-2 routers. Level-1/Level-2 routers maintain two LSDBs. Level-1 LSDB is used for internal routing, and Level-2 LSDB is used for inter-area routing. By default, Level-1/Level-2 routers redistribute Level-1 routes to Level-2 routers. If there are many Level-1 routes, the routes must be summarized and then redistributed to Level-2 routers.

All devices in an area know the network topology of the area and exchange data within the area. Level-1/Level-2 devices are border devices that belong to different areas and provide inter-area connections. Areas are connected by Level-2 devices. The border devices in various areas form a Level-2 backbone network for inter-area data exchange.

Level-1 devices are only interested in the local area's topology, including all nodes in the local area and the next-hop devices destined for the nodes. Level-1 devices access other areas through Level-2 devices and forward packets from a target network outside the local area to the closest Level-2 device.

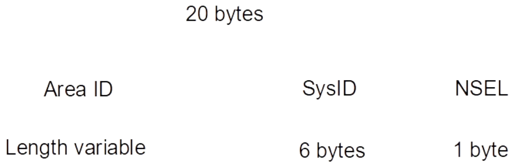
Figure 1-1IS-IS Network Architecture



- IS-IS address coding mode

An IS-IS address is called a network entity title (NET) and it consists of an area ID, a system ID, and a network service access point (NSAP) ID. An IS-IS address ranges from 8 to 20 bytes.

Figure 1-2NET Address Format



- ○ The area ID identifies the routing domain length in an area and is fixed relative to the routing domain. It ranges from 1 to 13 bytes.

  The area ID consists of an authority and format identifier (AFI), an initial domain identifier (IDI), and a high order DSP (HODSP). The AFI represents an address assignment authority and address format, the IDI is used to identify a domain, and the HODSP is used to distinguish areas.

- ○ The system ID is unique in an autonomous system (AS).

  Generally, a router ID (for example, 192.168.10.1) is translated to a system ID by extending each decimal in an IP address to three decimals. For if the decimals are less than three, 0 is added for supplementation. An extended IP address is 192.168.010.001. After the extended IP address is divided into three parts, the system ID is 1921.6801.0001.

- ○ The NSAP is a network selector and sometimes called SEL. In IS-IS, SEL is typically set to 00 to indicate a device.

- IS-IS packet types

  There are three types of IS-IS packets:

- ○ LSPs

  LSPs are used to transmit link state records within an area and are classified into Level-1 LSPs and Level-2 LSPs. LSPs are only flooded at the local level.

- ○ IS-to-IS Hello (IIH) PDUs

  IIH PDUs are used to maintain adjacency. They carry multicast MAC addresses used to determine whether other systems run IS-IS.

- ○ Sequence number PDUs (SNPs), including complete SNP (CSNP) and partial SNP (PSNP)

  CSNPs are used for LSDB synchronization. By default, a designated IS (DIS) sends a CSNP every 10s in a broadcast network. In a P2P network, a CSNP is sent only after a neighbor relationship is established.

  PSNPs are also used for LSDB synchronization.

- IS-IS supported type-length-value (TLV) types

  IS-IS supports 26 types of TLV.

  Table 1 lists IS-IS supported TLV types.

Table 1-1IS-IS Supported TLV Types

TLV Code	Description
Code=1	Area address
Code=2	Priority of an IS-IS neighbor
Code =3	ES neighbor
Code=6	MAC address of an IS-S neighbor
Code=8	Padded field
Code=9	LSP entity

TLV Code	Description
Code=10	Verification field
Code=14	Size of the source LSP buffer
Code=22	Extended IS reachability
Code=128	IP internal reachability information
Code=129	Supported protocol
Code =130	IP external reachability information
Code=131	Inter-domain routing protocol information
Code=132	IP interface address
Code=133	Verification information
Code=135	Extended IP reachability TLV
Code=137	Dynamic host name
Code = 211	Graceful Restart
Code = 222	MT IS TLV
Code = 229	Multi Topology TLV
Code=232	IPv6 interface
Code = 235	IPv4 MT IP reachability TLV
Code =236	IPv6 IP reachability TLV
Code = 237	IPv6 MT IP reachability TLV
Code =240	P2P three-way handshake TLV

- IS-IS supported network types

  IS-IS supported network types include P2P links and broadcast links.

2. Working Process of IS-IS

IS-IS working process consists of neighbor establishment, LSDB synchronization, and route computation. In a broadcast network, neighbor establishment involves DIS election.

- Neighbor establishment

  The IS-IS neighbor establishment procedure is similar to the OSPF neighbor establishment procedure. If the received hello packets do not contain any information, the neighbor state is reset to Initial. If the neighbor field in the received packets indicates the local MAC address, the neighbor state is Up. If the neighbor state of the local router and peer routers is Up, the neighbor relationship is successfully established.

- DIS election

  A DIS in a broadcast network works like a DR in OSPF.

  A pseudonode is generated by a DIS and sets up a relationship with each device in the local network.

  Like DR election in OSPF, a DIS is elected to reduce unnecessary neighbor relationships and route information exchanges. After neighbor establishment, the DIS election starts at respective levels of areas. The election priority also changes with the levels of areas.

  A DIS simulates multiple access links as a pseudonode and generates LSPs for the pseudonode. The pseudonode sets up a relationship with each device in the local network and forbids direct communication between the devices. A broadcast subnet and a non-broadcast multiple access (NBMA) network are considered as pseudonodes externally. Non-DIS devices report local link states to the DIS in the same network, and the DIS reports the link states on behalf of all the IS devices in the network.

  DIS election in IS-IS is preemptive. The election result can be manually controlled through interface priority configuration. The device with a higher interface priority is more likely to be elected as the DIS. A device with the priority 0 participates in DIS election as well.

- LSDB synchronization

  All devices running link state routing protocols send local link state and directly-connected network link state to neighbors. Upon receiving the link information, the neighbors record and forward the information to their neighbors. After link state update is completed, all routers obtain topological information of the entire network. This is referred to as LSDB flooding synchronization.

  Many neighbor actions such as neighbor or neighbor interface up/down, metric change, redistributed route change and periodic change, trigger LSDB synchronization.

  A router processes a received LSP as follows:

a The router searches for this LSP in the LSDB. If the LSP does not exist in the LSDB, the router records this packet in the LSDB and broadcasts it for synchronization.

b If the sequence number of this LSP is greater than that of the local LSP, the router updates the LSDB and broadcasts it for synchronization.

c If the sequence number of this LSP is smaller than that of the local DPS, the router replies to the local LSP.

- Route computation

  After the LSDB is synchronized, IS-IS computes the SPF and generates IS-IS routes based on the SPF.

  In the LSP sent by the Level-1/Level-2 routers, ATT is set to 1. A Level-1 router gets to know the closest Level-1/Level-2 router based on the ATT and route computation result, and considers the Level-1/Level-2 router a routing transit to other areas.

3. IS-IS Route Control

- Route redistribution

  IS-IS can introduce routes of other routing protocols and routes of other IS-IS processes to the IS-IS process and mutually introduce routes between Level-1 and Level-2 areas.

  In IS-IS, a Level-2 area does not synchronize the known routing information of the backbone areas and other Level-1 areas to a Level-1 area. The Level-2 area cannot obtain external routing information outside Level-1 area. During routing, secondary routes may be generated. During route redistribution, routes of other Level-1 areas and backbone areas that meet conditions can be introduced to the local Level-1 area based on the routing policy.

- Route summarization

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

- Load balancing

  If multiple equal-cost routes exist in a network, IS-IS can distribute load to the equal-cost routes to improve link usage.

4. IS-IS Wide Metric

The default metric type of IS-IS is narrow. In narrow mode, the maximum metric value of an interface is **63**. In a large network, the metric value range in narrow mode is not wide enough. Therefore, wide metric is developed. The metric value can reach 16777215.

5. LSP Fragment Extension

IS-IS advertises link state information by flooding LSPs. The size of an LSP is limited by the MTU size of the link. When the content to be advertised exceeds one LSP, IS-IS will create LSP fragments to carry new link state information. Based on ISO, an LSP fragment is indicated by an LSP number that is one byte long. Therefore, an IS-IS device can generate a maximum of 256 LSP fragments.

The 256 LSP fragments are insufficient in any of the following situations:

(1) New applications (such as traffic engineering) extend new TLV or sub-TLV.

(2) The network is expanded continuously.

(3) Routes with reduced granularity are advertised, or other routes are redistributed to IS-IS.

After LSP fragments are used up, new routing information and neighbor information will be discarded, causing network exceptions such as routing black holes or loops. To ensure normal network operation, LSP fragments must be extended to carry more link state information.

By configuration of an additional system ID and an fragment extension switch, IS-IS can advertise more link state information in extended LSP fragments. Each virtual system can be considered as a virtual device that establishes a neighbor relationship (with the path value 0) with the originating system. Extended LSPs are advertised by the neighbor of the originating system, that is, the virtual system.

The following terms are related to fragment extension:

- Normal system ID

  The system ID defined by ISO is used to establish neighbor relationships and learn routes. It is further defined as the normal system ID in order to be distinguished from the additional system ID introduced to fragment extension.

- Additional system ID

  The additional system ID is configured by an administrator to generate extended LSPs. The additional system ID shares the usage rules of the normal system ID (for example, the additional system ID must be unique in the entire area), except that the additional system ID is not carried in Hello packets for neighbor relationship establishment.

- Originating system

  An originating system is an IS-IS-enabled device and maps to a virtual system identified by the additional system ID.

- Virtual system

  A virtual system is identified by the additional system ID and used to generate extended LSPs. The concept of virtual system is proposed by RFC for distinguishing from the concept of originating system. Each virtual system can generate up to 256 LSP fragments. The administrator can configure multiple additional system IDs (virtual systems) to generate more LSP fragments.

- Original LSP

  An original LSP is the LSP whose system ID contained in the LSP ID is a normal system ID. Original LSPs are generated by an originating system.

- Extended LSP

  An extended LSP is the LSP whose system ID contained in the LSP ID is an additional system ID. Extended LSPs are generated by a virtual system.

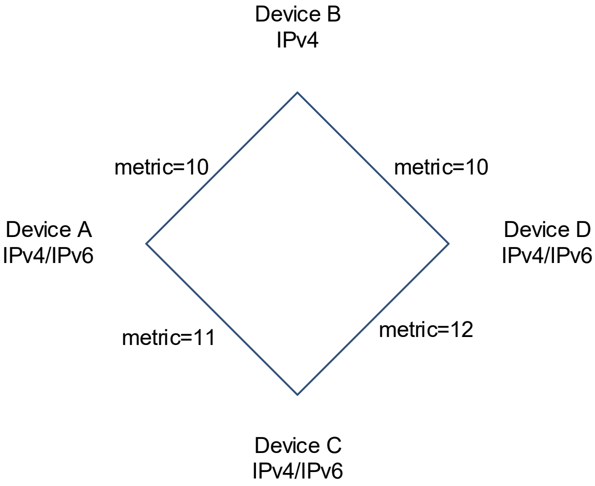
6. IS-IS MTR

IS-IS multi-topology routing (MTR) is an extended feature used to separate IPv4 unicast route computation from IPv6 unicast route computation based on topologies. New TLV types introduced to IIH packets and LSP packets of IS-IS to transmit IPv6 unicast topology information. One physical network can be divided into an IPv4 unicast logical topology and an IPv6 unicast logical topology. The two topologies perform SPF computation separately and maintain respective independent IPv4 and IPv6 unicast routing tables. In this way, IPv4 unicast service traffic and IPv6 unicast service traffic are forwarded by different paths. The IS-IS MTR technique helps users deploy IPv6 unicast networks without the constraint on consistency between IPv4 and IPv6 unicast topology information.

IS-IS MTR is derived from IS-IS MT, which is used to separate IPv4 unicast topology from IPv6 unicast topology, unicast topology from multicast topology, and topologies using different protocol stacks (such as IPv4 and Pv6). IS-IS MTR separates IPv4 unicast topology from IPv6 unicast topology based on IS-IS MT.

Figure 1-1 shows a typical networking application with the following implementation requirements: Deploy an IPv6 unicast topology in incremental mode and upgrade some devices to support IPv4 and IPv6 dual protocol stacks while keeping other IPv4-enabled devices unchanged.

Figure 1-1Physical Topology for IPv4/IPv6 Hybrid Deployment



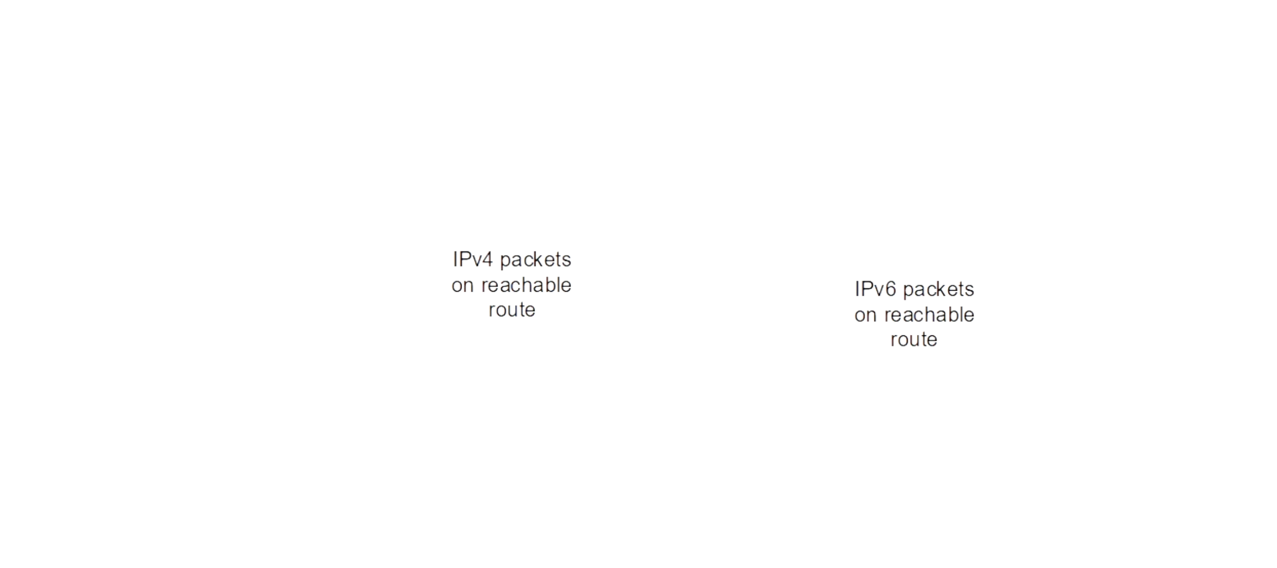
As shown in Figure 1-1, each link is marked by a number indicating its metric. Device B only supports the IPv4 protocol stack, whereas other devices support IPv4 and IPv6 dual protocol stacks.

The networking constraint on consistency between IPv4 and IPv6 unicast topologies must be removed to retain the use of Device B (supporting IPv4) so that Device B can establish a neighbor relationship with Device A or D. This, however, may cause new problems.

Figure 1-2IPv4/IPv6 Hybrid Topology

As shown in Figure 1-2, without IS-IS MTR, SPF computation performed by Devices A, B, C, and D only take into account the single hybrid topology. The calculated shortest path is Device A -> Device B -> Device D, with the cost 20. Device B will discard IPv6 packets because it does not support IPv6.

Figure 1-3Separation of IPv4 and IPv6 Topologies



As shown in Figure 1-3, after the IS-IS MTR technique is used to separate IPv4 unicast topology from IPv6 unicast topology, Devices A, B, C, and D establish neighbor relationships based on the IPv4 and IPv6 unicast topologies. The left part shows the IPv4 topology formed by IPv4-enabled routers. The calculated IPv4 shortest path is Device A -> Device B -> Device C, which realizes IPv4 packet forwarding. The right part shows the IPv6 topology formed by IPv6-enabled routers. The calculated IPv6 shortest path is Device A -> Device C -> Device D, which realizes IPv6 packet forwarding.

General IS-IS MTR deployment: IS-IS MTR must be deployed to avoid routing black holes when some devices support only one protocol. IS-IS MTR is not required when all devices support IPv4 and IPv6 dual protocol stacks.

Deployment of a new network: IS-IS MTR is not required when devices only support the IPv4 protocol stack. For devices that only support the IPv6 protocol stack or devices that support IPv4 and IPv6 dual protocol stacks, enable the MT mode of IS-IS MTR. You are not advised to enable Multi-Topology Transition (MTT) because loops may occur.

Reconstruction of an existing network with devices supporting only one protocol stack: Enable the MTT mode of IS-IS MTR on devices that support IPv4 and IPv6 dual protocol stacks in sequence (starting from the device closest to a device supporting only one protocol stack in the network topology). After the MTT mode is enabled on all new devices, switch the MTT mode to the MT mode on these devices in sequence (starting from the device farthest from a device supporting only one protocol stack in the network topology).

7. IS-IS Neighbor

In a broadcast network, neighbors elect a DIS and routers send routing information to the DIS.

On a P2P link, neighbor relationship can be established in two ways:

- Two-way handshake

  As long as an IIH packet is received, neighbor relationship is established. This method comes with low reliability.

- Three-way handshake

Neighbor relationship can be established after the IIH packet is sent three times. This method boasts high reliability.

In a link with one down end, if a neighbor relationship is established based on the IIH packet received from the peer device, the established neighbor relationship is abnormal. In a three-way handshake, an acknowledgment packet must be received from the peer device to confirm that the peer device has received the IIH packet before the neighbor relationship is established.

The following conditions must be met for two routing devices to establish a neighbor relationship when IS-IS MTR is not configured:

- The interface addresses on both routing devices are in the same network segment.
- The interface levels on both routing devices match.
- The routing devices are authenticated by each other.
- The routing devices support the same protocol.

The following conditions must be met for two routing devices to establish a neighbor relationship when IS-IS MTR is configured:

- The interface addresses on both routing devices are in the same network segment.
- The interface levels on both routing devices match.
- The routing devices are authenticated by each other.
- The routing devices have at least one consistent MT ID when P2P links are configured.
- There are no constraints on the MT IDs that the routing devices support when LAN links are configured.

8. IS-IS Authentication

Internet requirements for information security increase. To avoid data theft and tampering, operators apply the IS-IS authentication function on specified areas or interfaces to ensure data security.

- IS-IS authentication types

  Classification based on packet types:

  - Interface authentication: Authenticate Level-1 and Level-2 hello packets.
  - Area authentication: Authenticate Level-1 CSNP, PSNP, and LSP packets.
  - Routing domain authentication: Authenticate Level-2 CSNP, PSNP, and LSP packets.

  Classification based on authentication mode:

  - Simple authentication: Add a configured password to a packet. This authentication mode comes with low security.
  - MD5 authentication: A password is encrypted using MD5 algorithms and then added to a packet.
  - Keychain authentication: A keychain is configured so that the password changes with time.

- Implementation procedure

Upon receiving an IS-IS packet from another router, the local router checks whether the authentication password is correct. If not, the packet is discarded. The IS-IS packet carries authentication information by means of TLV. The TLV format is as follows:

- ○ Type: Indicates an authentication packet type. For TCP/IP packets, this value is 133.
- ○ Length: Indicates the length of a TLV.
- ○ Value: Indicates an authentication type and password.

Interface authentication: Indicates that authentication is configured in interface configuration mode. Interconnected router interfaces must be configured with the same password.

Area authentication: Indicates that authentication is configured in IS-IS routing process configuration mode. If the authentication is performed between routers in the same area, the key string or password must be the same.

Routing domain authentication: Indicates that authentication is configured in IS-IS routing process configuration mode. If the authentication is performed between routers in the same routing domain, the key string or password must be the same.

SNP packets can be authenticated separately from LSP packets and authentication check can be enabled for the received LSP or SNP packets.

9. IS-IS GR

For GR to be successful, the following two conditions must be met:

- The network topology is stable.
- The device can ensure uninterrupted forwarding when it restarts IS-IS.

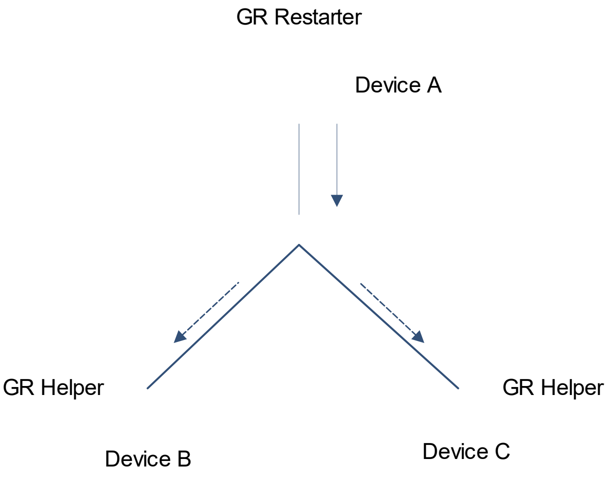
Two roles exist during the GR process: Restarter and Helper. Accordingly, the IS-IS GR function is divided into IS-IS GR Restart and IS-IS GR Help capabilities. A device with the IS-IS GR Restart capability can send GR requests and automatically execute GR. A device with the IS-IS GR Help capability can receive GR requests and assist neighbors in executing GR. The GR process starts when the Restarter sends a GR request. After receiving the GR request, the neighboring device enters Help mode to help the Restarter reestablish its LSDB while maintaining the neighbor relationship with the Restarter.

When an IS-IS device performs GR, it notifies its neighbors to maintain their neighbor relationship so that other devices in the network cannot sense the change in the topological relationship and the neighbors will not recalculate the route and update its forwarding table. The IS-IS device synchronizes and restores the LSDB to its pre-GR state with the help of the neighbors to ensure that the routing table and forwarding table remain unchanged before and after GR implementation and data forwarding is not interrupted.

The Restarter performs the following operations during the GR process:

(1) The GR Restarter notifies the GR Helpers that the local device will be restarted.

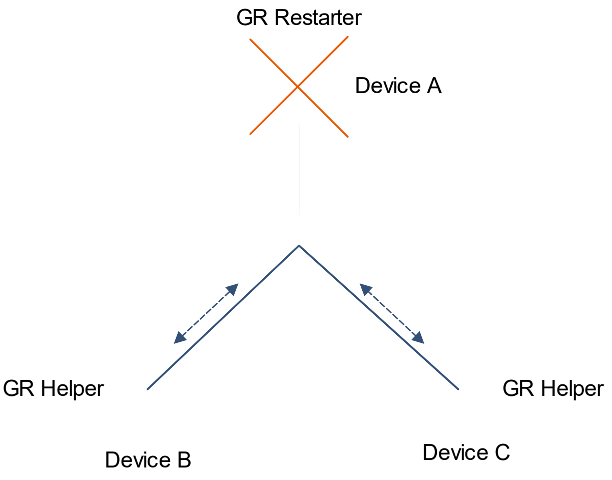
Figure 1-1Restarter Notifying Helpers of GR



Device A acts as the GR Restarter, and Devices B and C are GR Helpers of Device A. Device A sends a GR request instructing all its neighbors not to delete the neighbor relationships with Device A when it is restarted. After receiving the GR request, the neighbors send GR responses to the GR Restarter, and maintain their neighbor relationships with the GR Restarter during the GR time (specified by GR grace-period) notified by the GR Restarter.

(2) The GR Restarter is restarted.

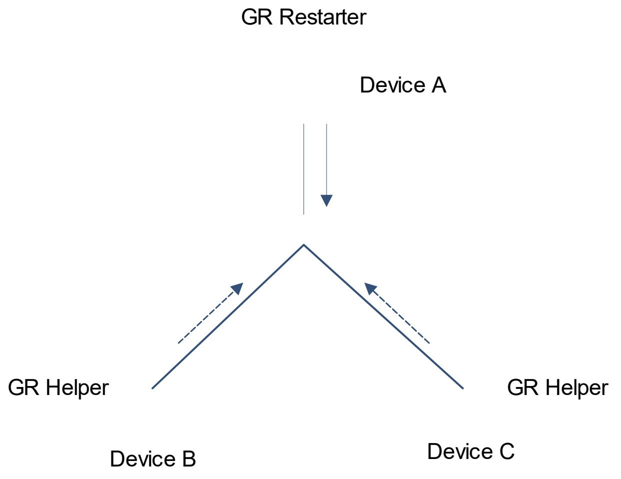
Figure 1-1Restarter Restart



When the GR Restarter is restarted, its IS-IS interface changes from down state to up state. The GR Helpers know that the GR Restarter is in IS-IS restart state, they maintain their neighbor relationships with the GR Restarter during the GR time and retain the routes from the GR Restarter.

(3) The GR Restarter synchronizes topology and routing information from the GR Helpers.

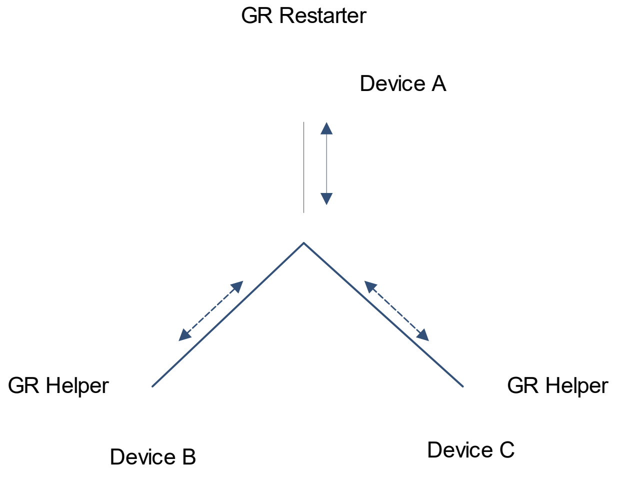
Figure 1-1LSDB Synchronization



After IS-IS restart, the GR Restarter synchronizes topology or routing information from the GR Helpers and recalculates its routing table. During the process, any change in the routing table is not updated to the forwarding table.

(4) GR is completed when the GR Restarter finishes LSDB synchronization. Then all devices enter IS-IS interaction state.

Figure 1-1GR Completion



After the GR Restarter synchronizes all required data, all devices enter IS-IS interaction state. The routing table of the GR Restarter is updated to the forwarding table and invalid entries are cleared. Because the GR Restarter is completely restored to the pre-restart state under stable network conditions, its routing table and forwarding table remain unchanged before and after GR.

10. Fast Convergence of IS-IS

IS-IS accelerates convergence by fast advertisement of LSPs and smart timer.

- Fast advertisement of LSPs

By modification of LSP flooding interval and maximum number of LSPs sent on an interface, LSPs can be advertised to the IS-IS area in the route computation time to reduce route computation and accelerate convergence when the LSPs trigger route computation.

- Smart timer

  LSP packet generation time and SPF algorithm computation time are adjusted based on the smart timer. In a stable IS-IS network, the route computation frequency is low and the first SPF algorithm time is short. In a network with ever-changing topology and network jitter, route computation frequency increases, which consumes CPU resources. In this case, the smart timer will increase SPF computation delay to accelerate convergence and reduce CPU consumption.

1.1.3 Protocols and Standards

- RFC 1142: OSI IS-IS Intra-domain Routing Protocol
- RFC 1195: Use of OSI IS-IS for routing in TCP/IP and dual environments
- RFC 3786: Extending the Number of Intermediate System to Intermediate System (IS-IS) Link State PDU (LSP) Fragments Beyond the 256 Limit
- RFC 3373: Three-Way Handshake for Intermediate System to Intermediate System (IS-IS) Point-to-Point Adjacencies
- RFC 3358: Optional Checksums in Intermediate System to Intermediate System (ISIS)
- RFC 3784: Intermediate System to Intermediate System (IS-IS) Extensions for Traffic Engineering (TE)
- RFC 2763: Dynamic Hostname Exchange Mechanism for IS-IS
- RFC 6119(draft-ietf-isis-ipv6-te-00): IPv6 Traffic Engineering in IS-IS
- RFC 2966: Domain-wide Prefix Distribution with Two-Level IS-IS
- RFC 5306: Restart Signaling for IS-IS

1.2 Restrictions and Guidelines

The PIM mode enabled on all interfaces of a device for an instance must be consistent.

1.3 Configuration Task Summary

IS-IS configuration includes the following tasks:

(1) Configuring Basic Settings of IS-IS

(2) (Optional) Configuring IS-IS network Levels

(3) (Optional) Configuring IS-IS Hello Packets

(4) (Optional) Configuring IS-IS LSPs

(5) (Optional) Configuring IS-IS SNPs

(6) (Optional) Configuring IS-IS Route Advertisement

(7) (Optional) Configuring IS-IS Route Summarization

(8) (Optional) Configuring an IS-IS Passive Interface

(9) (Optional) Controlling IS-IS Routing Factors

(10) (Optional) Configuring the Priority of an IS-IS Device

(11) (Optional) Configuring IS-IS Authentication

(12) (Optional) Configuring IS-IS GR

(13) (Optional) Configuring IS-IS NSR

(14) (Optional) Correlating IS-IS with BFD

(15) (Optional) Configuring the IS-IS Overload Bit

(16) (Optional) Configuring IS-IS VRF

(17) (Optional) Configuring IS-IS MTR

(18) (Optional) Configuring IS-IS SNMP

(19) (Optional) Enabling Super VLAN for IS-IS

(20) (Optional) Configuring IS-IS Two-way Maintenance

(21) (Optional) Configuring Extended Feature of IS-IS

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

- Configuring the Maximum Metric of a Neighbor
- Configuring the Maximum Number of Area Addresses
- Configuring SPF Calculation Interval
- Canceling Three-Way Handshake of a P2P Network
- Enabling TLV to Be Padded Based on Supported Protocol
- Configuring the Reachable Time of a Suppressed Neighbor
- Enabling Adjacency Event Output

1.4 Configuring Basic Settings of IS-IS

1.4.1 Overview

Basic settings of IS-IS are a precondition for configuration of all IS-IS features and basic internetworking.

1.4.2 Restrictions and Guidelines

- The Level-1 IS-IS devices in an area must be configured with the same area ID.
- The core routing table does not distinguish the routing entries generated by different IS-IS routing processes.
- The IP addresses of interfaces connected between neighbors must be in the same network segment.
- If the IP addresses are in different network segments, a neighbor relationship cannot be established.
- If you need to add an interface to the specified IS-IS routing process and configure the interface with the IPv4 IS-IS function, add the tag parameter after the **ip router isis** command to indicate the process name.

- If you run the **no ip routing** command in global configuration mode, IS-IS will disable IPv4 routing on all interfaces. That is, the **no ip router isis** *[tag]* command is automatically executed on all interfaces, with other IS-IS settings unchanged.
- If you need to add an interface to the specified IS-IS routing process and configure the interface with the IPv6 IS-IS function, add the tag parameter after the **ipv6 router isis** command to indicate the process name.
- If you run the **no ipv6 unicast-routing** command in global configuration mode, IS-IS will disable IPv6 routing on all interfaces. That is, the **no IPv6 router isis** *[tag]* command is automatically executed on all interfaces, with other IS-IS settings unchanged.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the IS-IS routing process and enter the IS-IS routing process configuration mode.

router isis [*tag*]

No IS-IS instance is configured by default.

If you configure the *tag* parameter when you start an IS-IS routing process, you need to add this tag parameter when you stop the IS-IS routing process.

(4) Configure a NET address in IS-IS.

net *net-address*

No NET address is configured in IS-IS by default.

Different NET addresses must have the same system ID.

(5) (Optional) Modify the system ID in IS-IS. Configure one of the following tasks.

- Replace the system ID of an instance with the configured name.

  is-**name** *name*

  The default system ID is used.

- Replace the system ID of a router with the host name of the destination router.

  hostname dynamic

  The host name replacement function is enabled by default.

(6) Return to the global configuration mode.

exit

(7) Enter the interface configuration mode.

interface *interface-type interface-number*

(8) Enable IS-IS on an interface.

- Enable IPv4 IS-IS on an interface.

  ip router isis [*tag*]

IPv4 IS-IS is not enabled on an interface by default.

- Enable IPv6 IS-IS on an interface.

  ipv6 router isis [*tag*]

  IPv6 IS-IS is not enabled on an interface by default.

1.5 Configuring IS-IS network Levels

1.5.1 Overview

IS-IS supports a two-Level system to realize routing management and extensible route selection in a large network. Each level is only concerned about maintaining the topology of the corresponding area.

1.5.2 Restrictions and Guidelines

- If the circuit-type is set to Level-1 or Level-2-only, IS-IS will only send PDUs at the corresponding level.
- If the circuit type of an interface is set to **external**, this interface will work as an external domain interface and IS-IS will not send PDUs at the corresponding level.
- A device can have only one instance running at Level-2 (including Level-1/Level-2).

1.5.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

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

router isis [*tag*]

(4) Configure a level of IS-IS.

is-type { **level-1 | level-1-2 | level-2-only** }

IS-IS runs at Level-1/Level-2 by default.

(5) Return to the global configuration mode.

exit

(6) Enter the interface configuration mode.

interface *interface-type interface-number*

(7) Configure an IS-IS level on an interface.

isis circuit-type { **level-1 | level-1-2 | level-2-only** [**external**] }

The circuit type of an interface is set to Level-1/Level-2 by default.

(8) Configure a broadcast interface as a P2P interface.

isis network point-to-point

The broadcast network type is unchanged by default.

1.6 Configuring IS-IS Hello Packets

1.6.1 Overview

Hello packet control parameters, including hello packet sending interval, hello holdtime, packet padding, and neighbor detection are configured. Neighbor establishment can be controlled to maintain neighbor interaction.

1.6.2 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 Hello packet sending interval of an interface.

isis hello-interval { *interval* | **minimal** } [**level-1 | level-2**]

The Level-1 and Level-2 hello packets are sent at an interval of **10** seconds by default.

(5) Configure the Hello packet holdtime multiplier on an interface.

isis hello-multiplier *multiplier-number* [**level-1** | **level-2**]

The default hello holdtime multiplier is **3**. That is, the hello holdtime is three times of the hello interval.

(6) Configure to pad IS-IS hello packets on an interface.

isis hello padding

Padding is enabled by default for hello packets sent on an interface.

(7) Enable neighbor supported protocol detection for hello packets in IPv4 environment.

adjacency-**check**

The neighbor supported protocol detection function for hello packets is enabled by default.

(8) Enter the IS-IS IPv6 address family configuration mode.

address-family ipv6 unicast

(9) Enable neighbor supported protocol detection for hello packets in IPv6 environment.

adjacency-**check**

The neighbor supported protocol detection function for hello packets is enabled by default.

(10) Exit the IS-IS IPv6 address family configuration mode.

exit-address-family

1.7 Configuring IS-IS LSPs

1.7.1 Overview

Adjusting timer and packet length of LSPs will affect LSP update timeliness and LSP frequency.

1.7.2 Restrictions and Guidelines

- The LSP generation time and refresh time can be configured to prevent network topology change from affecting the LSP transmission frequency.
- During LSDB change, IS-IS notifies the change by LSP advertisement. If a great number of IS-IS routes and interfaces exist on a device, a too small sending interval and a too great LSP number may cause LSP bursts. Therefore, the LSP sending interval and LSP number must be set to proper values. LSP retransmission interval is used in P2P network. In such a network, an LSP response must be returned to indicate completion of an LSP retransmission.
- The value of *lsp-refresh-interval* must be smaller than that of *max-lsp-lifetime*.
- The value of *max-lsp-lifetime* must be greater than that of *lsp-refresh-interval*.
- The value of the configured *initial-interval* cannot be greater than that of *maximum-interval*. Otherwise, the value of *initial-interval* is changed to that of *maximum-interval*.
- The value of the configured *hold-interval* cannot be greater than that of *maximum-interval*. Otherwise, the value of *hold-interval* is changed to that of *maximum-interval*.
- The value of the configured *initial-interval* cannot be greater than that of *hold-interval*. Otherwise, the value of *initial-interval* is changed to that of *hold-interval*.
- If no particular level is specified in the command, the default level is Level-1/Level-2, which means that the interval configuration takes effect to Level-1 and Level-2 concurrently.
- When you need to configure **mesh-group** on an IS-IS interface, run the **isis csnp-interval** command to configure the non-0 CSNP interval to ensure complete LSP synchronization between neighbors in the network. After that, CNSPs will be periodically sent to synchronize LSPs.

1.7.3 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) Modify LSP control parameters on the interface. The following configuration tasks are optional. Select tasks for configuration according to actual condition.

- Configure the LSP sending interval.

  isis lsp-interval *interval* [**level-1** | **level-2**]

  LSPs are sent at an interval of **33** ms by default on an IS-IS interface.

- Configure the maximum number of LSPs sent by an IS-IS interface at a time.

  isis lsp-flood *lsp-number* [**level-1** | **level-2**]

  An IS-IS interface sends at most 5 LSPs at a time by default.

- Configure the LSP retransmission interval.

  isis retransmit-interval *retransmit-interval* [**level**-1 | **level**-2]

  LSPs are retransmitted at an interval of **5** seconds by default.

  If *retransmit-interval* is set to **0**, no LSP is retransmitted.

(5) Return to the global configuration mode.

exit

(6) Enter the IS-IS routing process configuration mode.

router isis [*tag*]

(7) Modify LSP control parameters in the IS-IS process. The following configuration tasks are optional. Select tasks for configuration according to actual condition.

- Configure the LSP generation interval.

  lsp-gen-interval [**level-1** | **level-2**] *maximum-interval* [*initial-interval hold-interval*]

  The default maximum interval between two LSP generation times is **5** seconds, the delay for generating an LSP is **50** ms, and the minimum interval between the first LSP generation time and the second LSP generation time is **200** ms.

- Configure the LSP refresh interval.

  lsp-refresh-interval *interval*

  The default LSP refresh interval is **900** seconds.

- Configure the LSP lifetime.

  max-lsp-lifetime *max-lifetime*

  The default maximum LSP lifetime is **1200** seconds.

- Configure the interval for receiving duplicate LSP packets.

  min-lsp-arrival [**level-1** | **level-2**] *minimum-interval initial-interval hold-interval*

  The function of receiving duplicate LSP packets is not supported by default.

- Configure to ignore LSP checksum errors.

  ignore-lsp-errors

  LSP checksum errors are processed by default.

- Configure LSP fragment extension.

  lsp-fragments-extend [**level-1** | **level-2**] [**compatible rfc3786**]

  The fragment extension function is disabled by default. To enable fragment extension, run this command to configure fragment extension at the specified level and run the **virtual-system** command to configure an additional system ID.

- Configure the additional system ID of the IS-IS routing process.

  virtual-system *system-id*

  No additional system ID is configured by default. To enable fragment extension, run this command to configure an additional system ID and run the **lsp-fragments-extend** command to configure fragment extension.

- Configure the maximum length of received LSPs.

  lsp-length receive *size*

  The default maximum length of received LSPs is **1492** bytes.

- Configure the maximum length of sent LSPs.

  lsp-length originate *size* [**level-1** | **level-2**]

  The default maximum length of sent LSPs is **1492** bytes.

- Add an IS-IS interface to a specified mesh group.

  isis mesh-group { **blocked** | *mesh-group-id* }

  No interface joins any mesh group by default.

1.8 Configuring IS-IS SNPs

1.8.1 Overview

By default, a DIS in a broadcast network sends a CSNP every 10s for LSDB synchronization. In a P2P network, CSNPs are sent only after a neighbor relationship is established.

1.8.2 Restrictions and Guidelines

- If an interface is added to a mesh group, CSNP sending interval can be configured. If the CSNP interval is set to **0**, no CSNP is sent.

1.8.3 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 CSNP broadcast interval on an IS-IS interface.

isis csnp-interval *interval* [**level-1** | **level-2**]

CSNPs are sent at an interval of **10** seconds in a broadcast network by default. No CSNPs are sent in a P2P network by default.

When you configure a new CSNP interval without specifying Level-1 or Level-2, the interval configuration takes effect for Level-1 and Level-2 CSNPs by default.

(5) Configure the minimum PSNP sending interval.

isis psnp-interval *psnp-interval* [**level-1** | **level-2**]

The function of configuring the PSNP sending interval is disabled by default. In this case, the minimum PSNP sending interval is **2** seconds by default and it takes effect for Level-1 and Level-2 PSNPs.

1.9 Configuring IS-IS Route Advertisement

1.9.1 Overview

IS-IS can introduce routes of other routing protocols and routes of other IS-IS processes to the IS-IS process and mutually introduce routes between Level-1 and Level-2 areas.

1.9.2 Restrictions and Guidelines

- Because Level-2 domains do not generate any default route, the **default-information originate** command is run to allow a default route to enter a Level-2 domain.
- In the old versions of some vendors, if **metric-type** is set to **external**, the metric of redistributed routes is added by 64 during route calculation and used to determine routing. This practice does not comply with the related protocol. In the actual application, external routes may be preferred over internal routes. If this happens during interworking with old versions of some vendors, you can modify the related setting (such as **metric** or **metric-type**) of each device to ensure that internal routes are preferred over external routes.

1.9.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

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

router isis [*tag*]

(4) Generate a default route.

default-information originate [**route-map** *map-name*]

No default route is generated by default.

(5) Redistribute other routes to IS-IS.

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

Redistribution is disabled by default.

(6) Redistribute the Level-1 reachable routing information of the specified IS-IS instance to Level-2 of the current instance.

redistribute isis [*tag*] **level-1 into level-2** [**distribute**-**list** *acl-name* | **route-map** *route-map-name*]

Redistribution is disabled by default.

(7) Redistribute the Level-2 reachable routing information of the specified IS-IS instance to Level-1 of the current instance.

redistribute isis [*tag*] **level-2 into level-1** [**distribute**-**list** *acl-name* | {

ipv6-**prefix** *ipv6-address*/*length* |

prefix *ipv4-address net-mask* } | **route**-**map** *route-map-name*]

Redistribution is disabled by default.

1.10 Configuring IS-IS Route Summarization

1.10.1 Overview

Configuring route summarization can effectively reduce the size of a routing table and system resource usage. If the links in the range of the IP addresses to be summarized jitter (up and down), advertisement of the summarized routes is not affected to avoid route flapping. After route summarization, if any routing information about a reachable address or network segment exists, a summarized route, instead of a detailed route, is advertised externally.

1.10.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

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

router isis [*tag*]

(4) Configure an IPv4 summarized route.

summary-address *ipv4-address net-mask* [**level-1** | **level-1-2** | **level-2**] [**metric** *metric-value*]

The route summarization function is disabled by default.

(5) Enter the IS-IS IPv6 address family configuration mode.

address-family ipv6 unicast

(6) Enable IPv6 route summarization.

summary-prefix *ipv6-prefix/prefix-length* [**level-1** | **level-1-2** | **level-2**]

The route summarization function is disabled by default.

1.11 Configuring an IS-IS Passive Interface

1.11.1 Overview

This function prevents the specified interface from receiving and sending IS-IS packets, but the IP address of this interface will be flooded by other interfaces.

1.11.2 Restrictions and Guidelines

- If the number of interfaces with IS-IS not enabled exceeds 255, only the first 255 interfaces will be configured as passive interfaces. The remaining interfaces are non-passive interfaces.

1.11.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

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

router isis [*tag*]

(4) Configure a passive interface in the IS-IS routing process configuration mode.

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

The passive interface function is disabled by default.

(5) Return to the global configuration mode.

exit

(6) Enter the interface configuration mode.

interface *interface-type interface-number*

(7) Configure a passive interface.

isis passive

The configured passive interface in the IS-IS routing process configuration mode prevails by default.

1.12 Controlling IS-IS Routing Factors

1.12.1 Overview

IS-IS routing is determined by adjusting the number of equal-cost routes, reference bandwidth values, and interface costs.

1.12.2 Restrictions and Guidelines

- The **maximum-paths** command is used by IS-IS to control the number of IS-IS equal-cost paths to be added to a routing table. There is also a routing table command used to control the number of equal-cost paths. The number of effective equal-cost paths is determined by either of the two command values, whichever is smaller.
- The **bandwidth-reference** command is used to calculate the interface metric in an instance based on the bandwidth value configured in the instance. If a metric is configured, the metric prevails.
- The metric, which is used in SPF calculation, is stored in the IP reachability information TLV. A greater metric value indicates a greater routing consumption of this interface and a longer path of SPF calculation. The Narrow-metric value is valid only when Metric-style is set to **Narrow**. The Wide-metric value is valid only when Metric-style is set to **Wide**.

1.12.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

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

router isis [*tag*]

(4) Configure the administrative distance of an IS-IS route.

distance *distance-value*

The default administrative distance of IS-IS is **115**.

(5) Configure the maximum number of equal-cost paths.

maximum-paths *maximum*

The default maximum number of equal-cost paths is **2**.

(6) Configure the reference bandwidth value for cost computation.

bandwidth-reference *value*

The default reference bandwidth value for cost computation is **100** Mbps.

(7) Configure the metric type.

metric-style { **narrow** | **wide** } [**transition**] [**level-1** | **level-2** | **level-1-2**]

The default metric type is Narrow.

(8) Return to the global configuration mode.

exit

(9) Enter the interface configuration mode.

interface *interface-type interface-number*

(10) Configure metric of the IS-IS interface.

isis metric *metric* [**level-1 | level-2**]

Level-1 and Level-2 use the computation result of bandwidth-reference by default.

(11) Configure the wide metric value of an interface.

isis wide-metric *metric* [**level-1 | level-2**]

The default wide metric value of Level-1 and Level-2 is the computation result of **bandwidth-reference**.

1.13 Configuring the Priority of an IS-IS Device

1.13.1 Overview

Adjusting DIS election priority of a device on an interface can manually affect DIS election result and specify a device to become the DIS.

1.13.2 Restrictions and Guidelines

- A lower DIS priority of an interface indicates a lower priority of being elected as a DIS.
- This function is invalid on a P2P network interface.

1.13.3 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 device priority in DIS election.

isis priority *value* [**level-1 | level-2**]

The default priority of a device for Level-1 and Level-2 DIS election is **64**.

1.14 Configuring IS-IS Authentication

1.14.1 Overview

Internet requirements for information security increase. To avoid data theft and tampering, operators apply the IS-IS authentication function on specified areas or interfaces to ensure data security.

- Interface authentication is intended for establishing and maintaining neighbor relationships. A neighbor relationship cannot be established between two IS-IS devices with different interface authentication passwords. This prevents unauthorized or unauthenticated IS-IS devices from joining an IS-IS network that requires authentication. Interface authentication passwords are encapsulated in Hello packets before being sent.
- Area authentication and routing domain authentication in IS-IS are performed to verify LSPs, CSNPs, and PSNPs to prevent unauthorized or unauthenticated routing information from being injected into the LSDB. Authentication passwords are encapsulated in LSPs, CSNPs, and PSNPs before being sent.

1.14.2 Restrictions and Guidelines

- An interface authentication password is encapsulated in a Hello packet before being sent by an interface. When an interface receives a Hello packet, it checks the password in the packet against the existing one.
- Area authentication passwords are encapsulated in Level-1 LSPs, CSNPs, and PSNPs. When an interface receives an LSP, CSNP, or PSNP, it checks the password in the packet against the existing one.
- Routing domain authentication passwords are encapsulated in Level-2 LSPs, CSNPs, and PSNPs. When an interface receives an LSP, CSNP, or PSNP, it checks the password in the packet against the existing one.
- If no particular Level is specified in the command, the default level is Level-1/Level-2, which means that the authentication configuration takes effect to Level-1 and Level-2 concurrently.
- A key chain may contain multiple passwords. A password with a smaller SN is preferentially used for sending a packet. When the packet arrives at the peer device, the device will receive the packet if the password in the packet is consistent with a password in the key chain.
- For plaintext authentication, the *string-text* in the key chain cannot exceed 80 characters; otherwise, the key chain will be invalid.
- Only one key chain can be used at a time. After you configure a new key chain, it will replace the original

one.

- Before you deploy IS-IS interfaces and area authentication on all devices in the network or before you change the authentication password or authentication mode, run the **send-only** command. The devices will not authenticate received Hello packets to avoid network flapping when IS-IS interface authentication is deployed.

1.14.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a key chain, and enter the key chain configuration mode.

key chain *key-chain-name*

(4) Create a key chain, and enter the key chain configuration mode.

key *key-id*

(5) Configure the key.

key-string [**0** | **7**] *string-text*

(6) Exit the key chain configuration mode.

exit

(7) Return to the global configuration mode.

exit

(8) Enter the interface configuration mode.

interface *interface-type interface-number*

(9) Configure Hello packet authentication on an interface.

- Specify the authentication mode as plaintext or MD5.

  isis authentication mode { **md5** | **text** } [**level-1** | **level-2**]

  The interface authentication mode is disabled by default.

  The priority of the password is higher than that of the password configured using the **isis password** command.

- Configure the password for interface authentication.

  isis authentication key-chain *key-chain-name* [**level-1** | **level-2**]

  Authentication is not performed if no key chain is configured using the **key chain** command. In addition to the key chain command, you also need to run the **isis authentication mode** command to make IS-IS key chain authentication take effect.

- (Optional) Configure the password for plaintext authentication of hello packets on an interface.

  isis password [**0** | **7**] *password-string* [**send-only**] [**level-1** | **level-2**]

  Plaintext authentication is not enabled by default.

This command does not take effect if the **isis authentication mode** command has been run to configure authentication before.

- (Optional) Configure an authentication password in the Hello packets sent. Received Hello packets are not authenticated.

  isis authentication send-only [**level-1** | **level-2**]

  Packets sent and received on an interface are authenticated by default.

(10) Return to the global configuration mode.

exit

(11) Enter the IS-IS routing process configuration mode.

router isis [*tag*]

(12) Configure LSP, CSNP, and PSNP packet authentication in an IS-IS area.

- (Optional) Configure a password for plaintext authentication of a Level-1 area.

  area-password [**0** | **7**] *password-string* [**send-only**]

  The plaintext authentication function of a Level-1 area is disabled by default.

  All IS-IS devices in an area must be configured with the same authentication password. This command does not take effect if the **authentication mode** command has been run to configure authentication before.

- (Optional) Configure a password for plaintext authentication of a Level-2 routing domain.

  domain-password [**0** | **7**] *password-string* [**send-only**]

  The Level-2 area authentication password function is disabled by default.

  All IS-IS devices in Level-2 domain must be configured with the same authentication password. This command does not take effect if the **authentication mode** command has been run to configure authentication before.

- Specify the IS-IS routing domain authentication mode.

  authentication mode { **md5** | **text** } [**level-1** | **level-2**]

  The authentication function is disabled by default.

- Specify the key chain for IS-IS authentication.

  authentication key-chain *name-of-chain* [**level-1** | **level-2**]

  No authentication key chain is configured by default.

  Authentication is not performed if no key chain is configured using the **key chain** command. In addition to the key chain command, you also need to run the **authentication mode** command to make IS-IS key chain authentication take effect.

- (Optional) Apply IS-IS authentication only to send packets.

  authentication send-only [**level-1** | **level-2**]

  Packets sent and received are authenticated by default.

1.15 Configuring IS-IS GR

1.15.1 Overview

As long as the network conditions remain unchanged, GR enables IS-IS to be restarted and restored to the pre-restart state without impact on data forwarding. This improves system reliability.

Two roles exist during the GR process: Restarter and Helper. Accordingly, the IS-IS GR function is divided into IS-IS GR Restart and IS-IS GR Help capabilities. A device with the GR Restart capability can send a GR request and execute GR. A device with the GR Help capability can receive a GR request and help its neighbor with GR implementation. The GR process starts when the Restarter sends a GR request. After receiving the GR request, the neighboring device enters Help mode to help the Restarter reestablish its LSDB while maintaining the neighbor relationship with the Restarter. The main GR working mechanism is as follows:

1.15.2 Restrictions and Guidelines

✓ Specification

All products support the IS-IS GR Helper capability.

1.15.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

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

router isis [*tag*]

(4) Enable the IS-IS GR Restart capability.

graceful-restart

The IS-IS GR Restart capability is enabled by default.

(5) (Optional) Configure the maximum GR interval of a device.

graceful-restart grace-period *max-interval*

The maximum GR interval is **300** seconds by default.

(6) Enable the IS-IS GR Help capability.

graceful-restart helper disable

The IS-IS GR Helper function is enabled by default.

This command enables IS-IS to ignore the GR request sent by the device to be restarted.

1.16 Configuring IS-IS NSR

1.16.1 Overview

IS-IS nonstop routing (IS-IS NSR) helps improve system reliability. During the active/standby switchover of devices in distributed or Virtual Switch Unit (VSU) mode, user data traffic keeps being forwarded without interruption. Information that can be backed up includes command configuration, neighbor backup, and LSP DB.

NSR backs up relevant IS-IS information from the master Supervisor Engine to the slave Supervisor Engine of the distributed device, or from the master device to the salve device in VSU mode, so that the device can automatically recover the link state and regenerate a route upon active/standby switchover, without requiring help from neighbor devices during the recovery.

Compared with GR that needs the help of a neighbor, NSR does not need any help from neighbors.

1.16.2 Restrictions and Guidelines

- For the same IS-IS process, either NSP or GR is enabled, because they are exclusive.
- The switchover of distributed devices and VSU devices takes a period of time. If the IS-IS neighbor keepalive duration is less than the switchover duration, IS-IS neighbor relationship with the neighbor device is removed, and the services are interrupted during the switchover. Therefore, it is recommended that the IS-IS neighbor keepalive duration be set not less than the default value. When Fast Hello is enabled, the IS-IS neighbor keepalive duration is less than 1 second and the IS-IS neighbor relationship times out during the switchover, causing NSR failures. Therefore, it is recommended that Fast Hello be disabled when NSR is enabled.

1.16.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

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

router isis [*tag*]

(4) Enable the NSR function.

nsr

The NSR function is disabled by default.

1.17 Correlating IS-IS with BFD

1.17.1 Overview

Bidirectional Forwarding Detection (BFD) is used to test connectivity between devices. A link fault can be detected in as short as 150 ms. After IS-IS is correlated with BFD, IS-IS can sense the death of a neighbor in as short as 150 ms once a link is faulty. This accelerates route convergence and prevents traffic interruption.

Normally, BFD sends detection packets at millisecond intervals to detect the link state. When a link exception (such as a disconnected link) occurs, BFD can quickly detect it and instruct IS-IS to delete the neighbor relationship and the neighbor reachability information in LSPs. Then IS-IS recalculates and generates a new route to bypass the abnormal link, thus realizing fast convergence. With the introduction of new techniques such as the Multi-Service Transport Platform (MSTP), link congestion tends to occur during peak hours of data communication. BFD quickly detects the link exception and instructs IS-IS to delete the neighbor relationship and the neighbor reachability information in LSPs. Link switch is performed to bypass the congested link. A Hello packet for IS-IS neighbor detection is sent every 10s and its expiration time is 30s. The Hello packet can still be received normally when BFD detects an exception, and therefore an IS-IS neighbor relationship is reestablished quickly, causing the route to be restored to the congested link. Then BFD detects the abnormal link and link switch is performed again. This process is repeated, which makes the route be switched between the congested link and other links, causing repetitive flapping.

The anti-congestion option is used to avoid routing flapping in case of link congestion. After the option is configured, the IS-IS neighbor state is still kept alive when link congestion occurs, but the neighbor reachability information in LSPs is deleted. The route is switched to a normal link. When the congested link is restored, the neighbor reachability information in LSPs is recovered and the route is switched back, which avoids route flapping.

1.17.2 Restrictions and Guidelines

- You must configure BFD session parameters before you enable IS-IS correlation with BFD.
- When you run the **bfd up-dampening** command on an interface with IS-IS correlation with BFD, you must run the **bfd all-interfaces [anti-congestion]** command.
- When you run the **bfd all-interfaces [anti-congestion]** command, you must run the **bfd up-dampening** command on the interface. The two commands must be used together. If you run only one command, the anti-congestion feature may not take effect or other network exceptions may occur.
- IP routing may cause a neighbor's interface for BFD session setup to be inconsistent with the interface for outgoing BFD packets. If this happens, the BFD session cannot be set up.
- If a neighbor's interface for BFD session setup is inconsistent with the interface for outgoing BFD packets, the BFD session cannot be set up.

1.17.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

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

router isis [*tag*]

(4) Enable BFD correlation in IS-IS process mode.

bfd all-interfaces [**anti-congestion**]

The IS-IS correlation with BFD function is disabled on all interfaces by default.

(5) Return to the global configuration mode.

exit

(6) Enter the interface configuration mode.

interface *interface-type interface-number*

(7) Enable IS-IS correlation with BFD on an interface.

isis bfd [**disable** | **anti-congestion**]

The IS-IS correlation with BFD function is enabled on an interface by default if the **bfd all-interfaces** command is run. The IS-IS correlation with BFD function is not enabled on an interface if the **bfd all-interfaces** command is not run. The anti-congestion option is disabled by default.

1.18 Configuring the IS-IS Overload Bit

1.18.1 Overview

An IS-IS node is forced to configure the overload bit in a non-virtual LSP to instruct its IS-IS neighbors to avoid using the local node as a forwarding device.

1.18.2 Restrictions and Guidelines

- If the **on-startup** keyword is selected, the IS-IS node automatically enters overload state after restart. If the **on-startup** keyword is not selected, the IS-IS node enters overload state immediately after restart.
- The overload bit is used in the following three situations:

○ Device overload

The local IS-IS node has overload issues, such as insufficient memory or full CPU load; as a result, its routing table has incomplete routes or does not have resource forwarding data. You can configure the overload bit in an LSP to instruct the neighbor to avoid using the local node as a forwarding device.

To configure the overload bit, run the **set-overload-bit** command without the **on-startup** keyword. The overload bit can be configured or removed manually. When the local IS-IS node is restored, manually remove the command configuration; otherwise, the node is always in overload state.

○ Instantaneous black hole

In the scenario described by RFC 3277, the IS-IS convergence speed is faster than the BGP speed; as a result, after an IS-IS node is restarted, a route may be instantaneously unreachable, which is called an instantaneous black hole. You can set the overload bit in an LSP to instruct the neighbor to avoid using the local node as a forwarding device until the specified time has elapsed.

To set the overload bit, run the **set-overload-bit** command with the **on-startup** keyword. The overload bit can be configured or removed automatically by the IS-IS node based on the configuration. After the **on-startup** keyword is selected, the IS-IS node automatically enters instantaneous black hole state after restart. When a neighbor relationship is established, the IS-IS node sends an LSP with the overload bit to notify the neighbor that the local node enters instantaneous black hole (or overload) state and instruct the neighbor to avoid using the local node as a forwarding device. After the specified time has elapsed, the IS-IS node immediately sends an LSP with the overload bit canceled to notify the neighbor that the local node has exited instantaneous black hole (or overload) state and can work as a forwarding device.

○ Disabling real data forwarding on the local IS-IS node

If you only need to connect the local IS-IS node to a production network for testing or to meet other functional requirements, but does not require the node to forward real data in the network, you can set the overload bit in an LSP to instruct the neighbor to avoid using the local node as a forwarding device.

To set the overload bit, run the **set-overload-bit** command without the **on-startup** keyword. The overload bit can be configured or removed manually. You can set the **suppress** keyword based on requirements to limit the routing information carried in an LSP in case of overload. For example, internal and external routes can be suppressed, and only the local direct route is advertised. For example, the advertised direct route and the metric value to reach a neighbor are set to the maximum values.

1.18.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

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

router isis [*tag*]

(4) Configure the IS-IS overload bit.

set-overload-bit [**on-startup** { *overload-time* | **wait-for-bgp** [*bgp-convergence-time*] }] [**suppress** { **interlevel** | **external** | **max-metric** } *] [**level-1** | **level-2**]

A neighbor considers the local IS-IS node as a forwarding device to forward data by default.

1.19 Configuring IS-IS VRF

1.19.1 Overview

VPN routing and forwarding (VRF) is mainly used for local routing and packet. It avoids route conflict caused by use of the same prefix by multiple VPNs.

1.19.2 Restrictions and Guidelines

- The IS-IS instances bound with the same VRF table must be configured with different system IDs. The IS-IS instances bound with different VRF tables can be configured with the same system ID.
- One IS-IS instance can be bound with only one VRF table, but one VRF table can be bound to multiple IS-IS instances.
- When the VRF table bound to an IS-IS instance is changed, all IS-IS interfaces associated with the instance will be deleted. That is, the **ip router isis [tag] interface** configuration and the redistribution configuration in routing process configuration mode will be deleted.

1.19.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

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

router isis [*tag*]

(4) Configure IS-IS VRF.

vrf *vrf-name*

VRF binding of an IS-IS instance is disabled by default.

1.20 Configuring IS-IS MTR

1.20.1 Overview

The IS-IS MTR technique helps users deploy IPv6 unicast networks without the constraint on consistency between IPv4 and IPv6 unicast topology information.

1.20.2 Restrictions and Guidelines

- Metric-style must be set to **Wide** or **Transition** before you enable this function.
- The MTR feature will be disabled if Metric-style is set to **Narrow** or only one Level is configured to support Wide or Transition mode.

1.20.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the IS-IS IPv6 address family configuration mode.

address-family ipv6 unicast

(4) Configure IS-IS MTR.

multi-topology [*transition*]

IS-IS is not configured with MTR by default. That is, IS-IS does not support IPv6 unicast topologies. Configure IS-IS SNMP.

1.21 Configuring IS-IS SNMP

1.21.1 Overview

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

1.21.2 Restrictions and Guidelines

- The latest standards stipulate that the MIB operation can be performed on a single instance. By default, the MIB operation is performed on the first displayed IS-IS instance. Because multiple IS-IS instances can be configured, the administrator can use this command to specify the instances on which the MIB operation will be performed.

1.21.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable IS-IS trap globally.

snmp-server enable traps [*isis*]

The SNMP agent is forbidden to send Trap messages to the NMS by default.

This command must be used with the **snmp-server host** command in global configuration mode so that trap messages can be sent.

(4) Configure an SNMP host globally.

snmp-server host { *ipv4-addrress* | **ipv6** *ipv6-address* } [**vrf** *vrf-name*] [**traps**] [**version** { **1** | **2c** | **3** { **auth** | **noauth** | **priv** }] *community-string* [**udp-port** *port-num*] [*notification-type*]

No SNMP host address is configured by default.

(5) Enter the IS-IS routing process configuration mode.

router isis [*tag*]

(6) Bind the instances on which the IS-IS MIB operation will be performed.

enable mib-binding

By default, the SNMP operation is performed on the first displayed IS-IS instance.

(7) Allow sending trap messages.

enable traps { **all** | *traps set* }

The IS-IS trap message sending function is disabled by default.

1.22 Enabling Super VLAN for IS-IS

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 IS-IS multicast packets are sent over a super VLAN containing multiple sub VLANs, the IS-IS multicast packets are replicated multiple times, which exceeds the processing capability of the device. As a result, a large number of packets are discarded, causing protocol flapping. In most scenarios, the IS-IS function does not need to be enabled on a super VLAN, and it is disabled by default. In some application scenarios, the IS-IS function must be run on the super VLAN, but packets only need to be sent to one sub VLAN. In this case, you can decide to send multicast packets to a certain sub VLAN or to all sub VLANs as actually needed using this command. You must be cautious when configuring packet transmission to all sub VLANs, as the large number of sub VLANs may cause a device processing bottleneck, which will lead to the neighbor flapping.

1.22.2 Restrictions and Guidelines

- The IS-IS basic functions must be configured.

- The specified 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 *interface-type interface-number*

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

isis subvlan [**all |** *vlan-id*]

The IS-IS function takes effect in super VLAN only and is disabled by default.

1.23 Configuring IS-IS Two-way Maintenance

1.23.1 Overview

In a large-scale network, a large number of packets are sent and received, which occupies lots of CPU and memory resources, causing some IS-IS packets to be delayed or discarded. If the time required for processing hello packets exceeds the neighbor relationship maintenance time, the corresponding neighbor relationship times out and is removed. If the two-way maintenance function is enabled, in addition to the hello packets, the LSP, CSNP, and PSNP packets from a neighbor can also be used to maintain the bidirectional communication between neighbors when a large number of packets exist in the network. This prevents termination of the adjacency caused by delayed or discarded hello packets.

1.23.2 Restrictions and Guidelines

- The IS-IS basic functions must be configured.
- The neighbor relationship is successfully established.

1.23.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

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

router isis [*tag*]

(4) Enable the IS-IS two-way maintenance function.

two-way-maintain

The two-way maintenance function is enabled by default.

1.24 Configuring Extended Feature of IS-IS

1.24.1 Overview

IS-IS provides rich extended features that can be configured based on actual needs.

1.24.2 Configuration Tasks

The IS-IS extended feature configuration tasks are as follows and optional. Select tasks for configuration according to the actual condition.

- Configuring the Maximum Metric of a Neighbor
- Configuring the Maximum Number of Area Addresses
- Configuring SPF Calculation Interval
- Canceling Three-Way Handshake of a P2P Network
- Enabling TLV to Be Padded Based on Supported Protocol
- Configuring the Reachable Time of a Suppressed Neighbor
- Enabling Adjacency Event Output

1.24.3 Configuring the Maximum Metric of a Neighbor

1. Overview

In the Overlay scene where IS-IS is applied to Underlay, the Overlay tunnel may rely on Underlay routing. After the IS-IS neighbor is up, the Underlay route is reachable but the Overlay tunnel may not be created, which may lead to traffic interruption. This function can prevent traffic interruption.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

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

router isis [*tag*]

(4) Configure the maximum metric for the directly-connected route after the first neighbor is up.

max-metric on-neighbor-up *delay-time*

The metric of the directly-connected route is not set to the maximum value by default.

1.24.4 Configuring the Maximum Number of Area Addresses

1. Overview

Generally, an IS-IS process is configured with a NET address. During area reallocation, an IS-IS process can be configured with multiple NET addresses to ensure routing correctness. The system ID of multiple NET addresses must be the same. For Level-1 IS-IS routers, neighbor relationship can be created between the routers only when the maximum numbers of area addresses are the same.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

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

router isis [*tag*]

(4) Configure the maximum number of area addresses.

max-area-addresses *max-area-number*

The maximum number of area addresses is **3** by default.

1.24.5 Configuring SPF Calculation Interval

1. Overview

Increasing the maximum interval for performing SPF calculations can avoid frequent SPF calculations and waste of CPU resources. However, a larger interval also leads to slower responses to route changes.

2. Restrictions and Guidelines

- The first wait time for performing the SPF calculation is *initial-interval*. If the network is unstable, the SPF calculation trigger interval is smaller than *maximum-interval* and the second wait time for performing the SPF calculation is changed to *hold-interval*. A corresponding penalty is added to this interval: The next interval for the SPF calculation doubles the previous interval for the same SPF calculation, until the SPF calculation interval reaches the *maximum interval*. Subsequent SPF calculations are performed at the *maximum interval*. When the network becomes stable, the interval for performing the SPF calculation becomes greater than the *maximum interval*, and the wait time for performing the SPF calculation is restored to the *initial interval*.
- The value of the configured *initial-interval* cannot be greater than that of *maximum-interval*. Otherwise, the value of *initial-interval* is changed to that of *maximum-interval*.
- The value of the configured *hold-interval* cannot be greater than that of *maximum-interval*. Otherwise, the value of *hold-interval* is changed to that of *maximum-interval*.
- The value of the configured *initial-interval* cannot be greater than that of *hold-interval*. Otherwise, the value of *initial-interval* is changed to that of *hold-interval*.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

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

router isis [*tag*]

(4) Configure the SPF calculation interval.

spf-interval [**level-1** | **level-2**] *maximum-interval* [*initial-interval hold-interval*]

By default, the maximum calculation interval of two SPF calculations is **10** seconds, the delay of the first SPF calculation is **50** ms, and the maximum interval for the first and second SPF calculations is **200** ms. Exponential backoff algorithm uses Level-1/Level-2. That is, it takes effect for Level-1 and Level-2 concurrently.

1.24.6 Canceling Three-Way Handshake of a P2P Network

1. Overview

Neighbor establishment in a P2P network requires three-way handshake. The neighbor relationship can be established only after the three-way handshake succeeds. If you want to accelerate neighbor establishment or there is device that does not support three-way handshake, you can run this command to cancel three-way handshake.

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) Cancel three-way handshake of a P2P network.

isis three-way-handshake disable

Three-way handshake is performed by default.

1.24.7 Enabling TLV to Be Padded Based on Supported Protocol

1. Overview

When network devices supporting IPv4 IS-IS, IPv6 IS-IS, and IPv4 IS-IS and IPv6 are configured to establish a neighbor relationship, the calculated routes may be unreachable, resulting in routing black holes. To prevent routing black holes, the TLV (#129) field of device IS-IS protocol is padded based on protocols supported by an instance, that is, IS-IS instances that establish a neighbor relationship need to support the same protocol.

2. Restrictions and Guidelines

The TLV (#129) field of the IS-IS protocol supported by devices of some vendors is padded based on protocols supported by an interface. In single topology mode, a Orion_B26Q device connects to a device of another vendor, a loopback interface is configured on both devices, both IS-IS IPv4 IS-IS and IPv6 IS-IS are enabled, and only a single protocol stack (IPv4 IS-IS or IPv6 IS-IS) is configured on the interconnected interfaces of the two devices. The device of the other vendor sends TLV#129 (supporting only a single protocol stack) based on interfaces whereas Orion_B26Q device sends TLV#129 (supporting dual protocol stacks) based on instances. As a result, the displayed neighbor status on the device of the other vendor is "Init". Orion_B26Q devices failed to establish a neighbor relationship with the device of the other vendor. For this, the **interfaces-protocol-compatible** command can be configured to enable Orion_B26Q devices to establish a neighbor relationship with devices of other vendors.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

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

router isis [*tag*]

(4) Configure the TLV field of the IS-IS protocol to be padded based on protocols supported by an interface.

interfaces-protocol-compatible

The TLV field of the IS-IS protocol is padded based on protocols supported by an interface by default.

1.24.8 Configuring the Reachable Time of a Suppressed Neighbor

1. Overview

After the interface neighbor is up, this command prevents the neighbor reachability information from being added to LSP so as to delay the routing calculation. When the timer expires, the neighbor reachability information is added to LSP to start the routing calculation. This function prevents the route calculation from using the old LSP, which may lead to route flapping.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

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

router isis [*tag*]

(4) Suppress route calculation after the IS-IS neighbor is up.

isis suppress on-neighbor-up *delay-time*

The route calculation suppression function is disabled by default.

1.24.9 Enabling Adjacency Event Output

1. Overview

You can run a debug command to record neighbor state changes of IS-IS, but the command consumes many system resources. You can enable adjacency event output to avoid this issue.

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) Enable neighbor relationship event output.

log-adjacency-changes

The function of recording neighbor state changes of IS-IS is enabled by default without the debug command.

1.25 Monitoring

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

Run the **clear** command to clear information.

⚠ **Caution**

Running the **clear** command during operation of the device may lose vital information and interrupt services.

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

⚠ Caution

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

Table 1-1Monitoring

Command	Purpose
clear clns neighbors	Clears all IS-IS neighbor relationship tables.
clear isis *	Clears all IS-IS data structures.
clear isis [*tag*] **counter**	Clears different statistical information of IS-IS.
show clns [*tag*] **is-neighbors** [*interface-type interface-number*] [**detail**]	Displays all IS-IS neighbors and provides device adjacency relationships.
show clns [*tag*] **neighbors** [*interface-type interface-number*] [**detail**]	Displays all IS neighbors and provides device information and adjacency relationship information about terminals.
show isis [*tag*] **counter**	Displays different statistical information of IS-IS.
show isis [*tag*] **database** [*FLAGS*] [*LEVEL*]	Displays LSP DB information.

Command	Purpose
[*LSPID*]	
show isis [*tag*] **frr** *ipv4-net-address/mask*	Displays the IS-IS IP FRR routing information.
show isis [*tag*] **graceful-restart**	Displays the state information related to IS-IS GR.
show isis [*tag*] **hostname**	Displays the relationship between the device name and system ID.
show isis [*tag*] **interface** [*interface-type interface-number*] [*counter*]	Displays the details of an IS-IS interface.
show isis [*tag*] **mesh-groups**	Displays the mesh group configuration of different interfaces.
show isis [*tag*] **neighbors** [**detail**]	Displays IS-IS neighbor information.
show isis [*tag*] **nsr**	Displays IS-IS NSR information.
show isis [*tag*] **virtual-neighbors**	Displays the neighbor information of virtual systems in IS-IS.
show isis [*tag*] **protocol**	Displays the protocol information of IS-IS.
show isis [*tag*] **topology** [**frr** { **self-originate** | *WORD* | **all** }] [**l1** | **l2** | **level-1** | **level-2**]	Displays the topology of IS-IS device connection.
show isis [*tag*] **ipv6 topology** [**l1** | **l2** | **level-1** | **level-2**]	Displays IS-IS IPv6 unicast topology information of IS-IS.
debug isis { **all** | **auth | events** | **frr** | **gr** | **ifsm** | **lsp** | **mtr** | **nfsm** | **nsm** | **nsr** | **pdu** | **distribute**| **mom** | **spf** | **warn** }	Enables IS-IS debugging.

1.26 Configuration Examples

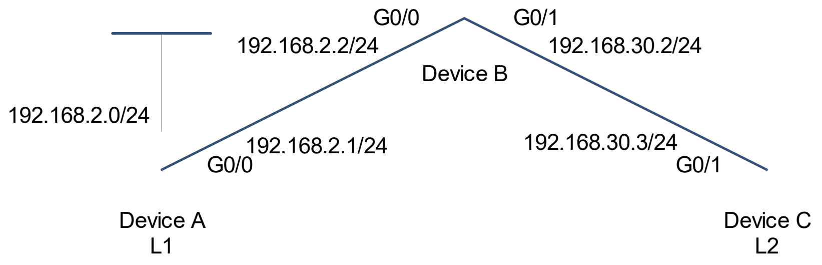
1.26.1 Performing Basic Authentication Configuration of IS-IS

1. Requirements

Devices A, B, and C are connected through the Ethernet and run IS-IS. Device A is a Level-1 device, Device B is a Level-1/Level-2 device, and Device C is a Level-2 device. The following configuration requirements exist: Plaintext authentication is applied to the Hello packets between Device A and Device B, as well as Level-1 LSPs and SNPs. MD5 authentication is applied to the Hello packets between Router B and Router C, as well as Level-2 LSPs and SNPs.

2. Topology

Figure 1-1Topology of Basic Authentication Configuration of IS-IS



3. Notes

- Configure a key string.
- Configure IS-IS area authentication and interface authentication.

4. Procedure

(1) Configure IP addresses for interfaces.

Configure Device A.

```
Device A> enable
Device A# configure terminal
Device A(config)# interface gigabitethernet 0/0
Device A(config-if-GigabitEthernet 0/0)# ip address 192.168.20.1 255.255.255.0
Device A(config-if)# exit
```

Configure Device B.

```
Device B> enable
Device B# configure terminal
Device B(config)# interface gigabitethernet 0/0
Device B(config-if-GigabitEthernet 0/0)# ip address 192.168.20.2 255.255.255.0
Device B(config-if-GigabitEthernet 0/0)# exit
Device B(config)# interface gigabitethernet 0/1
Device B(config-if-GigabitEthernet 0/1)# ip address 192.168.30.2 255.255.255.0
Device B(config-if-GigabitEthernet 0/1)# exit
```

Configure Device C.

```
Device C> enable
Device C# configure terminal
Device C(config)# interface gigabitethernet 0/1
Device C(config-if-GigabitEthernet 0/1)# ip address 192.168.30.3 255.255.255.0
Device C(config-if-GigabitEthernet 0/1)# exit
```

(2) Perform basic configuration of IS-IS.

Configure Device A.

```
Device A(config)# router isis
Device A(config-router)# net 49.0001.0000.0000.0001.00
Device A(config-router)# is-type level-1
Device A(config-router)# exit
Device A(config)# interface gigabitethernet 0/0
Device A(config-if-GigabitEthernet 0/0)# ip router isis
```

Configure Device B.

```
Device B(config)# router isis
Device B(config-router)# net 49.0001.0000.0000.0002.00
Device B(config-router)# exit
Device B(config)# interface gigabitethernet 0/0
Device B(config-if-GigabitEthernet 0/0# ip router isis
Device B(config-if-GigabitEthernet 0/0)# exit
Device B(config)# interface gigabitethernet 0/1
Device B(config-if-GigabitEthernet 0/1)# ip router isis
Device B(config-if-GigabitEthernet 0/1)# exit
```

Configure Device C.

```
Device C(config)# router isis
Device C(config-router)# net 49.0002.0000.0000.0003.00
Device C(config-router)# is-type level-2
Device C(config-router)# exit
Device C(config)# interface gigabitethernet 0/1
Device C(config-if-GigabitEthernet 0/1)# ip router isis
Device C(config-if-GigabitEthernet 0/1)# exit
```

(3) Enable IS-IS authentication.

Set the area authentication password of Device A to **aa**, and set the interface authentication password of GigabitEthernet 0/0 to **cc**.

```
Device A(config)# router isis
Device A(config-router)# area-password aa
Device A(config-router)# exit
Device A(config)# interface gigabitethernet 0/0
Device A(config-if-GigabitEthernet 0/0)# isis password cc
```

Configure Device B with Level-1 area plaintext authentication and set the key string to **kc1**; configure Level-2 area plaintext authentication and set the key string to kc**2**. Configure Device A with interface plaintext authentication and set the key string to **kc3**. Configure Device C with interface MD5 authentication and set the key string to **kc3**.

```
Device B(config)# key chain kc1
Device B(config-keychain)# key 1
Device B(config-keychain-key)# key-string aa
Device B(config-keychain-key)# exit
Device B(config-keychain)# exit
Device B(config)# key chain kc2
Device B(config-keychain)# key 1
Device B(config-keychain-key)# key-string bb
Device B(config-keychain-key)# exit
Device B(config-keychain)# exit
Device B(config)# key chain kc3
Device B(config-keychain)# key 1
Device B(config-keychain-key)# key-string cc
Device B(config-keychain-key)# exit
Device B(config-keychain)# exit
Device B(config)# router isis
Device B(config-router)# authentication mode text level-1
Device B(config-router)# authentication key-chain kc1 level-1
Device B(config-router)# authentication mode md5 level-2
Device B(config-router)# authentication key-chain kc2 level-2
Device B(config-router)# exit
Device B(config)# interface gigabitethernet 0/0
Device B(config-if-GigabitEthernet 0/0)# isis authentication mode text
Device B(config-if-GigabitEthernet 0/0)# isis authentication key-chain kc3
Device B(config-if-GigabitEthernet 0/0)# exit
Device B(config)# interface gigabitethernet 0/1
Device B(config-if-GigabitEthernet 0/1)# isis authentication mode md5
Device B(config-if-GigabitEthernet 0/1)# isis authentication key-chain kc3
```

Configure Device C with Level-2 area MD5 authentication and set the key string to **kc2**. Configure Device B with interface MD5 authentication and set the key string to **kc3**.

```
Device C(config)# key chain kc2
Device C(config-keychain)# key 1
Device C(config-keychain-key)# key-string bb
Device C(config-keychain-key)# exit
Device C(config-keychain)# exit
Device C(config)# key chain kc3
Device C(config-keychain)# key 1
Device C(config-keychain-key)# key-string cc
Device C(config-keychain-key)# exit
Device C(config-keychain)# exit
Device C(config)# router isis
Device C(config-router)# authentication mode md5 level-2
Device C(config-router)# authentication key-chain kc2
Device C(config)# interface gigabitethernet 0/1
Device C(config-if-GigabitEthernet 0/1)# isis authentication mode md5
Device C(config-if-GigabitEthernet 0/1)# isis authentication key-chain kc3
```

5. Verification

Check the neighbor information of Device A.

```
Device A# show isis neighbors
Area (null):
System Id       Type  IP Address        State   Holdtime  Circuit
Interface
```

```
B               L1    192.168.20.2      Up      28        A.01
GigabitEthernet 0/0
```

Check the IS-IS database information of Device A.

```
Device A# show isis database detail
Area (null):
IS-IS Level-1 Link State Database:
LSPID                  LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
A.00-00             *  0x00000011   0xBE84        918               0/0/1
  Auth: TEXT(aa) Length: 3
  Area Address: 49.0001
  NLPID:        0xCC
  Hostname:     A
  IP Address:   192.168.20.1
  Metric:   1          IS A.01
  Metric:   1          IP 192.168.20.0 255.255.255.0
A.01-00             *  0x0000000A   0xF80A        918               0/0/0
  Auth: TEXT(aa) Length: 3
  Metric:   0          IS A.00
  Metric:   0          IS B.00
B.00-00                0x00000013   0xF62B        1129              1/0/0
  Auth: TEXT(aa) Length: 3
  Area Address: 49.0001
  NLPID:        0xCC
  Hostname:     B
  IP Address:   192.168.20.2
  Metric:   1          IS A.01
  Metric:   1          IP 192.168.20.0 255.255.255.0
  Metric:   1          IP 192.168.30.0 255.255.255.0
```

Check the neighbor information of Device B.

```
Device B# show isis neighbors
Area (null):
System Id       Type  IP Address        State   Holdtime  Circuit
Interface
C               L2    192.168.30.3      Up      21        B.02
GigabitEthernet 0/1
A               L1    192.168.20.1      Up      8         A.01
GigabitEthernet 0/0
```

Check the neighbor information of Device C.

```
Device C# show isis neighbors
Area (null):
System Id       Type  IP Address        State   Holdtime  Circuit
Interface
B               L2    192.168.30.2      Up      9         B.02
GigabitEthernet 0/0
```

6. Configuration Files

- Device A configuration file

```
!
router isis
 net 49.0001.0000.0000.0001.00
 is-type level-1
 area-password aa
!
interface gigabitethernet 0/0
 ip address 192.168.20.1 255.255.255.0
 ip router isis
 isis password cc
!
```

- Device B configuration file

```
!
key chain kc1
 key 1
  key-string aa
key chain kc2
 key 1
  key-string bb
key chain kc3
 key 1
  key-string cc
!
router isis
 net 49.0001.0000.0000.0002.00
 authentication mode text level-1
 authentication key-chain kc1 level-1
 authentication mode md5 level-2
 authentication key-chain kc2 level-2
!
interface gigabitethernet 0/0
 ip address 192.168.20.2 255.255.255.0
 ip router isis
 isis authentication mode text
 isis authentication key-chain kc3
!
interface gigabitethernet 0/1
 ip address 192.168.30.2 255.255.255.0
 ip router isis
 isis authentication mode md5
 isis authentication key-chain kc3
!
```

- Device C configuration file

```
!
key chain kc2
 key 1
  key-string bb
!
key chain kc3
 key 1
  key-string cc
!
router isis
 net 49.0002.0000.0000.0003.00
 is-type level-2
 authentication mode md5 level-2
 authentication key-chain kc2
!
interface gigabitethernet 0/1
 ip address 192.168.30.3 255.255.255.0
 ip router isis
 isis authentication mode md5
 isis authentication key-chain kc3
!
```

7. Common Errors

- Different authentication passwords are configured between neighbors.
- Different authentication modes are configured between neighbors.

1.26.2 Configuring IS-IS MTR

1. Requirements

The typical application scenario of MTR is to retain devices that only support IPv4 services in a network where IPv6 service extension will be performed.

As shown in Figure 1-1, Device B only supports the IPv4 protocol stack but does not support the MTR feature; therefore, it can only run IPv4 services. The network capacity needs to be scaled to support IPv6 services in order to meet service extension requirements. (Devices A, C, and D that support the MTR feature will be added.) Device B that supports only one protocol stack must be replaced to maintain the stability of the network running IPv4 and IPv6 dual protocol stacks; otherwise, IPv6 routing black holes may occur.

If you need to retain Device B, you can configure the MTR feature on the new devices. The MTR feature enables Device B to continue to run IPv4 services without interference on the IPv4 and IPv6 services on the new devices. The MTR feature improves networking flexibility, indirectly prolongs the service life of old devices, and meets service extension requirements while maximizing the values of old devices.

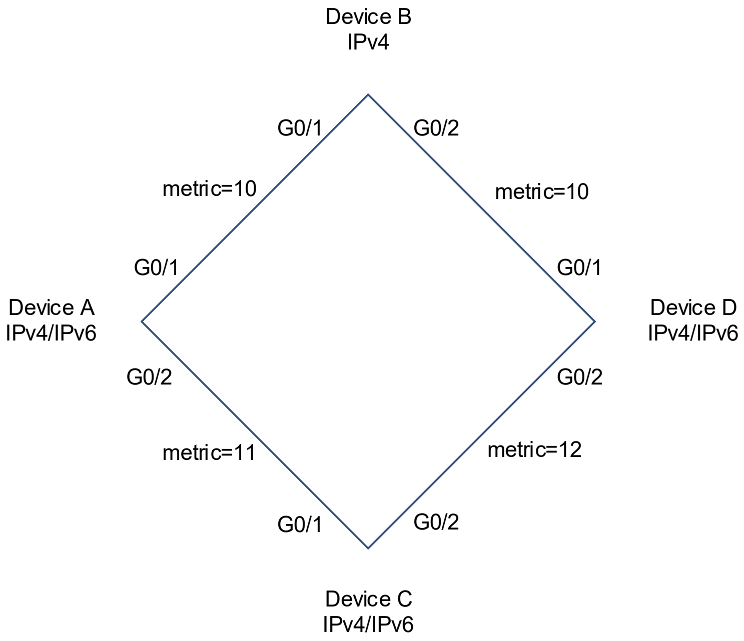
The configuration requirements are as follows:

- Retain Device B, which only supports IPv4 services.

- Add devices that support IPv4 and IPv6 dual protocol stacks, and separate IPv4 route calculation and IPv6 route calculation.

2. Topology

Figure 1-1Topology of IS-IS MTR Configuration



3. Notes

- Perform basic configuration of IS-IS.
- Enable the MTR function.

4. Procedure

- Configure Device A.

Configure IS-IS, set the metric type to Wide, and enable the MTR function.

```
Device A> enable
Device A# configure terminal
Device A(config)# router isis
Device A(config-router)# net 49.0001. 0000.0000.0001.00
Device A(config-router)# is-type level-1
Device A(config-router)# metric-style wide
Device A(config-router)# address-family ipv6
Device A(config-router-af)# multi-topology
Device A(config-router-af)# exit
Device A(config-router)# exit
```

Configure an IP address for the interface and add the interface to IS-IS.

```
Device A(config)# interface gigabitethernet 0/1
Device A(config-if-GigabitEthernet 0/1)# ipv6 enable
Device A(config-if-GigabitEthernet 0/1)# ipv6 address 1002::1/112
Device A(config-if-GigabitEthernet 0/1)# ipv6 router isis
Device A(config-if-GigabitEthernet 0/1)# ip address 192.168.1.1 255.255.255.0
Device A(config-if-GigabitEthernet 0/1)# ip router isis
Device A(config-if-GigabitEthernet 0/1)# exit
Device A(config)# interface gigabitethernet 0/2
Device A(config-if-GigabitEthernet 0/2)# ipv6 enable
Device A(config-if-GigabitEthernet 0/2)# ipv6 address 1003::1/112
Device A(config-if-GigabitEthernet 0/2)# ipv6 router isis
Device A(config-if-GigabitEthernet 0/2)# ip address 192.168.2.1 255.255.255.0
Device A(config-if-GigabitEthernet 0/2)# ip router isis
Device A(config-if-GigabitEthernet 0/2)#isis wide-metric 11
```

- Configure Device B.

Configure IS-IS, set the metric type to Wide, and enable the MTR function.

```
Device B> enable
Device B# configure terminal
Device B(config)# router isis
Device B(config-router)# net 49.0001. 0000.0000.0002.00
Device B(config-router)# is-type level-1
Device B(config-router)# metric-style wide
Device B(config-router)# address-family ipv6
Device B(config-router-af)# no adjacency-check
Device B(config-router-af)# exit
Device B(config-router)# exit
```

Configure an IP address for the interface and add the interface to IS-IS.

```
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)# ip router isis
Device B(config-if-GigabitEthernet 0/1)# exit
Device B(config)# interface gigabitethernet 0/2
Device B(config-if-GigabitEthernet 0/2)# ip address 192.168.3.2 255.255.255.0
Device B(config-if-GigabitEthernet 0/2)# ip router isis
```

- Configure Device C.

Configure IS-IS, set the metric type to Wide, and enable the MTR function.

```
Device C> enable
Device C# configure terminal
Device C(config)# router isis
Device C(config-router)# net 49.0001. 0000.0000.0003.00
Device C(config-router)# is-type level-1
Device C(config-router)# metric-style wide
Device C(config-router)# address-family ipv6
Device C(config-router-af)# multi-topology
Device C(config-router-af)# exit
Device C(config-router)# exit
```

Configure an IP address for the interface and add the interface to IS-IS.

```
Device C(config)# interface gigabitethernet 0/1
Device C(config-if-GigabitEthernet 0/1)# ipv6 enable
Device C(config-if-GigabitEthernet 0/1)# ipv6 address 3001::1/112
Device C(config-if-GigabitEthernet 0/1)# ipv6 router isis
Device C(config-if-GigabitEthernet 0/1)# ip address 192.168.2.3 255.255.255.0
Device C(config-if-GigabitEthernet 0/1)# ip router isis
Device C(config-if-GigabitEthernet 0/1)#isis wide-metric 11
Device C(config-if-GigabitEthernet 0/1)# exit
Device C(config)# interface gigabitethernet 0/2
Device C(config-if-GigabitEthernet 0/2)# ipv6 enable
Device C(config-if-GigabitEthernet 0/2)# ipv6 address 3004::1/112
Device C(config-if-GigabitEthernet 0/2)# ipv6 router isis
Device C(config-if-GigabitEthernet 0/2)# ip address 192.168.4.3 255.255.255.0
Device C(config-if-GigabitEthernet 0/2)# ip router isis
Device C(config-if-GigabitEthernet 0/2)# isis wide-metric 12
```

- Configure Device D.

Configure IS-IS, set the metric type to Wide, and enable the MTR function.

```
Device D> enable
Device D# configure terminal
Device D(config)# router isis
Device D(config-router)# net 49.0001.0000.0000.0004.00
Device D(config-router)# is-type level-1
Device D(config-router)# metric-style wide
Device D(config-router)# address-family ipv6
Device D(config-router-af)# multi-topology
Device D(config-router-af)# exit
Device D(config-router)# exit
```

Configure an IP address for the interface and add the interface to IS-IS.

```
Device D(config)# interface gigabitethernet 0/1
Device D(config-if-GigabitEthernet 0/1)# ipv6 enable
Device D(config-if-GigabitEthernet 0/1)# ipv6 address 4002::1/112
Device D(config-if-GigabitEthernet 0/1)# ipv6 router isis
Device D(config-if-GigabitEthernet 0/1)# ip address 192.168.3.4 255.255.255.0
Device D(config-if-GigabitEthernet 0/1)# ip router isis
Device D(config-if-GigabitEthernet 0/1)# exit
Device D(config)# interface gigabitethernet 0/2
Device D(config-if-GigabitEthernet 0/2)# ipv6 enable
Device D(config-if-GigabitEthernet 0/2)# ipv6 address 4003::1/112
Device D(config-if-GigabitEthernet 0/2)# ipv6 router isis
Device D(config-if-GigabitEthernet 0/2)# ip address 192.168.4.4 255.255.255.0
Device D(config-if-GigabitEthernet 0/2)# ip router isis
```

5. Verification

Run the **show** command on Device A to view IPv4 route information and check whether the next hop of the IPv4 route destined for Device D is Device B.

```
Device A# show ip route
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    192.168.1.0/24 is directly connected, GigabitEthernet 0/1
C    192.168.1.1/32 is local host.
C    192.168.2.0/24 is directly connected, GigabitEthernet 0/2
C    192.168.2.1/32 is local host.
i L1 192.168.3.0/24 [115/20] via 192.168.1.2, 00:13:14, GigabitEthernet 0/1
i L1 192.168.4.0/24 [115/23] via 192.168.2.3, 00:02:40, GigabitEthernet 0/2
```

Run the **show** command on Device A to view IPv6 route information and check whether the next hop of the IPv6 route destined for Device D is Device C.

```
Device A# show ipv6 route
IPv6 routing table name is - Default - 16 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra area, OI - OSPF inter area,  OE1 - OSPF external type 1,
OE2 - OSPF external type 2
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
L      ::1/128 via Loopback, local host
C      1002::/112 via GigabitEthernet 0/1, directly connected
L      1002::1/128 via GigabitEthernet 0/1, local host
C      1003::/112 via GigabitEthernet 0/2, directly connected
L      1003::1/128 via GigabitEthernet 0/2, local host
I1     3001::/112 [115/21] via FE80::C806:5FF:FEE8:38, GigabitEthernet 0/2
I1     3004::/112 [115/21] via FE80::C806:5FF:FEE8:38, GigabitEthernet 0/2
I1     4002::/112 [115/31] via FE80::C806:5FF:FEE8:38, GigabitEthernet 0/2
I1     4003::/112 [115/31] via FE80::C806:5FF:FEE8:38, GigabitEthernet 0/2
L      FE80::/10 via ::1, Null0
C      FE80::/64 via GigabitEthernet 0/2, directly connected
L      FE80::1614:4BFF:FE12:ADFC/128 via GigabitEthernet 0/2, local host
C      FE80::/64 via GigabitEthernet 0/1, directly connected
L      FE80::1614:4BFF:FE12:ADFD/128 via GigabitEthernet 0/1, local host
C      FE80::/64 via Local 0, directly connected
L      FE80::1614:4BFF:FE12:ADFC/128 via Local 0, local host
```

6. Configuration Files

Device A configuration file

```
!
router isis
 net 49.0001. 0000.0000.0001.00
 is-type level-1
 metric-style wide
 address-family ipv6
  multi-topology
!
interface gigabitethernet 0/1
 ipv6 enable
 ipv6 address 1002::1/112
 ipv6 router isis
 ip address 192.168.1.1 255.255.255.0
 ip router isis
!
interface gigabitethernet 0/2
 ipv6 enable
 ipv6 address 1003::1/112
 ipv6 router isis
 ip address 192.168.2.1 255.255.255.0
 ip router isis
 isis wide-metric 11
!
```

Device B configuration file

```
!
router isis
 net 49.0001. 0000.0000.0002.00
 is-type level-1
 metric-style wide
 address-family ipv6
  no adjacency-check
!
 interface gigabitethernet 0/1
 ip address 192.168.1.2 255.255.255.0
 ip router isis
!
interface gigabitethernet 0/2
 ip address 192.168.3.2 255.255.255.0
 ip router isis
!
```

Device C configuration file

```
!
router isis
 net 49.0001. 0000.0000.0003.00
 is-type level-1
 metric-style wide
 address-family ipv6
  multi-topology
!
 interface gigabitethernet 0/1
 ipv6 enable
 ipv6 address 3001::1/112
 ipv6 router isis
 ip address 192.168.2.3 255.255.255.0
 ip router isis
 isis wide-metric 11
!
interface gigabitethernet 0/2
 ipv6 enable
 ipv6 address 3004::1/112
 ipv6 router isis
 ip address 192.168.4.3 255.255.255.0
 ip router isis
 isis wide-metric 12
!
```

Device D configuration file

```
!
router isis
 net 49.0001.0000.0000.0004.00
 is-type level-1
 metric-style wide
 address-family ipv6
  multi-topology
!
interface gigabitethernet 0/1
 ipv6 enable
 ipv6 address 4002::1/112
 ipv6 router isis
 ip address 192.168.3.4 255.255.255.0
 ip router isis
!
interface gigabitethernet 0/2
 ipv6 enable
 ipv6 address 4003::1/112
 ipv6 router isis
 ip address 192.168.4.4 255.255.255.0
 ip router isis
!
```

7. Common Errors

- The metric-style is not set to **Wide** or **Transition**.

- The protocol types used by two neighbors do not match; therefore, a neighbor relationship cannot be established.
- The IP addresses of the interfaces connected between neighbors are not in the same network segment.
- The **ip router isis** command is not executed on interfaces.
- No NET address is configured, or different NET addresses exist at Level-1.
- max-area-addresses is configured differently on both sides.
- metric-style is configured differently on both sides.
- The interface Levels on both sides are different. One side is Level-1, whereas the other side is Level-2.
- One side is configured with the P2P mode, whereas the other side is configured with the broadcast mode.
- One side is enabled with authentication, whereas the other side is not.

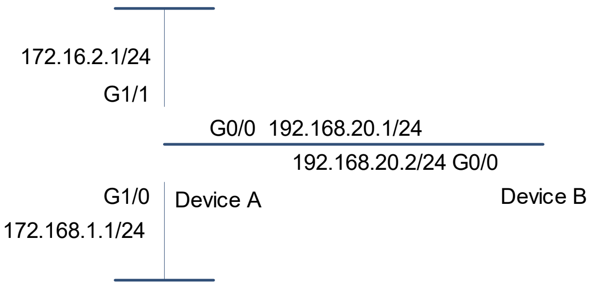
1.26.3 Configuring IS-IS Route Summarization

1. Requirements

Device A and Device B are connected through the Ethernet and run IS-IS. Device A is configured to advertise only the 172.16.0.0/22 route instead of the 172.16.1.0/24 and 172.16.2.0/24 routes.

2. Topology

Figure 1-1Topology of IS-IS Route Summarization



3. Notes

- Configure IS-IS.
- Configure route summarization.

4. Procedure

(1) Configure IS-IS.

Configure Device A.

```
Device A> enable
Device A# configure terminal
Device A(config)# router isis
Device A(config-router)# net 49.0001.0000.0000.0001.00
Device A(config-router)# exit
Device A(config)# interface gigabitethernet 0/0
Device A(config-if)# ip address 192.168.20.1 255.255.255.0
Device A(config-if)# ip router isis
Device A(config)# interface gigabitethernet 1/0
Device A(config-if)# ip address 172.16.1.1 255.255.255.0
Device A(config-if)# ip router isis
Device A(config)# interface gigabitethernet 1/1
Device A(config-if)# ip address 172.16.2.1 255.255.255.0
Device A(config-if)# ip router isis
Device A(config-if)# exit
```

Configure Device B.

```
Device B> enable
Device B# configure terminal
Device B(config)# router isis
Device B(config-router)# net 49.0001.0000.0000.0002.00
Device B(config-router)# exit
Device B(config)# interface gigabitethernet 0/0
Device B(config-if)# ip address 192.168.20.2 255.255.255.0
Device B(config-if)# ip router isis
```

(2) Configure route summarization.

Configure Device A.

```
Device A(config)# router isis
Device A(config-router)# summary-address 172.16.0.0/16 level-1-2
```

5. Verification

Run the **show ip route** command on Device B to check whether only one summary route exists.

```
Device B# show ip route
i L1    172.16.0.0/16 [115/20]  via 192.168.20.1, FastEthernet0/0
```

6. Configuration Files

- Device A configuration file

```
!
router isis
 net 49.0001.0000.0000.0001.00
 summary-address 172.16.0.0/16 level-1-2
!
interface gigabitethernet 0/0
 ip address 192.168.20.1 255.255.255.0
 ip router isis
!
interface gigabitethernet 1/0
 ip address 172.16.1.1 255.255.255.0
 ip router isis
```

```
!
interface gigabitethernet 1/1
 ip address 172.16.2.1 255.255.255.0
 ip router isis
!
```

- Device B configuration file

```
!
router isis
 net 49.0001.0000.0000.0002.00
!
interface gigabitethernet 0/0
 ip address 192.168.20.2 255.255.255.0
 ip router isis
!
```

1.26.4 Correlating IS-IS with BFD

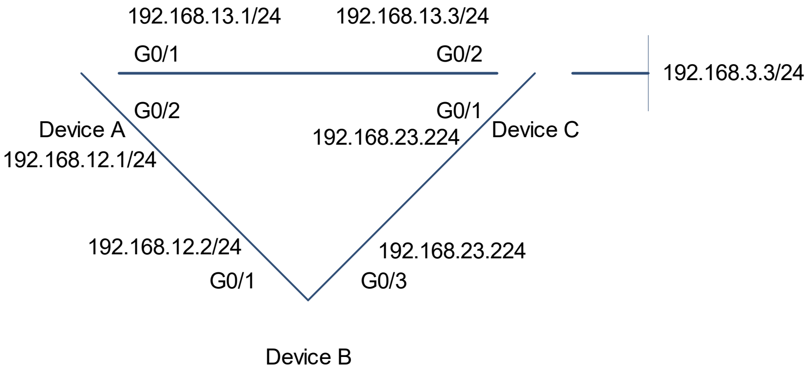
1. Requirements

Devices A, B, C, and D are interconnected through IS-IS routing protocol. The devices are Level-2 devices.

When a link from Device A to Device C fails, services can be quickly switched to Device B.

2. Topology

Figure 1-1Topology for IS-IS Correlation with BFD



3. Notes

- Configure interface IP addresses for all the devices.
- Configure the basic IS-IS functions on all devices.
- Enable the BFD function in the IS-IS routing process mode.

4. Procedure

(1) Configure interface IP addresses and perform basic configuration of IS-IS.

Configure Device A.

```
Device A> enable
Device A# configure terminal
Device A(config)# interface gigabitethernet 0/2
Device A(config-if-GigabitEthernet 0/2)# ip address 192.168.12.1/24
Device A(config-if-GigabitEthernet 0/2)# ip router isis
Device A(config-if-GigabitEthernet 0/2)# exit
Device A(config)# interface gigabitethernet 0/1
Device A(config-if-GigabitEthernet 0/1)# ip address 192.168.13.1/24
Device A(config-if-GigabitEthernet 0/1)# ip router isis
Device A(config-if-GigabitEthernet 0/1)# exit
Device A(config)# router isis
Device A(config-router)# net 49.0001.0000.0000.0001.00
Device A(config-router)# is-type level-2-only
```

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 192.168.12.2/24
Device B(config-if-GigabitEthernet 0/1)# ip router isis
Device B(config-if-GigabitEthernet 0/1)# exit
Device B(config)# interface gigabitethernet 0/3
Device B(config-if-GigabitEthernet 0/3)# ip address 192.168.23.2/24
Device B(config-if-GigabitEthernet 0/3)# ip router isis
Device B(config-if-GigabitEthernet 0/3)# exit
Device B(config)# router isis
Device B(config-router)# net 49.0001.0000.0000.0002.00
Device B(config-router)# is-type level-2-only
```

Configure Device C.

```
Device C> enable
Device C# configure terminal
Device C(config)# interface gigabitethernet 0/2
Device C(config-if-GigabitEthernet 0/2)# ip address 192.168.13.3/24
Device C(config-if-GigabitEthernet 0/2)# ip router isis
Device C(config-if-GigabitEthernet 0/2)# exit
Device C(config)# interface gigabitethernet 0/1
Device C(config-if-GigabitEthernet 0/1)# ip address 192.168.23.3/24
Device C(config-if-GigabitEthernet 0/1)# ip router isis
Device C(config-if-GigabitEthernet 0/1)# exit
Device C(config)# router isis
Device C(config-router)# net 49.0001.0000.0000.0003.00
Device C(config-router)# is-type level-2-only
```

(2) Correlate IS-IS with BFD globally.

Configure Device A.

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

Configure Device B.

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

Configure Device C.

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

5. Verification

- Normal network environment

Check the routing table of Device A.

```
Device A# show ip route isis
I L2  192.168.23.0/24 [115/2] via 192.168.13.3, 00:19:07, GigabitEthernet 0/1
                      [115/2] via 192.168.12.2, 00:19:07, GigabitEthernet 0/2
I L2  192.168.33.0/24 [115/1] via 192.168.13.3, 00:17:40, GigabitEthernet 0/1
```

Run **traceroute 192.168.3.3** on Device A.

```
Device A# traceroute 192.168.3.3
  < press Ctrl+C to break >
Tracing the route to 192.168.3.3

 1       192.168.3.3     <1 msec    5 msec    9 msec
```

- Link from Device A to Device C fails

Check the routing table of Device A.

```
Device A# show ip route isis
I L2  192.168.23.0/24 [115/2] via 192.168.12.2, 00:00:08, GigabitEthernet 0/2
I L2  192.168.33.0/24 [115/2] via 192.168.12.2, 00:00:08, GigabitEthernet 0/2
```

Run **traceroute 192.168.3.3** on Device A.

```
Device A# traceroute 192.168.3.3
  < press Ctrl+C to break >
Tracing the route to 192.168.3.3

 1       192.168.12.2      9 msec    8 msec   13 msec
 2       192.168.3.3      8 msec   10 msec    9 msec
```

6. Configuration Files

- Device A configuration file

```
!
interface gigabitethernet 0/2
 ip address 192.168.12.1/24
 ip router isis
!
interface gigabitethernet 0/1
 ip address 192.168.13.1/24
 ip router isis
```

```
!
router isis
 net 49.0001.0000.0000.0001.00
 is-type level-2-only
!
```

- Device B configuration file

```
!
interface gigabitethernet 0/1
 ip address 192.168.12.2/24
 ip router isis
!
interface gigabitethernet 0/3
 ip address 192.168.23.2/24
 ip router isis
!
router isis
 net 49.0001.0000.0000.0002.00
 is-type level-2-only
!
```

- Device C configuration file

```
!
interface gigabitethernet 0/2
 ip address 192.168.13.3/24
 ip router isis
!
interface gigabitethernet 0/1
 ip address 192.168.23.3/24
 ip router isis
!
router isis
 net 49.0001.0000.0000.0003.00
 is-type level-2-only
!
```