

1 IS-IS Commands

Command	Function
address-family ipv6	Enter the IS-IS IPv6 address family configuration mode.
adjacency-check	Enable the neighbor supported protocol detection function in Hello packets.
area-password	Configure plaintext authentication password of Level-1 areas.
authentication key-chain	Configure a key chain for IS-IS authentication.
authentication mode	Enable an IS-IS authentication mode.
authentication send-only	Apply a specified IS-IS authentication mode to only sent packets. Received packets are not authenticated.
bandwidth-reference	Configure the reference bandwidth value of IS-IS.
bfd all-interfaces	Enable BFD for IS-IS interfaces.
clear clns neighbors	Clear all neighbor relationship tables of IS-IS.
clear isis *	Clear all data structures of IS-IS.
clear isis counter	Clear statistical information of IS-IS.
default-information originate	Generate a default route and advertise the route in LSPs.
distance	Configure the administrative distance of an IS-IS route.
domain-password	Configure plaintext authentication password of Level-2 areas.
enable mib-binding	Bind an IS-IS instance for SNMP operation.
enable traps	Enable the trap message sending function of IS-IS.
exit-address-family	Exit the IS-IS IPv6 address family configuration mode and go back to the IS-IS routing process configuration mode.
graceful-restart	Enable the GR capability of IS-IS.

<u>graceful-restart grace-period</u>	Configure the maximum GR interval of a device.
<u>graceful-restart helper disable</u>	Disable the IS-IS GR Helper capability.
<u>hello padding</u>	Enable padding specified IS-IS Hello packets.
<u>hostname dynamic</u>	Replace the system ID of a device with the host name of the destination device.
<u>ignore-lsp-errors</u>	Ignore LSP checksum errors.
<u>interfaces-protocol-compatible</u>	Pad the TLV field of the IS-IS protocol based on protocols supported by an interface.
<u>ip router isis</u>	Enable the IPv4 IS-IS routing function on an interface.
<u>ipv6 router isis</u>	Enable the IPv6 IS-IS routing function on an interface.
<u>isis authentication key-chain</u>	Configure a key chain for IS-IS interface authentication.
<u>isis authentication mode</u>	Enable an authentication mode of an IS-IS interface.
<u>isis authentication send-only</u>	Apply a specified IS-IS interface authentication mode to only sent packets. Received packets are not authenticated.
<u>isis bfd</u>	Enable IS-IS correlation with BFD on an interface.
<u>isis circuit-type</u>	Configure an IS-IS level on an interface.
<u>isis csnp-interval</u>	Specify the CSNP broadcast interval on an IS-IS interface.
<u>isis hello padding</u>	Enable padding IS-IS hello packets sent on an IS-IS interface.
<u>isis hello-interval</u>	Configure the hello packet sending interval on an interface.
<u>isis hello-multiplier</u>	Configure the multiplier of the hello holdtime on an interface.
<u>isis lsp-flood</u>	Configure the maximum number of LSP packets sent by the IS-IS interface at a time.
<u>isis lsp-interval</u>	Configure the LSP sending interval on an interface.
<u>isis mesh-group</u>	Add an IS-IS interface to a specified mesh group.
<u>isis metric</u>	Configure the metric for an IS-IS interface.

isis network point-to-point	Change the type of an interface from broadcast to P2P.
isis passive	Configure an interface as a passive interface.
isis password	Configure the password for plaintext authentication of hello packets on an interface.
isis priority	Configure the priority for DIS election in a LAN.
isis psnp-interval	Configure the minimum PSNP sending interval.
isis retransmit-interval	Configure the LSP retransmission interval on an IS-IS interface.
isis subvlan	Enable the IS-IS function in a super VLAN.
isis suppress on-neighbor-up	Suppress routing calculation after an IS-IS neighbor is up.
isis three-way-handshake disable	Disable three-way handshake of a P2P network.
isis wide-metric	Configure the wide metric value for an interface.
is-name	Replace the system ID of an instance with the configured name.
is-type	Specify the level at which IS-IS runs.
log-adjacency-changes	Record neighbor state changes of IS-IS without enabling the debug command.
lsp-fragments-extend	Enable fragment extension.
lsp-gen-interval	Configure an exponential backoff algorithm of LSP generation.
lsp-length originate	Configure the maximum length of sent LSPs.
lsp-length receive	Configure the maximum length of received LSPs.
lsp-refresh-interval	Configure the LSP refresh interval.
max-area-addresses	Configure the maximum number of area addresses.
maximum-paths	Configure the maximum number of IS-IS equal-cost paths to be added to a routing table.
max-lsp-lifetime	Configure the maximum LSP lifetime.
max-metric on-neighbor-up	Configure the maximum metric for the directly-connected routes after the first neighbor is up.
metric-style	Configure a metric type.

<u>min-lsp-arrival</u>	Configure the delay for receiving duplicate LSPs.
<u>multi-topology</u>	Configure IS-IS to support IPv6 unicast topologies. After that, IPv4 and IPv6 unicast routes in IS-IS will be calculated based on different topologies.
<u>net</u>	Configure a NET address in IS-IS.
<u>nsr</u>	Enable the NSR function for current IS-IS instance.
<u>passive-interface</u>	Configure a passive interface.
<u>redistribute</u>	Redistribute other routes to IS-IS.
<u>redistribute isis level-1 into level-2</u>	Redistribute the Level-1 reachable routing information of the specified IS-IS instance to Level-2 of the current instance.
<u>redistribute isis level-2 into level-1</u>	Redistribute the Level-2 reachable routing information of the specified IS-IS instance to Level-1 of the current instance.
<u>router isis</u>	Create an IS-IS instance.
<u>set-overload-bit</u>	Prevent neighbors from using the local IS-IS node as a forwarding device to forward data.
<u>show clns is-neighbors</u>	Display all IS-IS neighbors and provide device adjacency relationship information.
<u>show clns neighbors</u>	Display all IS-IS neighbors and provide device information and adjacency relationship information about terminals.
<u>show isis counter</u>	Display statistical information of IS-IS.
<u>show isis database</u>	Display the information of an LSP database.
<u>show isis graceful-restart</u>	Display the state information about IS-IS GR.
<u>show isis hostname</u>	Display the mapping of a host name to a system ID.
<u>show isis interface</u>	Display details of an IS-IS interface.
<u>show isis ipv6 topology</u>	Display the IPv6 unicast topology information of an IS-IS device.
<u>show isis mesh-groups</u>	Display the mesh group configuration of interfaces.
<u>show isis neighbors</u>	Display neighbor information of IS-IS.
<u>show isis nsr</u>	Display NSR information of IS-IS.
<u>show isis protocol</u>	Display protocol information of IS-IS.

<u>show isis topology</u>	Display the topology information of connected IS-IS devices.
<u>show isis virtual-neighbors</u>	Display virtual system neighbor information of IS-IS.
<u>spf-interval</u>	Configure the exponential backoff algorithm of SPF calculation.
<u>summary-address</u>	Configure IPv4 summarized routes.
<u>summary-prefix</u>	Configure IPv6 summarized routes.
<u>two-way-maintain</u>	Enable the two-way maintenance function of IS-IS.
<u>virtual-system</u>	Configure an additional system ID for fragment extension.
<u>vrf</u>	Bind an IS-IS instance to a VRF table.

1.1 address-family ipv6

Function

Run the **address-family ipv6** command to enter the IS-IS IPv6 address family configuration mode.

Run the **no** form of this command to remove this configuration.

A device does not enter the IPv6 address family configuration mode by default.

Syntax

```
address-family ipv6 [ unicast ]
```

```
no address-family ipv6 [ unicast ]
```

Parameter Description

unicast: Specifies to use the IPv6 unicast address prefix of the IPv6 address family. This parameter is optional and does not make any difference no matter whether it is configured.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

Run this command to enter the IS-IS IPv6 address family configuration mode. Special IS-IS IPv6 configuration can be made in this mode.

To exit the IS-IS IPv6 address family configuration mode, run the **exit-address-family** command.

Examples

The following example enters the IS-IS IPv6 address family configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# address-family ipv6 unicast
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- [router isis](#)

1.2 adjacency-check

Function

Run the **adjacency-check** command to enable the neighbor supported protocol detection function in Hello packets.

Run the **no** form of this command to disable this function.

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

Syntax

adjacency-check

no adjacency-check

Parameter Description

N/A

Command Modes

IS-IS routing process configuration mode

IS-IS IPv6 address family configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example disables the neighbor supported protocol detection function in hello packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# no adjacency-check
Hostname(config-router)# address-family ipv6
Hostname(config-router-af)# no adjacency-check
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 area-password

Function

Run the **area-password** command to configure plaintext authentication password of Level-1 areas.

Run the **no** form of this command to remove this configuration.

The authentication password configuration function is disabled by default.

Syntax

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

```
no area-password [ send-only ]
```

Parameter Description

0: Indicates that the key is displayed in plaintext.

7: Indicates that the key is displayed in ciphertext.

password-string: Password string for plaintext authentication. The string can contain up to 126 characters.

send-only: Indicates that the plaintext authentication password is only used to authenticate sent Hello packets in Level-1 areas. Received Hello packets are not authenticated.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

If a password is a Type 7 ciphertext password, the password may not be identified when the device version does not support AES128/SHA256. Therefore, before the device version is degraded, you must reconfigure the password as plaintext or a Type 7 ciphertext password that is generated on the earlier device version.

Run this command to enable authentication of received LSPs, CSNPs, and PSNPs in Level-1 areas and include authentication information in these packets before they are sent. All IS-IS devices in an area must be configured with the same *password-string*.

This command does not take effect if the **authentication mode** command is executed. You need to first delete the previous command configuration.

To delete the password, run the **no area-password** command. If you run the **no area-password send-only** command, only the **send-only** setting is canceled. If you run the **area-password psw send-only** and **no area-password send-only** commands in sequence, the configuration is changed to **area-password psw**.

Examples

The following example sets the plaintext authentication password of Level-1 areas to **redgiant** and applies the password to only sent packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
```



```
Hostname(config-router)# area-password redgiant send-only
```

Notifications

If authentication is configured using the **authentication mode** command, the following notification will be displayed:

```
% Please configure password using authentication command.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 authentication key-chain

Function

Run the **authentication key-chain** command to configure a key chain for IS-IS authentication.

Run the **no** form of this command to remove this configuration.

The authentication key chain function is disabled by default.

Syntax

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

```
no authentication key-chain name-of-chain [ level-1 | level-2 ]
```

Parameter Description

name-of-chain: Name of a key chain. The maximum length is 255.

level-1: Indicates that the authentication key chain takes effect for Level-1.

level-2: Indicates that the authentication key chain takes effect for Level-2.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

Authentication is not performed if no key chain is configured using the **key chain** command.

- (1) If the **authentication mode** command is run with this command, the authentication type configured in the **authentication mode** command is used as an encryption and authentication type, and the key specified by the key-chain is used as an authentication key. You can run the **authentication mode** command to specify the authentication mode.

(2) If only this command is run, the authentication type specified by the key-chain is used as an encryption and authentication type, and the key specified by the key-chain is used as an authentication key. You can run the **key chain** command to specify the authentication mode.

For plaintext authentication, the key-string 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.

If no Level is specified, the key chain takes effect for Level-1 and Level-2.

The key chain is applicable to LSPs, CSNPs, and PSNPs. IS-IS will send or receive passwords that belong to the key chain.

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 packet-carried password is consistent with a password in the key chain.

If key chain authentication is configured and the authentication type specified in the key chain is SM3, the range of Algorithm-ID is 0 to 255. If the Algorithm-ID exceeds the range, IS-IS packets do not carry TLV information for authentication. In this case, local authentication and checking will fail.

Examples

The following example specifies the Level-1 key chain with the name kc for IS-IS authentication.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# authentication key-chain kc level-1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- [authentication mode](#)

1.5 authentication mode

Function

Run the **authentication mode** command to enable an IS-IS authentication mode.

Run the **no** form of this command to disable this mode.

The authentication mode function is disabled by default.

Syntax

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

no authentication mode { **md5** | **text** } [**level-1** | **level-2**]

Parameter Description

md5: Specifies the MD5 authentication mode.

text: Specifies the plaintext authentication mode.

level-1: Specifies that the authentication mode takes effect for Level-1.

level-2: Specifies that the authentication mode takes effect for Level-2.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

If no Level is specified, the authentication mode will take effect for Level-1 and Level-2.

If you use the **authentication mode** command after the **area-password** or **domain-password** command is executed to configure plaintext authentication, the previous command configuration will be overwritten.

The **area-password** or **domain-password** command does not take effect if the **authentication mode** command is executed. To run the **area-password** or **domain-password** command, delete the **authentication mode** command configuration first.

Examples

The following example specifies the IS-IS authentication mode as MD5.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# authentication mode md5 level-1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.6 authentication send-only

Function

Run the **authentication send-only** command to apply a specified IS-IS authentication mode to only sent packets. Received packets are not authenticated.

Run the **no** form of this command to restore the default configuration.

Packets sent and received are authenticated by default.

Syntax

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

```
no authentication send-only [ level-1 | level-2 ]
```

Parameter Description

level-1: Applies authentication to only the sent packets on Level-1.

level-2: Applies authentication to only the sent packets on Level-2.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

Use this command to enable IS-IS to set an authentication password in the Hello packets to be sent. Received packets are not authenticated. You can use this command before you deploy IS-IS authentication on all devices in the network or before you change the authentication password or authentication mode. Before using this command, you should run the **authentication send-only** command. The devices will not authenticate received packets to avoid network flapping during authentication deployment. After authentication is deployed in the entire network, run the **no isis authentication send-only** command to cancel the **send-only** setting.

This command is applicable to plaintext authentication and MD5 authentication. You can run the **authentication mode** command to specify the authentication mode.

If no Level is specified, the authentication mode will take effect for Level-1 and Level-2.

Examples

The following example specifies that IS-IS authentication is performed only on sent packets. Received packets are not authenticated.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# authentication send-only level-1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- [show isis database](#)

1.7 bandwidth-reference

Function

Run the **bandwidth-reference** command to configure the reference bandwidth value of IS-IS.

Run the **no** form of this command to remove this configuration.

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

Syntax

bandwidth-reference *bandwidth*

no bandwidth-reference

Parameter Description

bandwidth: Reference bandwidth value for automatic cost computation of an IS-IS link, in Mbps. The value range is from 1 to 4294967.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

If an IS-IS interface is configured with a metric value, the bandwidth value in this command does not involve in cost computation of a link.

Examples

The following example sets the reference bandwidth value of IS-IS to **200** Mbps.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# bandwidth-reference 200
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8 bfd all-interfaces

Function

Run the **bfd all-interfaces** command to enable BFD for IS-IS interfaces.

Run the **no** form of this command to disable this function.

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

Syntax

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

no bfd all-interfaces [**anti-congestion**]

Parameter Description

anti-congestion: Indicates the IS-IS BFD anti-congestion option.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

You can enable or disable BFD on an IS-IS interface by using any of the following two methods:

Method 1: Run the [**no**] **bfd all-interfaces** [**anti-congestion**] command in IS-IS routing process configuration mode to enable or disable BFD on all IS-IS interfaces.

Method 2: Run the **isis bfd** [**disable** | **anti-congestion**] command in interface configuration mode to enable or disable BFD on the specified interface.

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 many new techniques such as Multi-Service Transport Platform (MSTP) emerging, links become easily congested in peak hours of data communication. In this case, BFD can quickly detect the abnormal link and instruct 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 route 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.

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.

Note

- You must configure a BFD session on the interface 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** command with the **[anti-congestion]** option selected, run the **bfd up-dampening** command on the interface.
-

Examples

The following example configures all interfaces running IS-IS protocol to perform BFD for link detection.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis 123
Hostname(config-router)# bfd all-interface
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **bfd up-dampening** (reliability/BFD)

1.9 clear clns neighbors

Function

Run the **clear clns neighbors** command to clear all neighbor relationship tables of IS-IS.

Syntax

```
clear clns neighbors
```

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

Run this command to refresh the neighbor relationship tables of IS-IS immediately.

Examples

The following example clears all neighbor relationship tables of IS-IS.

```
Hostname> enable
Hostname# clear clns neighbors
```

Notifications

N/A

Platform Description

N/A

1.10 clear isis *

Function

Run the **clear isis *** command to clear all data structures of IS-IS.

Syntax

```
clear isis *
```

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

Run this command to refresh LSPs immediately. After the **area-password** and **domain-password** commands are run, if old LSPs remain existent in the local device, you can use this command to clear these LSPs.

Examples

The following example clears all data structures of IS-IS.

```
Hostname> enable
Hostname# clear isis *
```


Notifications

N/A

Platform Description

N/A

1.11 clear isis counter

Function

Run the **clear isis counter** command to clear statistical information of IS-IS.

Syntax

```
clear isis [ tag ] counter
```

Parameter Description

tag: Name of an IS-IS instance.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

Run this command to clear statistical information of IS-IS.

Examples

The following example clears statistical information of IS-IS.

```
Hostname> enable
Hostname# clear isis counter
```

Notifications

N/A

Platform Description

N/A

1.12 default-information originate

Function

Run the **default-information originate** command to generate a default route and advertise the route in LSPs.

Run the **no** form of this command to remove this configuration.

The default route function is disabled by default.

Syntax

```
default-information originate [ route-map route-map-name ]  
no default-information originate
```

Parameter Description

route-map *route-map-name*: Associates a route map.

Command Modes

IS-IS routing process configuration mode
IS-IS IPv6 address family configuration mode

Default Level

14

Usage Guidelines

Because Level-2 domains do not generate any default route, use this command to allow a default route to enter a Level-2 domain.

Examples

The following example generates a default route and advertises the route in LSPs.

```
Hostname> enable  
Hostname# configure terminal  
Hostname(config)# router isis  
Hostname(config-router)# default-information originate  
Hostname(config-router)# address-family ipv6  
Hostname(config-router-af)# default-information originate
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- [show isis database](#)

1.13 distance

Function

Run the **distance** command to configure the administrative distance of an IS-IS route.

Run the **no** form of this command to restore the default configuration.

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

Syntax

distance *distance-value*

no distance

Parameter Description

distance-value: Administrative distance of a route. The value range is from 1 to 255.

Command Modes

IS-IS routing process configuration mode

IS-IS IPv6 address family configuration mode

Default Level

14

Usage Guidelines

If the administrative distance of a route is set to a smaller value, the routing information becomes more trustworthy and the priority of the route in the routing table is higher.

Examples

The following example sets the administrative distance of an IS-IS route to **100** Mbps.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# distance 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.14 domain-password

Function

Run the **domain-password** command to configure plaintext authentication password of Level-2 areas.

Run the **no** form of this command to remove this configuration.

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

Syntax

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

```
no domain-password [ send-only ]
```

Parameter Description

0: Indicates that the key is displayed in plaintext.

7: Indicates that the key is displayed in ciphertext.

password-string: Password string for plaintext authentication. The string can contain up to 126 characters.

send-only: Indicates that the plaintext authentication password is only used to authenticate sent Hello packets in Level-2 areas. Received Hello packets are not authenticated.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

If a password is a Type 7 ciphertext password, the password may not be identified when the device version does not support AES128/SHA256. Therefore, before the device version is degraded, you must reconfigure the password as plaintext or a Type 7 ciphertext password that is generated on the earlier device version.

Run this command to enable authentication of received LSPs, CSNPs, and PSNPs in Level-2 areas and include authentication information in these packets before they are sent. All IS-IS devices in a Level-2 area must be configured with the same *password-string*.

This command does not take effect if the **authentication mode** command is executed. You need to first delete the previous command configuration.

To delete the password, run the **no domain-password** command. If you run the **no domain-password send-only** command, only the **send-only** setting is canceled. If you run the **domain-password psw send-only** and **no domain-password send-only** commands in sequence, the configuration is changed to **domain-password psw**.

Examples

The following example sets the plaintext authentication password of Level-2 domain to **redgiant**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# domain-password redgiant
```

Notifications

If authentication has been configured for Level-2 area by the **authentication mode** command, the following notification will be displayed:

```
% Please configure password using authentication command.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.15 enable mib-binding

Function

Run the **enable mib-binding** command to bind an IS-IS instance for SNMP operation.

Run the **no** form of this command to remove this configuration.

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

Syntax**enable mib-binding****no enable mib-binding****Parameter Description**

N/A

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage 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.

Examples

The following example binds an instance for IS-IS MIB operation.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# enable mib-binding
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.16 enable traps

Function

Run the **enable traps** command to enable the trap message sending function of IS-IS.

Run the **no** form of this command to disable this function.

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

Syntax

```
enable traps { all | traps set }
```

```
no enable traps { all | traps set }
```

Parameter Description

all: Indicates all IS-IS trap messages.

traps set: Trap message type in any set.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

IS-IS packets are classified into 18 types and grouped into several sets based on characteristics, with each set containing several trap message types. To send IS-IS trap messages, run the **snmp-server enable traps isis** command to enable the global trap switch of IS-IS, specify a host to receive IS-IS trap messages, and then run this command to specify the types of IS-IS trap messages that can be sent.

Examples

The following example enables the trap message sending function and sets the IP address of the message receiving host to 10.1.1.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server enable traps isis
Hostname(config)# snmp-server host 10.1.1.1 traps version 2c public
Hostname(config)# router isis
```

```
Hostname(config-router)# enable traps all
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.17 exit-address-family

Function

Run the **exit-address-family** command to exit the IS-IS IPv6 address family configuration mode and go back to the IS-IS routing process configuration mode.

Syntax

```
exit-address-family
```

Parameter Description

N/A

Command Modes

IS-IS IPv6 address family configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example exits the IS-IS IPv6 address family configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis 1
Hostname(config-router)# address-family ipv6 unicast
Hostname(config-router-af)# exit-address-family
Hostname(config-router)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.18 graceful-restart

Function

Run the **graceful-restart** command to enable the GR capability of IS-IS.

Run the **no** form of this command to disable this capability.

The IS-IS GR capability is enabled by default.

Syntax**graceful-restart****no graceful-restart****Parameter Description**

N/A

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

Use this command to configure the IS-IS GR capability. As long as the network conditions remain unchanged, IS-IS can be restarted and restored to the pre-restart state without impact on data forwarding.

Examples

The following example enables the IS-IS GR capability.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# graceful-restart
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- [show isis graceful-restart](#)

1.19 graceful-restart grace-period

Function

Run the **graceful-restart grace-period** command to configure the maximum GR interval of a device.

Run the **no** form of this command to restore the default configuration.

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

Syntax

graceful-restart grace-period *max-interval*

no graceful-restart grace-period

Parameter Description

max-interval: Maximum GR interval of a device, in seconds. The value range is from 1 to 65535.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the maximum GR interval of a device to **40** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# graceful-restart grace-period 40
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.20 graceful-restart helper disable

Function

Run the **graceful-restart helper disable** command to disable the IS-IS GR Helper capability.

Run the **no** form of this command to enable this capability.

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

Syntax

graceful-restart helper disable

no graceful-restart helper disable

Parameter Description

N/A

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

After you use this command to disable the IS-IS GR Helper capability, IS-IS ignores GR requests of the device.

Examples

The following example disables the IS-IS GR Helper capability.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# graceful-restart helper disable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.21 hello padding

Function

Run the **hello padding** command to enable padding specified IS-IS Hello packets.

Run the **no** form of this command to disable this function.

Padding is enabled for hello packets of the LAN and P2P types by default.

Syntax

```
hello padding [ multi-point | point-to-point ]
```

```
no hello padding [ multi-point | point-to-point ]
```

Parameter Description

multi-point: Pads the hello packets of the LAN type.

point-to-point: Pads the hello packets of the P2P type.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

By padding hello packets, IS-IS can advertise neighbors of the MTU supported by the local device. You can use this command to enable or disable padding all hello packets sent by the local IS-IS process. You can also use this command to disable padding all hello packets of the LAN type or P2P type.

The **isis hello padding** command applies to padding in interface configuration mode. To disable padding hello packets on a specified interface, disable padding the packets in IS-IS routing process configuration mode or interface configuration mode.

Examples

The following example disables padding hello packets of the P2P type.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# no hello padding point-to-point
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.22 hostname dynamic

Function

Run the **hostname dynamic** command to replace the system ID of a device with the host name of the destination device.

Run the **no** form of this command to remove this configuration.

The dynamic host name function is enabled by default.

Syntax

hostname dynamic

no hostname dynamic

Parameter Description

N/A

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

Run this command to replace the system ID of a device with the host name of the destination device. The system IDs that can be displayed by running the **show isis database** and **show isis neighbors** commands are replaced with the host name of the destination device.

Examples

The following example replaces the system ID of a device with the host name of the destination device.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# hostname dynamic
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- [show isis neighbors](#)
- [show isis database](#)

1.23 ignore-lsp-errors

Function

Run the **ignore-lsp-errors** command to ignore LSP checksum errors.

Run the **no** form of this command to remove this configuration.

LSP checksum errors are processed by default.

Syntax

ignore-lsp-errors

no ignore-lsp-errors

Parameter Description

N/A

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

After receiving an LSP, the local IS-IS router calculates its checksum and compares it with the checksum contained in the LSP. If the two checksums are inconsistent, the LSP will be discarded by default. If you run the **ignore-lsp-errors** command to ignore checksum errors, the LSP will be processed normally despite checksum inconsistency.

Examples

The following example configures to ignore LSP checksum errors.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# ignore-lsp-errors
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.24 interfaces-protocol-compatible

Function

Run the **interfaces-protocol-compatible** command to pad the TLV field of the IS-IS protocol based on protocols supported by an interface.

Run the **no** form of this command to restore the default configuration.

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

Syntax

```
interfaces-protocol-compatible  
no interfaces-protocol-compatible
```

Parameter Description

N/A

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

In single topology mode, a Orion 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 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 device failed to establish a neighbor relationship with the device of the other vendor. To solve this issue, this command can be configured to enable neighbor relationship establishment between Orion devices and devices of other vendors.

Examples

The following example pads the TLV field of the IS-IS protocol based on protocols supported by an interface.

```
Hostname> enable  
Hostname# configure terminal  
Hostname(config)# router isis  
Hostname(config-router)# interfaces-protocol-compatible
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.25 ip router isis

Function

Run the **ip router isis** command to enable the IPv4 IS-IS routing function on an interface.

Run the **no** form of this command to disable this function.

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

Syntax

ip router isis [*tag*]

no ip router isis [*tag*]

Parameter Description

tag: Name of an IS-IS instance.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Note

This command must be run to enable the IS-IS function on an interface in an IPv4 network.

An IS-IS instance named *tag* runs on an interface. If no such instance exists or will be started and initialized in the name of *tag*, the IS-IS routing function will not be started on this interface.

Use this command to enable an interface to participate in IS-IS IPv4 routing. Use the **no** form of this command to disable the IS-IS routing process on the interface.

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. Other IS-IS settings remain unchanged.

An instance named *tag* can be started on 255 broadcast network interfaces at most, whereas, it can be started on unlimited number of P2P network interfaces.

Examples

The following example enables the IPv4 IS-IS routing function on TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# ip router isis
```

Notifications

If this interface has been added to another IS-IS instance, the following notification will be displayed:

```
% Interface enabled in another area
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- [ip routing](#) (IP routing/routing management)
- [show isis interface](#)
- [show isis protocol](#)

1.26 ipv6 router isis

Function

Run the **ipv6 router isis** command to enable the IPv6 IS-IS routing function on an interface.

Run the **no** form of this command to disable this function.

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

Syntax

```
ipv6 router isis [ tag ]
no ipv6 router isis [ tag ]
```

Parameter Description

tag: Name of an IS-IS instance.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Note

This command must be run to enable the IS-IS function on an interface in an IPv6 network.

After this command is run, an IS-IS instance named tag runs on an interface. If no such instance exists or will be started and initialized in the name of tag, the IPv6 IS-IS routing function will not be started on this interface.

If you run the **no ipv6 unicast-routing** command in global configuration mode, IS-IS will disable IPv6 routing on all interfaces.

An instance named tag can be started on 255 broadcast network interfaces at most, whereas, it can be started on unlimited number of P2P network interfaces.

Examples

The following example enables the IPv6 IS-IS routing function on an interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# ipv6 router isis
```

Notifications

If this interface has been added to another IS-IS instance, the following notification will be displayed:

```
% Interface enabled in another area
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 unicast-routing** (IP routing basics)
- [show isis interface](#)
- [show isis protocol](#)

1.27 isis authentication key-chain

Function

Run the **isis authentication key-chain** command to configure a key chain for IS-IS interface authentication.

Run the **no** form of this command to remove this configuration.

The IS-IS interface authentication key chain function is disabled by default.

Syntax

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

no isis authentication key-chain *name-of-chain* [**level-1** | **level-2**]

Parameter Description

name-of-chain: Name of a key chain. The maximum length is 255.

level-1: Indicates that the authentication key chain takes effect for Level-1.

level-2: Indicates that the authentication key chain takes effect for Level-2.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Authentication is not performed if no key chain is configured using the **key chain** command.

- (1) If the **authentication mode** command is run with this command, the authentication type configured in the **authentication mode** command is used as an encryption and authentication type, and the key specified by the key-chain is used as an authentication key. You can run the **authentication mode** command to specify the authentication mode.
- (2) If only this command is run, the authentication type specified by the key-chain is used as an encryption and authentication type, and the key specified by the key-chain is used as an authentication key. You can run the **key chain** command to specify the authentication mode.

For plaintext authentication, the key-string 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.

If no Level is specified, the key chain takes effect for Level-1 and Level-2.

The key chain is applicable to Hello packets. IS-IS will send or receive passwords that belong to the key chain.

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 packet-carried password is consistent with a password in the key chain.

The authentication commands (for example, **authentication key-chain**) executed in IS-IS routing process configuration mode are intended for LSPs and SNPs. They do not take effect for IS-IS interfaces.

If key chain authentication is configured and the authentication type specified in the key chain is SM3, the range of Algorithm-ID is 0 to 255. If the Algorithm-ID exceeds the range, IS-IS packets do not carry TLV information for authentication. In this case, local authentication and checking will fail.

Examples

The following example specifies the key chain with the name kc for authentication on the IS-IS interface TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
```

```
Hostname(config-if-TenGigabitEthernet 0/1)# isis authentication key-chain kc
```

Notifications

N/A

Common Errors

- The key-string in the key chain exceeds 80 characters.

Platform Description

N/A

Related Commands

- [isis authentication mode](#)

1.28 isis authentication mode

Function

Run the **isis authentication mode** command to enable an authentication mode of an IS-IS interface.

Run the **no** form of this command to disable this mode.

The interface authentication mode is disabled by default.

Syntax

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

```
no isis authentication mode { md5 | text } [ level-1 | level-2 ]
```

Parameter Description

md5: Specifies the MD5 authentication mode.

text: Specifies the plaintext authentication mode.

level-1: Specifies that the interface authentication mode takes effect for Level-1.

level-2: Specifies that the interface authentication mode takes effect for Level-2.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If no Level is specified, the authentication mode will take effect for Level-1 and Level-2.

Run the **authentication mode** command to specify the authentication mode before you can make the key chain configured using the **authentication key-chain** command take effect.

If you use the **isis authentication mode** command after the **isis password** command is executed to configure plaintext authentication, the previous command configuration will be overwritten.

The **isis password** command does not take effect if the **isis authentication mode** command is executed. To run the **isis password** command, delete the **isis authentication mode** command configuration first.

Examples

The following example specifies the Level-2 authentication mode on the IS-IS interface TenGigabitEthernet 0/1 as MD5.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# isis authentication mode md5 level-2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.29 isis authentication send-only

Function

Run the **isis authentication send-only** command to apply a specified IS-IS interface authentication mode to only sent packets. Received packets are not authenticated.

Run the **no** form of this command to restore the default configuration.

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

Syntax

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

```
no isis authentication send-only [ level-1 | level-2 ]
```

Parameter Description

level-1: Sets **send-only** for Level-1 on an interface.

level-2: Sets **send-only** for Level-2 on an interface.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Use this command to enable IS-IS to set an authentication password in the Hello packets sent by an interface. Received packets are not authenticated. You can use this command before you deploy IS-IS interface authentication on all devices in the network or before you change the authentication password or authentication mode. After you run the **isis authentication send-only** command, the devices will not authenticate received Hello packets to avoid network flapping when IS-IS interface authentication is deployed. After authentication is deployed in the entire network, run the **no isis authentication send-only** command to cancel the **send-only** setting.

This command is applicable to plaintext authentication and MD5 authentication. You can run the **isis authentication mode** command to specify the authentication mode for an IS-IS interface.

If no Level is specified, the authentication mode will take effect for Level-1 and Level-2 on the interface.

Examples

The following example specifies that Level-1 authentication applies to only sent packets on the IS-IS interface TenGigabitEthernet 0/1. Received packets are not authenticated.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# isis authentication send-only level-1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- [show isis database](#)

1.30 isis bfd

Function

Run the **isis bfd** command to enable IS-IS correlation with BFD on an interface.

Run the **no** form of this command to disable this function.

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.

Syntax

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

no isis bfd [anti-congestion | disable]

Parameter Description

anti-congestion: Indicates the IS-IS BFD anti-congestion option.

disable: Disables IS-IS correlation with BFD on an interface.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

You can enable or disable BFD on an IS-IS interface by using any of the following two methods:

Method 1: Run the **[no] bfd all-interfaces [anti-congestion]** command in IS-IS routing process configuration mode to enable or disable BFD on all IS-IS interfaces.

Method 2: Run the **isis bfd [disable | anti-congestion]** command in interface configuration mode to enable or disable BFD on the specified interface.

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.

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.

Note

- You must configure a BFD session on the interface 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** command with the **[anti-congestion]** option selected, run the **bfd up-dampening** command on the interface.
-

Examples

The following example disables IS-IS correlation with BFD on TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# no switchport
Hostname(config-if-TenGigabitEthernet 0/1)# isis bfd disable
```

The following example enables the IS-IS BFD anti-congestion option on TenGigabitEthernet 0/1 and runs the BFD anti-congestion option.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# no switchport
Hostname(config-if-TenGigabitEthernet 0/1)# isis bfd anti-congestion
Hostname(config-if-TenGigabitEthernet 0/1)# bfd up-dampening 60000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- [show isis interface](#)
- [show isis neighbors](#)
- [show bfd neighbors detail](#) (reliability/BFD)

1.31 isis circuit-type

Function

Run the **isis circuit-type** command to configure an IS-IS level on an interface.

Run the **no** form of this command to restore the default configuration.

An interface runs on Level-1/Level-2 by default.

Syntax

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

```
no isis circuit-type
```

Parameter Description

- level-1**: Establishes a Level-1 neighbor relationship.
- level-2-only**: Establishes a Level-2 neighbor relationship.
- level-1-2**: Establishes a Level-1/Level-2 neighbor relationship.
- external**: Uses the interface as an external domain interface.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If **circuit-type** is set to Level-1 or Level-only, IS-IS will only send PDUs at the corresponding level.

If **is-type** is set to **level-1** or **level-only**, the IS-IS instance only processes transactions at the corresponding level. In this case, the interface only sends the PDUs of the same Level specified by the **is-type** and **circuit-type** commands.

If the interface is set to external, the interface is used as an external domain interface and IS-IS will not send PDUs at the corresponding Level.

Examples

The following example sets the level of TenGigabitEthernet 0/1 to level-2-only.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# isis circuit-type level-2-only
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.32 isis csnp-interval

Function

Run the **isis csnp-interval** command to specify the CSNP broadcast interval on an IS-IS interface.

Run the **no** form of this command to restore the default configuration.

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.

Syntax

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

```
no isis csnp-interval [ interval ] [ level-1 | level-2 ]
```

Parameter Description

interval: CSNP transmission interval, in seconds. The value range is from 0 to 65535.

level-1: Applies transmission interval only to Level-1 CSNPs.

level-2: Applies transmission interval only to Level-2 CSNPs.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Use this command to change the CSNP interval. By default, the DIS sends CSNPs every 10s in a broadcast network.

In a P2P network, CSNPs are sent only after a neighbor relationship is established. If an interface is configured as **mesh-groups**, CSNP sending interval can be configured. If **csnp-interval** is set to 0, no CSNP is sent.

If the **level-1** or **level-2** parameter is not specified when the command is configured, the interval configuration takes effect for Level-1 and Level-2 CSNPs.

Examples

The following example sets the CSNP broadcast interval to **20** seconds on TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# isis csnp-interval 20
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.33 isis hello padding

Function

Run the **isis hello padding** command to enable padding IS-IS hello packets sent on an IS-IS interface.

Run the **no** form of this command to remove this configuration.

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

Syntax

isis hello padding

no isis hello padding

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

By padding hello packets, IS-IS can advertise neighbors of the MTU supported by the local device.

The **hello padding** command applies to padding in IS-IS routing process configuration mode. To disable padding hello packets on a specified interface, disable padding the packets in IS-IS routing process configuration mode or interface configuration mode.

Examples

The following example disables padding IS-IS hello packets on TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# no isis hello padding
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.34 isis hello-interval

Function

Run the **isis hello-interval** command to configure the hello packet sending interval on an interface.

Run the **no** form of this command to restore the default configuration.

Hello packet are sent at an interval of **10** seconds by default.

Syntax

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

```
no isis hello-interval { interval | minimal } [ level-1 | level-2 ]
```

Parameter Description

interval: Hello packet sending interval, in seconds. The value range is from 1 to 65535.

minimal: Uses the minimum holdtime **1** second.

level-1: Takes effect for Level-1 Hello packets.

level-2: Takes effect for Level-2 Hello packets.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If the **level-1** or **level-2** parameter is not specified when the command is configured, the interval configuration takes effect for Level-1 and Level-2 LSPs.

Use this command to modify the Hello packet sending interval. Hello packets are sent at an interval of **10** seconds by default. A DIS sends Hello packets at a frequency three times that by non-DIS devices in a broadcast network. If the local device is elected as the DIS on the interface, this interface sends hello packet every 3.3s by default.

The default hello multiplier of an IS-IS interface is **3**. The holdtime in hello packets is the hello-interval multiplied by this multiplier. If the keyword **minimal** is used, the holdtime in hello packets is set to **1**, the hello packet sending interval is the result of one divided by the hello multiplier. If the hello multiplier is set to **4** and the **isis hello-interval minimal** command is executed, the packet sending interval is **250** ms.

CPU protection is enabled by default. For packets sent to each destination group address (AllISSystems, AllL1ISSystems, and AllL2ISSystems), the number of packets sent to the CPU is limited to 400 per second. If a device has many neighbor relationships or sends Hello packets at short intervals, the IS-IS packets that the device receives may exceed the default limit, causing frequent flapping of neighbor relationships. To solve the problem, you can use the CPU protection command in global configuration mode to increase the limit.

Examples

The following example sets the Level-1 hello packet sending interval to **5** seconds on TenGigabitEthernet 0/1.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# isis hello-interval 5 level-1
```

The following example sets the minimum hello packet holdtime to **1** second on TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# isis hello-interval minimal
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.35 isis hello-multiplier

Function

Run the **isis hello-multiplier** command to configure the multiplier of the hello holdtime on an interface.

Run the **no** form of this command to restore the default configuration.

The default multiplier of the hello holdtime on an interface is **3**.

Syntax

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

```
no isis hello-multiplier [ multiplier-number ] [ level-1 | level-2 ]
```

Parameter Description

multiplier-number: Multiplier of the hello holdtime on an IS-IS interface. The value range is from 2 to 100.

level-1: Takes effect for Level-1 hello packets.

level-2: Takes effect for Level-2 hello packets.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The holdtime in hello packets is equal to the hello-interval multiplied by the hello multiplier.

Examples

The following example sets the multiplier of the hello holdtime to **5** on TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# isis hello-multiplier 5
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.36 isis lsp-flood

Function

Run the **isis lsp-flood** command to configure the maximum number of LSP packets sent by the IS-IS interface at a time.

Run the **no** form of this command to restore the default configuration.

An interface can send a maximum of 5 LSP packets at a time by default.

Syntax

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

```
no isis lsp-flood [ level-1 | level-2 ]
```

Parameter Description

lsp-number: Maximum number of LSP packets sent by the IS-IS interface at a time. The value range is from 1 to 1000.

level-1: Takes effect for Level-1 LSPs.

level-2: Takes effect for Level-2 LSPs.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the maximum number of Level-2 LSP packets sent by TenGigabitEthernet 0/1 at a time to **10**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# isis lsp-flood 10 level-2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.37 isis lsp-interval

Function

Run the **isis lsp-interval** command to configure the LSP sending interval on an interface.

Run the **no** form of this command to restore the default configuration.

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

Syntax

```
isis lsp-interval pdu-interval [ level-1 | level-2 ]
```

```
no isis lsp-interval [ level-1 | level-2 ]
```

Parameter Description

pdu-interval: LSP sending interval, in milliseconds. The value range is from 1 to 4294967295.

level-1: Takes effect for Level-1 LSPs.

level-2: Takes effect for Level-2 LSPs.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If the **level-1** or **level-2** parameter is not specified when the command is configured, the interval configuration takes effect for Level-1 and Level-2 LSPs.

Examples

The following example sets the Level-2 LSP sending interval to **100** ms on TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# isis lsp-interval 100 level-2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.38 isis mesh-group

Function

Run the **isis mesh-group** command to add an IS-IS interface to a specified mesh group.

Run the **no** form of this command to remove this configuration.

No interface joins any mesh group by default.

Syntax

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

```
no isis mesh-group
```

Parameter Description

blocked: Blocks all LSP forwarding on this interface.

mesh-group-id: ID of a mesh group an interface joins. The value range is from 1 to 4294967295.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Mesh-groups can control transitional and redundant LSPs in an NBMA network. In normal cases, an IS-IS device advertises LSPs from all other interfaces except the packet receiving interface. If a device is configured with multiple interfaces, LSPs will be sent from all these interfaces. In this case, neighbors will receive duplicate LSPs. This wastes a huge amount of CPU and bandwidth resources.

The IS-IS mesh group allows a device to group interfaces. If an LSP is received by any interface in a group, this LSP will not be advertised by other interfaces in the group. If the LSP is received from an interface out of the group, the LSP will be advertised from other interfaces as usual.

When you need to set **mesh-group** on an IS-IS interface, run the **isis csnp-interval** command to configure the non-0 CSNP sending interval to ensure complete LSP synchronization between neighbors in the network. After that, CNSPs will be periodically sent to synchronize LSPs.

Examples

The following example adds the IS-IS interface TenGigabitEthernet 0/1 to a specified mesh group 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# isis mesh-group 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.39 isis metric

Function

Run the **isis metric** command to configure the metric for an IS-IS interface.

Run the **no** form of this command to configure the metric for an IS-IS interface as a default value.

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

Syntax

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

```
no isis metric [ metric ] [ level-1 | level-2 ]
```


Parameter Description

metric: Metric value. The value range is from 1 to 63.

level-1: Takes effect for Level-1 circuit type.

level-2: Takes effect for Level-2 circuit type.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The metric value, which is used in IP calculation, is stored in the TLV of the IP reachability information. A greater metric value indicates a greater routing consumption of this interface and a longer path of SPF calculation.

The metric belongs to the narrow type and is valid only when **metric-style** is set to Narrow.

Examples

The following example sets the metric on the IS-IS interface TenGigabitEthernet 0/1 to 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# isis metric 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- [metric-style](#)

1.40 isis network point-to-point

Function

Run the **isis network point-to-point** command to change the type of an interface from broadcast to P2P.

Run the **no** form of this command to restore the default configuration.

The default type of an interface is broadcast.

Syntax

```
isis network point-to-point
no isis network [ point-to-point ]
```

Parameter Description

point-to-point: Configures an interface as a P2P interface.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Use this command to change the type of an interface from broadcast to P2P. This command is valid to broadcast network interfaces.

If the current interfaces have been configured with the IS-IS protocol and the number of broadcast network interfaces configured with the same IS-IS protocol reaches 255 (for example, **ip router isis [tag]** or **ipv6 router isis [tag]** is configured, or the interfaces are passive interfaces), this configuration cannot be deleted.

Examples

The following example changes the interface type of TenGigabitEthernet 0/1 from broadcast to P2P.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# isis network point-to-point
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- [show isis interface](#)

1.41 isis passive

Function

Run the **isis passive** command to configure an interface as a passive interface.

Run the **no** form of this command to remove this configuration.

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

Syntax

isis passive

no isis passive

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

This command prevents the interface from receiving or sending IS-IS packets, but the IP address of this interface is flooded through other interfaces. The command is valid only for the generated IS-IS interface.

Examples

The following examples configures TenGigabitEthernet 0/1 as a passive interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# isis passive
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- [show isis interface](#)

1.42 isis password

Function

Run the **isis password** command to configure the password for plaintext authentication of hello packets on an interface.

Run the **no** form of this command to remove this configuration.

Syntax

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

```
no isis password [ send-only ] [ level-1 | level-2 ]
```

Parameter Description

0: Indicates that the key is displayed in plaintext.

7: Indicates that the key is displayed in ciphertext.

password-string: Password string for plaintext authentication. The string can contain up to 126 characters.

send-only: Indicates that the plaintext authentication password is only used to authenticate sent packets. Received packets are not authenticated.

level-1: Takes effect for Level-1 circuit type.

level-2: Takes effect for Level-2 circuit type.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If a password is a Type 7 ciphertext password, the password may not be identified when the device version does not support AES128/SHA256. Therefore, before the device version is degraded, you must reconfigure the password as plaintext or a Type 7 ciphertext password that is generated on the earlier device version.

Use this command to configure the password for Hello packet authentication on an interface. Use the **no** form of this command to clear the password.

If no Level is specified by default, the password takes effect for Level-1 and Level-2 circuit types.

This command does not take effect if the **isis authentication mode** command is executed. You need to first delete the previous command configuration.

If you include the **send-only** parameter when deleting the **isis authentication mode** command configuration, only the parameter setting is canceled.

Examples

The following example sets the password for plaintext authentication of hello packets to **redgiant** on an interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# isis password redgiant
```

Notifications

If authentication is configured using the **isis authentication mode** command, the following notification will be displayed:

```
% Please configure password using isis authentication command.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.43 isis priority

Function

Run the **isis priority** command to configure the priority for DIS election in a LAN.

Run the **no** form of this command to restore the default configuration.

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

Syntax

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

```
no isis priority [ value ] [ level-1 | level-2 ]
```

Parameter Description

value: Priority for DIS election in a LAN. The value range is from 0 to 127.

level-1: Takes effect for Level-1 circuit type.

level-2: Takes effect for Level-2 circuit type.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Use this command to change the priority in Hello packets in a LAN.

A lower DIS priority of an interface indicates a lower priority of being elected as a DIS.

This command is invalid on a P2P network interface.

The **no isis priority** command, with or without parameters, restores the priority to its default value. To change the configured priority, run the **isis priority** command with the priority specified to overwrite the existing configuration, or you can first restore the priority to its default value and then configure a new priority.

Examples

The following example sets the priority for Level-1 DIS election on TenGigabitEthernet 0/1 to 127.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# isis priority 127 level-1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- [show isis interface](#)

1.44 isis psnp-interval

Function

Run the **isis psnp-interval** command to configure the minimum PSNP sending interval.

Run the **no** form of this command to remove this configuration.

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

Syntax

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

```
no isis psnp-interval [ level-1 | level-2 ]
```

Parameter Description

psnp-interval: PSNP interval, in seconds. The value range is from 1 to 120.

level-1: Takes effect for Level-1 PSNPs.

level-2: Takes effect for Level-2 PSNPs.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If the **level-1** or **level-2** parameter is not specified when the command is configured, the interval configuration takes effect for Level-1 and Level-2 CSNPs.

PSNPs are mainly used to request LSPs that are absent locally or respond to received LSPs (in a P2P network). The PSNP interval should be minimized. If many LSPs exist and the device performance is low, you can increase the PSNP sending interval and LSP retransmission interval to reduce the device load.

Examples

The following example sets the Level-2 PSNP sending interval to 5 seconds on TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# isis psnp-interval 5 level-2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.45 isis retransmit-interval

Function

Run the **isis retransmit-interval** command to configure the LSP retransmission interval on an IS-IS interface.

Run the **no** form of this command to restore the default configuration.

The default LSP Retransmit-interval is **5** seconds, and it takes effect for Level-1 and Level-2 LSPs.

Syntax

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

```
no isis retransmit-interval [ level-1 | level-2 ]
```

Parameter Description

retransmit-interval: Retransmission interval, in seconds. The value range is from 0 to 65535.

level-1: Takes effect for Level-1 LSPs.

level-2: Takes effect for Level-2 LSPs.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If the **level-1** or **level-2** parameter is not specified when the command is configured, the interval configuration takes effect for Level-1 and Level-2 CSNPs.

Use this command to configure the LSP retransmission interval. In a P2P network, after a device sends an LSP, if the device receives no PSNP response within the time specified by `retransmit-interval`, it will resend the LSP. If the retransmission interval is set to **0**, the LSP will not be resent.

Examples

The following example sets the Level-2 LSP sending interval to **10** seconds on TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# isis retransmit-interval 10 level-2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.46 isis subvlan

Function

Run the **isis subvlan** command to enable the IS-IS function in a super VLAN.

Run the **no** form of this command to restore the default configuration.

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

Syntax

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

```
no isis subvlan
```

Parameter Description

all: Allows sending packets to all sub VLANs

vlan-id: Sub VLAN ID. The value range is from 1 to 4094.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

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. However, in some scenarios, the IS-IS function must be run on the super VLAN, but packets need to be sent to only 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. You can use this command to specify a particular sub VLAN. You must be cautious when configuring packet transmission to all sub VLANs, as the large number of sub VLANs may cause a device processing bottleneck, which will lead to the neighbor flapping.

Examples

The following example enables the IS-IS function on super VLAN 300 and allows sending packets to sub VLAN 1024.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface vlan 300
Hostname(config-if-VLAN 300)# isis subvlan 1024
```

Notifications

N/A

Common Errors

- The function is configured on a non-super VLAN.
- The specified sub VLAN on the super VLAN cannot implement interworking with its neighbors.

Platform Description

N/A

Related Commands

N/A

1.47 isis suppress on-neighbor-up

Function

Run the **isis suppress on-neighbor-up** command to suppress routing calculation after an IS-IS neighbor is up.

Run the **no** form of this command to remove this configuration.

The route calculation suppression function is disabled by default.

Syntax

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

no isis suppress on-neighbor-up

Parameter Description

delay-time: Delay time of suppressing route calculation, in seconds. The value range is from 1 to 60.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

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.

Examples

The following example suppresses route calculation after the IS-IS neighbor on TenGigabitEthernet 0/1 is up.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# isis suppress on-neighbor-up 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip route** (IP routing basic)

1.48 isis three-way-handshake disable

Function

Run the **isis three-way-handshake disable** command to disable three-way handshake of a P2P network.

Run the **no** form of this command to enable three-way handshake of a P2P network.

Three-way handshake is performed in a P2P network by default.

Syntax

```
isis three-way-handshake disable
no isis three-way-handshake disable
```

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

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.

Examples

The following example disables three-way handshake on TenGigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface tenGigabitEthernet 0/1
Hostname(config-if-TenGigabitEthernet 0/1)# isis network point-to-point
Hostname(config-if-TenGigabitEthernet 0/1)# isis three-way-handshake disable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.49 isis wide-metric

Function

Run the **isis wide-metric** command to configure the wide metric value for an interface.

Run the **no** form of this command to configure the wide metric value of an interface as a default value.

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

Syntax

```
isis wide-metric metric [ level-1 | level-2 ]  
no isis wide-metric [ metric ] [ level-1 | level-2 ]
```

Parameter Description

metric: Metric value. The value range is from 1 to 16777214, and the default value is the computation result of **bandwidth-reference**.

level-1: Takes effect for the Level-1 links.

level-2: Takes effect for the Level-2 links.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The metric value, which is used in IP calculation, is stored in the TLV of the IP reachability information. A greater metric value indicates a greater routing consumption of this interface and a longer path of SPF calculation.

The metric is valid only when **metric-style** is set to **Wide**.

Examples

The following example sets the wide metric value of TenGigabitEthernet 0/1 to **1000**.

```
Hostname> enable  
Hostname# configure terminal  
Hostname(config)# interface tenGigabitEthernet 0/1  
Hostname(config-if-TenGigabitEthernet 0/1)# isis wide-metric 1000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- [metric-style](#)

1.50 is-name

Function

Run the **is-name** command to replace the system ID of an instance with the configured name.

Run the **no** form of this command to remove this configuration.

The name customization function is disabled by default.

Syntax

is-name *name*

no is-name

Parameter Description

name: Alias of an instance, which is a string of a maximum of 64 characters.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

Use this command to replace the system ID of an instance with the configured name. The system IDs that can be displayed by running the **show isis database** and **show isis neighbors** commands are replaced with the configured name.

Examples

The following example replaces the system ID of an instance with dut.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# is-name dut
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- [show isis neighbors](#)
- [show isis database](#)

1.51 is-type

Function

Run the **is-type** command to specify the level at which IS-IS runs.

Run the **no** form of this command to restore the default configuration.

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

Syntax

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

no is-type

Parameter Description

level-1: Indicates that IS-IS only runs at Level-1.

level-1-2: Indicates that IS-IS runs at Level-1 and Level-2.

level-2-only: Indicates that IS-IS only runs at Level-2.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

Changing the IS-IS type will enable or disable the routes of the corresponding level.

Examples

The following example enables IS-IS to only run at Level-1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# is-type level-1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.52 log-adjacency-changes

Function

Run the **log-adjacency-changes** command to record neighbor state changes of IS-IS without enabling the **debug** command.

Run the **no** form of this command to disable this function.

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

Syntax

log-adjacency-changes

no log-adjacency-changes

Parameter Description

N/A

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

Using the **debug** command to record neighbor state changes of IS-IS will consume a great amount of system resources. Run this command to record neighbor state changes of IS-IS without enabling the **debug** command.

Examples

The following example records neighbor state changes of IS-IS without enabling the **debug** command.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# log-adjacency-changes
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.53 Isp-fragments-extend

Function

Run the **Isp-fragments-extend** command to enable fragment extension.

Run the **no** form of this command to disable this function.

The fragment extension function is disabled by default.

Syntax

```
lsp-fragments-extend [ level-1 | level-2 ] [ compatible rfc3786 ]  
no lsp-fragments-extend [ level-1 | level-2 ] [ compatible rfc3786 ]
```

Parameter Description

level-1: Enables LSP fragment extension on Level-1.

level-2: Enables LSP fragment extension on Level-2.

compatible: Indicates compatibility with the RFC version of extended LSPs.

rfc3786: Indicates the old version of extended LSPs.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

If the **level-1** or **level-2** parameter is not specified when the command is configured, the interval configuration takes effect for Level-1 and Level-2 CSNPs.

There are up to 256 LSP fragments. When the fragments are used up, subsequent link state information, including neighbor information and IP route information, will be discarded, causing a network exception.

To solve this problem, enable fragment extension at the specified level and configure an additional system ID by using the **virtual-system** command.

When you enable or disable the **compatible** option for a network containing RFC 3786 compliant devices of other vendors, observe the LSDB of the related devices. If there are LSPs affecting network routing existing in the network, run the **clear isis *** command to clear the LSPs and trigger LSDB synchronization.

Examples

The following example enables fragment extension on Level-2.

```
Hostname> enable  
Hostname# configure terminal  
Hostname(config)# router isis  
Hostname(config-router)# lsp-fragments-extend level-2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.54 Isp-gen-interval

Function

Run the **isp-gen-interval** command to configure an exponential backoff algorithm of LSP generation.

Run the **no** form of this command to restore the default configuration.

The default maximum interval of two LSP generations is **5** seconds, the delay of LSP generation is **50** ms, and the maximum interval for the first and second LSP generations is **200** ms. The configuration takes effect for Level-1 and Level-2 LSPs.

Syntax

```
isp-gen-interval [ level-1 | level-2 ] maximum-interval [ initial-interval hold-interval ]
```

```
no isp-gen-interval [ level-1 | level-2 ]
```

Parameter Description

level-1: Takes effect for Level-1 IS-IS LSPs.

level-2: Takes effect for Level-2 IS-IS LSPs.

maximum-interval: Maximum interval for generating two consecutive LSPs, in seconds. The value range is from 1 to 65535.

initial-interval: Delay for generating LSPs for the first time, in milliseconds. The value range is 0 to 60000.

hold-interval: Minimum interval for the first and second LSP generations, in milliseconds. The value range is 10 to 60000.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

If the **level-1** or **level-2** parameter is not specified when the command is configured, the interval configuration takes effect for Level-1 and Level-2 CSNPs.

The LSP packet generation interval refers to the interval for generating two different LSP packets. A smaller generation interval indicates faster network convergence, which, however, will be accompanied by frequent flooding in the network.

The wait time for generating an LSP packet for the first time is the *initial-interval*. If the network becomes unstable, the LSP packet regeneration interval changes to be less than the *maximum-interval*, and the interval for generating an LSP packet for the second time changes to *hold-interval*. A corresponding penalty will be added to this interval: The next interval for regenerating an LSP packet doubles the previous interval for generating the same LSP packet, until the regeneration interval reaches the *maximum-interval*. Subsequent LSP packets will be generated at the *maximum-interval*. When the network becomes stable, the LSP packet

regeneration interval becomes greater than the *maximum-interval*, and the wait time for LSP packet generation is restored to the *initial interval*.

Link changes have high requirements for convergence. The *initial-interval* can be set to a small value. You can also appropriately increase the values of the preceding parameters to reduce the CPU usage.

Note

- 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*.
-

Examples

The following example configures an exponential backoff algorithm of LSP generation, and sets the maximum interval of two LSP generations to **10** seconds, the wait time of LSP generation for the first time to **100** ms, and the interval for the first and second LSP generations to **200** ms.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# lsp-gen-interval 10 100 200
```

The following example configures an exponential backoff algorithm of LSP generation, sets the maximum interval of two LSP generations to **5** seconds, and uses the default values of other exponential backoff parameters.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# lsp-gen-interval 5
```

Notifications

If the configured value of *hold-interval* is greater than *maximum-interval* (for example, the configured value of *hold-interval* is **1500** ms, and the *maximum-interval* is **1** second), the following notification will be displayed:

```
% ISIS: hold_interval (1500ms) should be no more than maximum_interval (1s), set
to (1000ms).
```

If the configured value of *initial-interval* is greater than *hold-interval* (for example, the configured value of *initial-interval* is **20** ms, and the *hold-interval* is **10** ms), the following notification will be displayed:

```
% ISIS: initial_interval (20ms) should be no more than hold_interval (10ms), set
to (10ms).
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.55 lsp-length originate

Function

Run the **lsp-length originate** command to configure the maximum length of sent LSPs.

Run the **no** form of this command to restore the default configuration.

The default maximum length of sent LSPs is **1492** bytes, and it takes effect for Level-1 and Level-2 LSPs.

Syntax

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

no lsp-length originate [**level-1** | **level-2**]

Parameter Description

size: Maximum length of sent LSPs, in bytes. The value range is from 512 to 16000.

level-1: Takes effect for Level-1 LSPs.

level-2: Takes effect for Level-2 LSPs.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

If the **level-1** or **level-2** parameter is not specified when the command is configured, the interval configuration takes effect for Level-1 and Level-2 CSNPs.

In principle, the maximum length of LSPs and SNPs cannot be greater than the interface MTU; otherwise, the packets will be discarded when being sent.

Examples

The following example sets the maximum length of sent LSPs on Level-2 to **1498** bytes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis1
Hostname(config-router)# lsp-length originate 1498 level-2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.56 lsp-length receive

Function

Run the **lsp-length receive** command to configure the maximum length of received LSPs.

Run the **no** form of this command to restore the default configuration.

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

Syntax

lsp-length receive *size*

no lsp-length receive

Parameter Description

size: Maximum length of received LSPs, in bytes. The value range is from 1492 to 16000.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

Use this command to control the maximum length of LSPs received by the local device. Intermediate nodes with sufficient memory are required to receive LSPs whose maximum length is equal to the interface MTU in order to avoid a route convergence failure. From this perspective, the command is meaningless. The maximum length of received LSPs cannot be smaller than that of sent LSPs; otherwise, the former will be automatically adjusted to be equal to the latter.

Examples

The following example sets the maximum length of received LSPs to **1498** bytes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# lsp-length receive 1498
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.57 lsp-refresh-interval

Function

Run the **lsp-refresh-interval** command to configure the LSP refresh interval.

Run the **no** form of this command to restore the default configuration.

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

Syntax

lsp-refresh-interval *interval*

no lsp-refresh-interval

Parameter Description

interval: LSP refresh interval, in seconds. The value range is from 1 to 65535.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

After an LSP has remained stable for the time specified by this command, it will be refreshed and then advertised.

The LSP refresh interval must be at least 300 seconds less than the maximum LSP lifetime. If the difference of the configured LSP lifetime *max-lifetime* from the LSP refresh interval *interval* is less than 300s, the value of *max-lifetime* minus 300s is used as the LSP refresh interval.

Examples

The following example sets the LSP refresh interval to **600** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# lsp-refresh-interval 600
```

Notifications

If the difference of the configured LSP lifetime from the LSP refresh interval is less than 300s, for example, the maximum LSP lifetime is 1000 and the LSP refresh interval is 900, the following notification will be displayed:

```
% ISIS: max-lsp-lifetime should be 300s greater than lsp-refresh-interval
```

```
% ISIS: set lsp-refresh-interval to 700s
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.58 max-area-addresses

Function

Run the **max-area-addresses** command to configure the maximum number of area addresses.

Run the **no** form of this command to restore the default configuration.

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

Syntax

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

no max-area-addresses

Parameter Description

max-area- number: Maximum number of area addresses. The value range is from 3 to 6.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

Generally, an IS-IS process is configured with a Network Entry Title (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 devices, neighbor relationship can be created between the routers only when the maximum numbers of area addresses are the same.

Examples

The following example sets the maximum number of area addresses to **5**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# max-area-addresses 5
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.59 maximum-paths

Function

Run the **maximum-paths** command to configure the maximum number of IS-IS equal-cost paths to be added to a routing table.

Run the **no** form of this command to restore the default configuration.

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

Syntax

maximum-paths *maximum*

no maximum-paths

Parameter Description

maximum: Maximum number of IS-IS equal-cost routes to be added to a routing table. The value range is from 1 to 32.

Command Modes

IS-IS routing process configuration mode

IS-IS IPv6 address family configuration mode

Default Level

14

Usage Guidelines

This command is used by IS-IS to control the number of IS-IS equal-cost paths to be added to a routing table. The routing table also has a 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.

Examples

The following example sets the maximum number of IS-IS IPv4 equal-cost routes to be added to a routing table to **5**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# maximum-paths 5
```

The following example sets the maximum number of IS-IS IPv6 equal-cost routes to be added to a routing table to **6**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# address-family ipv6
Hostname(config-router-af)# maximum-paths 6
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.60 max-lsp-lifetime

Function

Run the **max-lsp-lifetime** command to configure the maximum LSP lifetime.

Run the **no** form of this command to restore the default configuration.

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

Syntax

max-lsp-lifetime *max-lifetime*

no max-lsp-lifetime

Parameter Description

max-lifetime: Maximum LSP lifetime, in seconds. The value range is from 1 to 65535.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

The maximum LSP lifetime must be at least 300s greater than the LSP refresh interval. If the difference of the configured LSP lifetime *max-lifetime* from the LSP refresh interval *interval* is less than 300s, the value of *max-lifetime* minus 300s is used as the LSP refresh interval.

Examples

The following example sets the maximum LSP lifetime to **1200** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# max-lsp-lifetime 1200
```

Notifications

If the difference of the configured maximum LSP lifetime from the LSP refresh interval is less than 300s, for example, the maximum LSP lifetime is 1000 and the LSP refresh interval is 900, the following notification will be displayed:

```
% ISIS: max-lsp-lifetime should be 300s greater than lsp-refresh-interval
% ISIS: set lsp-refresh-interval to 700s
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.61 max-metric on-neighbor-up

Function

Run the **max-metric on-neighbor-up** command to configure the maximum metric for the directly-connected routes after the first neighbor is up.

Run the **no** form of this command to remove this configuration.

The metric of the directly-connected route is not modified by default after the first neighbor is up.

Syntax

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

```
no max-metric on-neighbor-up
```

Parameter Description

delay-time: Delay for configuring the maximum metric for the directly-connected routes after the first neighbor is up, in seconds. The value range is from 5 to 1800.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

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 routing is reachable but the Overlay tunnel may not be created, which may lead to traffic interruption. In this case, run this command to prevent traffic interruption. According to the metric type, the maximum metric for Narrow is 63 and for Wide is 16777214.

Examples

The following example sets the delay for configuring the maximum metric for the directly-connected routes to **100** seconds after the first neighbor is up.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# max-metric on-neighbor-up 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.62 metric-style

Function

Run the **metric-style** command to configure a metric type.

Run the **no** form of this command to restore the default configuration.

The narrow metric type is used by default.

Syntax

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

```
no metric-style { narrow | wide } [ transition ] [ level-1 | level-1-2 | level-2 ]
```

Parameter Description

narrow: Uses the narrow metric type. The value range of interface metrics is from 1 to 63.

wide: Uses the wide metric type. The value range of interface metrics is from 1 to 16777214.

transition: Allows a device to send and receive narrow and wide metric types.

level-1: Takes effect for Level-1 interface.

level-1-2: Takes effect for Level-1 and Level-2 interfaces.

level-2: Takes effect for Level-2 interface.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

When the metric type is Narrow, run the **isis metric** command to configure metric values of an interface.

When the metric type is Wide or Transition, run the **isis wide-metric** command to configure metric values of an interface.

Examples

The following example configures the metric type as Wide.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# metric-style wide
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- [isis metric](#)
- [isis wide-metric](#)

1.63 min-lsp-arrival

Function

Run the **min-lsp-arrival** command to configure the delay for receiving duplicate LSPs.

Run the **no** form of this command to remove this configuration.

The function of delaying receiving duplicate LSPs packets is not supported on Level-1 and Level-2 by default.

Syntax

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

no min-lsp-arrival [**level-1** | **level-2**]

Parameter Description

level-1: Takes effect for Level-1 IS-IS LSPs.

level-2: Takes effect for Level-2 IS-IS LSPs.

minimum-interval: Minimum interval for receiving two duplicate LSP packets, in seconds. The value range is from 1 to 120.

initial-interval: Interval for receiving duplicate LSP packets for the first time, in milliseconds. The value range is 0 to 60000.

hold-interval: Minimum interval for receiving duplicate LSP packets for the first and second times, in milliseconds. The value range is 10 to 60000.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

If the **level-1** or **level-2** parameter is not specified when the command is configured, the interval configuration takes effect for Level-1 and Level-2 CSNPs.

The interval for receiving duplicate LSP packets for the first time is the *initial-interval*. When the interval for receiving duplicate LSP packets is less than the *minimum-interval*, the interval for receiving duplicate LSP packets for the second time becomes the *hold-interval*. In addition, a corresponding penalty is added to this interval: The next interval for receiving duplicate LSP packets doubles the previous interval for receiving the same LSP packets, until this interval reaches the *minimum-interval*. The interval for receiving duplicate LSP packets is changed to *minimum-interval*. When the network becomes stable, the interval for receiving duplicate LSP packets becomes greater than the *minimum-interval*, and the delay for receiving duplicate LSP packets is restored to the *initial-interval*.

Link changes have high requirements for convergence. The *initial-interval* can be set to a small value. You can also appropriately increase the values of the preceding parameters to reduce the CPU usage.

Note

- The value of the configured *hold-interval* cannot be greater than that of *minimum-interval*. Otherwise, the value of *hold-interval* is changed to that of *minimum-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*.
-

Examples

The following example sets the minimum interval of receiving duplicate LSP packets to **10** seconds, the interval of receiving duplicate LSP packets for the first time to **100** ms, and the interval of receiving duplicate LSP packets for the first and second times to **200** ms.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# min-lsp-arrival 10 100 200
```

Notifications

If the configured value of *hold-interval* is greater than the *minimum-interval* (for example, the configured value of *hold-interval* is 1500 ms, and the *minimum-interval* is 1 second), the following notification will be displayed:

```
% ISIS: hold_interval (1500ms) should be no more than minimum_interval (1s), set to (1000ms).
```

If the configured value of *initial-interval* is greater than the *hold-interval* (for example, the configured value of *initial-interval* is 20 ms, and the *hold-interval* is 10 ms), the following notification will be displayed:

```
% ISIS: initial_interval (20ms) should be no more than hold_interval (10ms), set to (10ms).
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.64 multi-topology

Function

Run the **multi-topology** command to configure IS-IS to support IPv6 unicast topologies. After that, IPv4 and IPv6 unicast routes in IS-IS will be calculated based on different topologies.

Run the **no** form of this command to restore the default configuration.

IS-IS does not support IPv6 unicast topologies by default.

Syntax

```
multi-topology [ transition ]
```

```
no multi-topology [ transition ]
```

Parameter Description

transition: Configures the MT mode, which supports smooth migration from an IPv4/IPv6 hybrid topology to separate IPv4 and IPv6 topologies.

Command Modes

IS-IS IPv6 address family configuration mode

Default Level

14

Usage Guidelines

The configuration of this command is applied in the following scenarios:

- If this command is not configured, IPv4 and IPv6 share the same IS-IS physical topology. This is a default

topology.

- If this command is configured without the **transition** parameter, the router runs in MT mode, and IS-IS IPv4 runs in the default topology and IS-IS IPv6 runs in the IPv6 unicast topology.
- If this command is configured with the **transition** parameter, the router runs in MTT mode, and IS-IS IPv6 runs in the default topology and the IPv6 unicast topology.

The routers in MTT mode can **transfer** the MT TLV or the default topology TLV. The MTT mode is applicable to incremental deployment to ensure smooth network migration. The MTT mode can cause route leaking between the default topology and IPv6 unicast topology. If the MTT mode is configured improperly, network failures such as routing black holes and loops may occur.

The metric type must be set to Wide or Transition before you run this command. The MTR feature will be disabled if the metric type is set to Narrow or only one Level is configured to support the Wide or Transition mode.

Examples

The following example configures IS-IS to support IPv6 unicast topologies.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# address-family ipv6
Hostname(config-router-af)# multi-topology
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- [address-family ipv6](#)
- [metric-style](#)

1.65 net

Function

Run the **net** command to configure a NET address in IS-IS.

Run the **no** form of this command to remove this configuration.

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

Syntax

net *net-address*

no net *net-address*

Parameter Description

net-address: NET address, in the format of XX.XXXX.YYYY.YYYY.YYYY.00. In this format, XX.XXXX indicates the area ID and YYYY.YYYY.YYYY indicates the system ID.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

Use this command to configure an area ID and a system ID in IS-IS.

Different NET addresses must have the same system ID.

Examples

The following example sets the NET address of IS-IS to 49.0000.0001.0002.0003.00.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# net 49.0000.0001.0002.0003.00
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.66 nsr

Function

Run the **nsr** command to enable the NSR function for current IS-IS instance.

Run the **no** form of this command to restore the default configuration.

The NSR function is disabled by default.

Syntax

nsr

no nsr

Parameter Description

N/A

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

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 slave 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. Information that should be backed up includes the neighbor relationship and link state.

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.

Examples

The following example enables the NSR function for current IS-IS instance.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis 1
Hostname(config-router)# nsr
```

Notifications

N/A

Common Errors

- If the neighbor keepalive duration is short, when fast hello is enabled, IS-IS neighbor relationship is disconnected during a switchover, causing forwarding interruption.

Platform Description

N/A

Related Commands

- [show isis protocol](#)
- [show isis nsr](#)

1.67 passive-interface

Function

Run the **passive-interface** command to configure a passive interface.

Run the **no** form of this command to restore the default configuration.

The passive interface function is not enabled by default.

Syntax

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

```
no passive-interface { default | interface-type interface-number }
```

Parameter Description

default: Configures all IS-IS interfaces that are not enabled as passive interfaces.

interface-type: Interface type.

interface-number: Interface number.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

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. 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.

Examples

The following examples configures TenGigabitEthernet 0/1 as a passive interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis 1
Hostname(config-router)# passive-interface tenGigabitEthernet 0/1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.68 redistribute

Function

Run the **redistribute** command to redistribute other routes to IS-IS.

Run the **no** form of this command to remove this configuration.

Redistribution is disabled by default.

Syntax

```
redistribute { bgp | connected | ospf process-id [ match { external [ 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 ] *
```

```
no redistribute { bgp | connected | ospf process-id [ match { external [ 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 ] *
```

Parameter Description

bgp: Indicates redistribution from BGP.

connected: Indicates redistribution from direct routes.

ospf *process-id*: Performs redistribution from OSPF. *process-id* specifies an OSPF process. The value range is from 1 to 65535 and the default value is 1.

match { **external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**] } *: Filters route sub-types of OSPF during OSPF route redistribution. If the **match** parameter is not included, all route sub-types of OSPF are received. If **1** or **2** is not specified after **match external**, OSPF routes of **external 1** and **external 2** are redistributed. If **1** or **2** is not specified after **match nssa-external**, OSPF routes of **nssa-external 1** and **nssa-external 2** are redistributed.

match: Redistributes specific OSPFv3 routes that meet the filtering conditions.

external [**1** | **2**]: Redistributes E1, E2, or all external routes.

internal: Redistributes internal routes and inter-area routes.

nssa-external [**1** | **2**]: Redistributes N1, N2, or all external routes of all NSSAs.

rip: Indicates redistribution from RIP.

static: Indicates redistribution from static routes.

level-1 | **level-1-2** | **level-2**: Indicates the Level of redistributed routes received by IS-IS. If no Level is specified, routes are redistributed to Level-2.

level-1: Redistributes routes to Level-1.

level-1-2: Redistributes routes to Level-1 and Level-2.

level-2: Redistributes routes to Level-2.

metric *metric-value*: Sets the metric of a redistributed route. The value range is from 0 to 4261412864. The metric of external routes is used when the **metric** option is not specified.

metric-type { external | internal }: Indicates the metric type of redistributed routes. If no metric type is specified, the metric belongs to the **internal** type.

external: Indicates that the metric belongs to the external type.

internal: Indicates that the metric belongs to the internal type.

route-map *route-map-name*: Indicates the route map used for external route redistribution. It is used to filter redistributed routes or configure the attributes of the redistributed routes. The value of *route-map-name* cannot exceed 32 characters. No route map is configured by default.

Command Modes

IS-IS routing process configuration mode

IS-IS IPv6 address family configuration mode

Default Level

14

Usage Guidelines

Run the **no redistribute { bgp | connected | ospf *processs-id* | rip | static }** command to cancel the redistribution of routes mapped to the specified protocol. If **no redistribute** is followed by other parameters, the command will restore the default configuration, rather than cancel route redistribution. For example: **no redistribute bgp** cancels BGP route redistribution, whereas **no redistribute bgp route-map aa** cancels the route map named **aa** associated with BGP route redistribution.

When external routes are redistributed in IPv4 mode, the routing information is stored in LSPs' IP External Reachability Information TLV.

When external routes are redistributed in IPv6 mode, the routing information is stored in LSPs' IPv6 Reachable TLV.

In the old versions of some vendors, if the metric type is set to **external**, the metric of redistributed routes is added by 64 during route calculation and routes are selected based on the metric. 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 value or metric type) of each device to ensure that internal routes are preferred over external routes.

Examples

The following example redistributes static routes to Level-1 of the current instance and sets the metric value to **10**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# redistribute static metric 10 level-1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- [show isis protocol](#)

1.69 redistribute isis level-1 into level-2

Function

Run the **redistribute isis level-1 into level-2** command to redistribute the Level-1 reachable routing information of the specified IS-IS instance to Level-2 of the current instance.

Run the **no** form of this command to remove this configuration.

All Level-1 routes will be automatically redistributed to Level-2 by default.

Syntax

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

```
no redistribute isis [ tag ] level-1 into level-2 [ distribute-list acl-name | route-map route-map-name ]
```

Parameter Description

tag: Name of the IS-IS instance whose routing information will be redistributed. **distribute-list** *acl-name*: Filters redistributed routes by using **distribute-list**. *acl-name* indicates the associated prefix list, which can be a standard, an extended, or a name prefix list. The format is as follows:

```
{ <1-99> | <100-199> | <1300-1999> | <2000-2699> | acl-name }
```

In IS-IS IPv6 address family configuration mode, only the name prefix list can be used, in the format of *acl-name*.

route-map *route-map-name*: Indicates the route map used for route redistribution. It is used to filter redistributed routes or configure the attributes of redistributed routes. The value of *route-map-name* cannot exceed 32 characters. No route map is configured by default.

Command Modes

IS-IS routing process configuration mode

IS-IS IPv6 address family configuration mode

Default Level

14

Usage Guidelines

You can use the **route-map** or **distribute-list** parameter to filter the specified instance's Level-1 routes to be redistributed. Only the routes that meet specific criteria can be redistributed to Level-2 of the current instance. The **route-map** and **distribute-list** parameters cannot be used at the same time.

The **no redistribute isis [tag] level-2 into level-1** command is used to cancel the redistribution of the specified instance's routes. If **no redistribute** is followed by other parameters, the command will restore the default configuration, rather than cancel route redistribution.

For example, **no redistribute isis tag1 level-1 into level-2** cancels the redistribution of the routes of the IS-IS instance name *tag1*. **no redistribute isis tag1 level-1 into level-2 route-map aa** cancels the use of the route map named *aa* to filter redistributed routes.

Examples

The following example redistributes the Level-1 reachable routing information of the specified IS-IS instance to Level-2 of the current instance.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis aa
Hostname(config-router)# redistribute isis bb level-1 into level-2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- [show isis protocol](#)

1.70 redistribute isis level-2 into level-1

Function

Run the **redistribute isis level-2 into level-1** command to redistribute the Level-2 reachable routing information of the specified IS-IS instance to Level-1 of the current instance.

Run the **no** form of this command to remove this configuration.

Redistribution is disabled by default.

Syntax

```
redistribute isis [ tag ] level-2 into level-1 [distribute-list acl-name | { prefix ipv4-address net-mask| ipv6-prefix ipv6-address/length} | route-map route-map-name ]
```

```
no redistribute isis [ tag ] level-2 into level-1 [ distribute-list acl-name | { prefix ipv4-address net-mask| ipv6-prefix ipv6-address/length} | route-map route-map-name ]
```

Parameter Description

tag: Name of the IS-IS instance whose routing information will be redistributed.

distribute-list acl-name: Filters redistributed routes by using **distribute-list**. *access-list-name* indicates the associated prefix list, which can be a standard, an extended, or a name prefix list. The format is as follows:

```
{ <1-99> | <100-199> | <1300-1999> | <2000-2699> | acl-name }
```

In IS-IS IPv6 address family configuration mode, only the name prefix list can be used, in the format of *acl-name*.

prefix *ipv4-address net-mask*: Configures IPv4 routes that can be redistributed. Routes are specified by address and prefix length.

ipv6-prefix *ipv6-address/length*: Configures IPv6 routes that can be redistributed. Routes are specified by address and prefix length.

route-map *route-map-name*: Indicates the route map used for route redistribution. It is used to filter redistributed routes or configure the attributes of redistributed routes. The value of *route-map-name* cannot exceed 32 characters. No route map is configured by default.

Command Modes

IS-IS routing process configuration mode

IS-IS IPv6 address family configuration mode

Default Level

14

Usage Guidelines

You can use the **route-map**, **distribute-list**, or **prefix** parameter to filter the specified instance's Level-2 routes to be redistributed. Only the routes that meet specific criteria can be redistributed to Level-1 of the current instance.

The **route-map**, **distribute-list**, and **prefix** parameters cannot be used at the same time. If routes are filtered based on the prefix, only the Level-2 routes of local instance can be filtered.

The **no redistribue isis [tag] level-2 into level-1** command is used to cancel the redistribution of the specified instance's routes. If **no redistribute** is followed by other parameters, the command will restore the default configuration, rather than cancel route redistribution.

For example:

no redistribue isis tag1 level-2 into level-1 cancels the redistribution of the routes of the IS-IS instance name tag1. **no redistribue isis tag1 level-2 into level-1 route-map aa** cancels the use of the route map named aa to filter redistributed routes, rather than redistribution of the routes of the IS-IS instance name tag1.

Examples

The following example redistributes the Level-2 reachable routing information of the specified IS-IS instance to Level-1 of the current instance.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis aa
Hostname(config-router)# redistribute isis bb level-2 into level-1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- [show isis protocol](#)

1.71 router isis

Function

Run the **router isis** command to create an IS-IS instance.

Run the **no** form of this command to remove this configuration.

No IS-IS instance is configured by default.

Syntax

router isis [*tag*]

no router isis [*tag*]

Parameter Description

tag: Name of an IS-IS instance.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Use this command to initialize an IS-IS instance and enter IS-IS routing process configuration mode. An IS-IS instance will start running after a NET address is configured.

If you set the tag parameter when you start an IS-IS routing process, you need to add the tag parameter when closing the IS-IS routing process.

CPU protection is enabled by default. For packets sent to each destination group address (AllISSystems, AllL1ISSystems, and AllL2ISSystems), the number of packets sent to the CPU is limited to 400 per second. If a device has many neighbor relationships or sends Hello packets at short intervals, the IS-IS packets that the device receives may exceed the default limit, causing frequent flapping of neighbor relationships. To solve the problem, you can use the CPU protection command in global configuration mode to increase the limit.

Examples

The following example creates an IS-IS instance.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# router isis
Hostname(config-router)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.72 set-overload-bit

Function

Run the **set-overload-bit** command to prevent neighbors from using the local IS-IS node as a forwarding device to forward data.

Run the **no** form of this command to remove this configuration.

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

Syntax

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

```
no set-overload-bit [ level-1 | level-2 ]
```

Parameter Description

on-startup: Indicates that an IS-IS node enters overload state temporarily after restart.

overload-time: Duration when an IS-IS node remains in overload state after restart, in seconds. The value range is from 5 to 86400, and the default value is **600**.

wait-for-bgp: Indicates that an IS-IS node automatically enters overload state after restart and waits for BGP convergence completion or timeout. This option is used with the keyword **on-startup**.

bgp-convergence-time: Time for waiting for BGP convergence completion, in seconds. The value range is from 5 to 86400, and the default value is **600**.

suppress: Indicates that an IS-IS node does not advertise internal routes (intra-area and inter-area routes) or external routes to neighbors when the IS-IS node is in overload state.

external: Indicates that an IS-IS node does not advertise external routes to neighbors when the IS-IS node is in overload state. This option is used with the keyword **suppress**.

interlevel: Indicates that an IS-IS node does not advertise intra-area and inter-area routes to neighbors when the IS-IS node is in overload state. This option is used with the keyword **suppress**.

max-metric: Sets the metric values of the advertised direct routes and neighbor reachable routes to the maximum values when the IS-IS node is in overload state. This option is used with the keyword **suppress**.

level-1: Sends LSPs with the overload bit only to Level-1 neighbors.

level-2: Sends LSPs with the overload bit only to Level-2 neighbors.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

This command forces an IS-IS node to configure the overload bit in non-virtual LSPs to instruct its IS-IS neighbors to avoid using the local node as a forwarding device.

If the **on-startup** keyword is included, the IS-IS node temporarily enters overload state after restart. The overload bit is automatically configured or removed by the IS-IS node based on configuration.

If the **on-startup** keyword is not included, the IS-IS node enters overload state immediately after restart. The overload bit is configured or removed manually.

Note

At the same Level, the configuration with the **on-startup** keyword and the configuration without the **on-startup** keyword are mutually exclusive.

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.

The timer is configured based on the number of routes in the network. If there are a great number of routes in the network, the timer is set to a larger value. Otherwise, the timer is set to a smaller value.

- 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.

Examples

The following example enables an IS-IS node to automatically enter overload state after restart and not to advertise internal routes (intra-area and inter-area routes) or external routes to neighbors in the wait time 300s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# set-overload-bit on-startup 300 suppress interlevel
external
```

The following example enables an IS-IS node not to advertise internal routes (intra-area and inter-area routes) or external routes to neighbors when the IS-IS node is in overload state.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# set-overload-bit suppress interlevel external
```

The following example enables an IS-IS node to automatically enter overload state after restart, wait for 300s, BGP route convergence completion or specified timer timeout, and set the metric values of the advertised direct routes and neighbor reachable routes to the maximum values.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# set-overload-bit on-startup wait-for-bgp 300 suppress
max-metric
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- [show isis database](#)

1.73 show clns is-neighbors

Function

Run the **show clns is-neighbors** command to display all IS-IS neighbors and provide device adjacency relationship information.

Syntax

```
show clns [ tag ] is-neighbors [ interface-type interface-number ] [ detail ]
```

Parameter Description

tag: Name of a specified IS-IS instance.

interface-type interface-number: Name of a specified interface.

detail: Displays detailed information of all interfaces.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays all IS-IS neighbors and provides device adjacency relationship information.

```
Hostname> enable
Hostname# show clns is-neighbors detail
Area (null):
System Id   Type   IP Address   State   Holdtime   Circuit   Interface
r1          L1    1.0.0.2     Up      9          r1.01    TenGigabitEthernet 0/1
L2         1.0.0.2   Up      9          r1.01    TenGigabitEthernet 0/1
Adjacency ID: 1
Uptime: 00:00:54
Area Address(es): 49.1111
SNPA: 00d0.f8bc.de08
IPv6 Address(es): fe80::2a9:15ff:fe36:5413
Level-1 MTID: Standard
Level-2 MTID: Standard
Level-1 Protocols Supported: IPv4, IPv6
Level-2 Protocols Supported: IPv4, IPv6
BFD(IPv4) session state: Up
BFD(IPv6) session state: Up
```

Table 1-1 Output Fields of the show clns is-neighbors detail Command

Field	Description
Area	Instance tag
System Id	System ID
Type	Neighbor type
IP Address	IP address of the neighbor
State	State of the neighbor
Holdtime	Holdtime of the neighbor
Circuit	Link ID
Interface	Interface for neighbor establishment
Adjacency ID	Neighbor ID, arranged based on interface. The value range is from 1 to 255.
Uptime	Uptime of a neighbor connection
Area Address(es)	Area address
SNPA	SNPA address of the neighbor
IPv6 Address(es)	IPv6 address of the neighbor
Level-1 MTID	Topology mode of the Level-1 neighbor
Level-2 MTID	Topology mode of the Level-2 neighbor
Level-1 Protocols Supported	IP protocol type supported by the Level-1 neighbor
Level-2 Protocols Supported	IP protocol type supported by the Level-2 neighbor
BFD (IPv4) session state	BFDv4 session status corresponding to the IS-IS neighbor
BFD (IPv6) session state	BFDv6 session status corresponding to the IS-IS neighbor

Notifications

N/A

Platform Description

N/A

1.74 show clns neighbors**Function**

Run the **show clns neighbors** command to display all IS-IS neighbors and provide device information and adjacency relationship information about terminals.

Syntax

```
show clns [ tag ] neighbors [ interface-type interface-number ] [ detail ]
```

Parameter Description

tag: Name of a specified IS-IS instance.

interface-type interface-number: Name of a specified interface.

detail: Displays detailed information of all interfaces.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays all IS neighbors and provides device information and adjacency relationship information about terminals.

```

Hostname> enable
Hostname# show clns neighbors detail
Area (null):
System Id      SNPA                State  Holdtime  Type Protocol Interface
r1             00d0.f8bc.de08      Up     7         L1   IS-IS
TenGigabitEthernet 0/1
                                   Up     9         L2   IS-IS
TenGigabitEthernet 0/1
  Adjacency ID: 1
  Uptime: 00:01:40
  Area Address(es): 49.1111
IP Address(es): 1.0.0.2
IPv6 Address(es): fe80::2a9:15ff:fe36:5413
Level-1 MTID: Standard
Level-2 MTID: Standard
  Level-1 Protocols Supported: IPv4, IPv6
  Level-2 Protocols Supported: IPv4, IPv6
BFD(IPv4) session state: Up
BFD(IPv6) session state: Up

```

Table 1-1 Output Fields of the show clns neighbors detail Command

Field	Description
Area	Instance tag
System Id	System ID

Field	Description
SNPA	SNPA address of the neighbor
State	State of the neighbor
Holdtime	Holdtime of the neighbor
Type	Neighbor type
Protocol	Protocol type
Interface	Interface for neighbor establishment
Adjacency ID	Neighbor ID, arranged based on interface. The value range is from 1 to 255.
Uptime	Uptime of a neighbor connection
Area Address(es)	Area address
IP Address(es)	IP Address
IPv6 Address(es)	IPv6 address of the neighbor
Level-1 MTID	Topology mode of the Level-1 neighbor
Level-2 MTID	Topology mode of the Level-2 neighbor
Level-1 Protocols Supported	IP protocol type supported by the Level-1 neighbor
Level-2 Protocols Supported	IP protocol type supported by the Level-2 neighbor
BFD (IPv4) session state	BFDv4 session status corresponding to the IS-IS neighbor
BFD (IPv6) session state	BFDv6 session status corresponding to the IS-IS neighbor

Notifications

N/A

Platform Description

N/A

1.75 show isis counter

Function

Run the **show isis counter** command to display statistical information of IS-IS.

Syntax

```
show isis [ tag ] counter
```

Parameter Description

Tag: Name of an IS-IS instance.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example display statistical information of IS-IS.

```
Hostname> enable
Hostname# show isis counter
Area (null):
IS-IS Level-1 isisSystemCounterEntry:
isisSysStatCorrLSPs: 0
isisSysStatAuthTypeFails: 0
isisSysStatAuthFails: 0
isisSysStatLSPDbaseOloads: 0
isisSysStatManAddrDropFromAreas: 0
isisSysStatAttmptToExMaxSeqNums: 0
isisSysStatSeqNumSkips: 0
isisSysStatOwnLSPPurges: 0
isisSysStatIDFieldLenMismatches: 0
isisSysStatMaxAreaAddrMismatches: 0
isisSysStatPartChanges: 0
isisSysStatSPFRuns: 30
isisSysStatLSPErrors: 0
IS-IS Level-2 isisSystemCounterEntry:
isisSysStatCorrLSPs: 0
isisSysStatAuthTypeFails: 0
isisSysStatAuthFails: 0
isisSysStatLSPDbaseOloads: 0
isisSysStatManAddrDropFromAreas: 0
isisSysStatAttmptToExMaxSeqNums: 0
isisSysStatSeqNumSkips: 0
isisSysStatOwnLSPPurges: 0
isisSysStatIDFieldLenMismatches: 0
isisSysStatMaxAreaAddrMismatches: 0
isisSysStatPartChanges: 0
isisSysStatSPFRuns: 30
isisSysStatLSPErrors: 0
```

Table 1-1 Output Fields of the show isis counter Command

Field	Description
Area	Instance tag
IS-IS Level-1 isisSystemCounterEntry	Statistical table of the Level-1 system
isisSysStatCorrLSPs	Number of LSPs with length error
isisSysStatAuthTypeFails	Number of authentication failures with type error
isisSysStatAuthFails	Number of authentication failures with password inconsistency
isisSysStatLSPDbaseOloads	Number of overload times of the LSP database
isisSysStatManAddrDropFromAreas	Number of invalid area address drop times
isisSysStatAtmptToExMaxSeqNums	Number of LSP SNs exceeding maximum values
isisSysStatSeqNumSkips	Number of LSP SN skip times
isisSysStatOwnLSPPurges	Number of local failed LSPs
isisSysStatIDFieldLenMismatches	Number of system ID length mismatches
isisSysStatMaxAreaAddrMismatches	Number of maximum area address mismatches
isisSysStatPartChanges	Number of partition change times
isisSysStatSPFRuns	Number of SPF computation times
isisSysStatLSPErrors	Number of incorrect LSPs

Notifications

N/A

Platform Description

N/A

1.76 show isis database**Function**

Run the **show isis database** command to display the information of an LSP database.

Syntax

```
show isis [ tag ] database [ detail | verbose ] [ I1 | I2 | level-1 | level-2 ] [ LSPID ]
```

Parameter Description

tag: Name of a specified IS-IS instance.

detail: Displays detailed information.

verbose: Displays more detailed information than **detail**.

I1 | I2 | level-1 | level-2: **I1** and **level-1:** Specify the Level-1 LSP database. **I2** and **level-2:** Specify the Level-2 LSP database.

LSPID: ID of the specified LSP. Only the corresponding LSP information is displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the information of an LSP database.

```

Hostname> enable
Hostname# show isis database detail
Area (null):
IS-IS Level-1 Link State Database:
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
-----
Hostname.00-00 * 0x00000007  0xCDD5        1011          0/0/0
  Area Address: 49.1111
  NLPID:        0xCC
  Hostname:     Hostname
  IP Address:   1.0.0.1
  Metric: 10    IS r1.01
  Metric: 10    IP 1.0.0.0 255.255.255.0
r1.00-00        0x00000006  0xA771        1032          0/0/0
  Area Address: 49.1111
  NLPID:        0xCC
  Hostname:     r1
  IP Address:   1.0.0.2
  Metric: 10    IS r1.01
  Metric: 10    IP 1.0.0.0 255.255.255.0
r1.01-00        0x00000002  0x062A        989           0/0/0
  Metric: 0     IS r1.00
  Metric: 0     IS Hostname.00
IS-IS Level-2 Link State Database:
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
-----
Hostname.00-00 * 0x0000000A  0xC7D8        1033          0/0/0
  Area Address: 49.1111
  NLPID:        0xCC
  Hostname:     Hostname
  IP Address:   1.0.0.1
  Metric: 10    IS r1.01

```

```

Metric: 10          IP 1.0.0.0 255.255.255.0
r1.00-00          0x00000006 0xA771          1032          0/0/0
Area Address: 49.1111
NLPID:          0xCC
Hostname:       r1
IP Address:     1.0.0.2
Metric: 10          IS r1.01
Metric: 10          IP 1.0.0.0 255.255.255.0
r1.01-00          0x00000002 0x062A          989          0/0/0
Metric: 0          IS r1.00
Metric: 0          IS Hostname.00

```

Table 1-1 Output Fields of the show isis database detail Command

Field	Description
Area	Instance tag
IS-IS Level-1 Link State Database	Level-1 LSDB
LSPID	LSP ID
LSP Seq Num	LSP SN
LSP Checksum	LSP checksum
LSP Holdtime	LSP holdtime
ATT	Additional bit
P	Split bit
OL	Overload bit
Area Address	Area address
NLPID	Protocol supported by ISIS. 0xCC indicates the IP protocol.
Hostname	Host name
IP Address	IP address
Metric	Metric

The following example displays the STLV information of an LSP database.

```

Hostname> enable
Hostname# show isis database verbose
IS-IS Level-1 Link State Database
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime  TT/P/OL
1111.1111.1111.00-00  0x00000005  0xB56A        1000          0/0/0
Area Address: 49
NLPID:         0xCC

```

```

Hostname: r1
Router ID: 1.1.1.1
IP Address: 192.17.10.2
Metric: 10      IP  192.17.10.0/24
1111.1111.1111.01-00  0x00000002      0xBDCA      1020      0/0/0
Metric: 10      IS-Extended 1111.1111.1111.00
Affinity: 0x00000000
Interface IP address: 192.17.10.2
Physical BW: 10000000 bits/sec
Reservable BW: 1000000 bits/sec
BW Unreserved[0]: 1000000 bits/sec, BW Unreserved[1]: 1000000 bits/sec
BW Unreserved[2]: 1000000 bits/sec, BW Unreserved[3]: 1000000 bits/sec
BW Unreserved[4]: 1000000 bits/sec, BW Unreserved[5]: 1000000 bits/sec
BW Unreserved[6]: 1000000 bits/sec, BW Unreserved[7]: 1000000 bits/sec

```

Table 1-2Output Fields of the show isis database verbose Command

Field	Description
LSPID	LSP ID
LSP Seq Num	LSP SN
LSP Checksum	LSP checksum
LSP Holdtime	LSP holdtime
ATT	Additional bit
P	Split bit
OL	Overload bit
Area Address	Area address that this device can reach
NLPID	Network protocol ID
Hostname	Host name of the node
Router ID	TE router ID of the node
IP Address	IPv4 address of the interface
Metric	IS-IS metric
Affinity	Management group attribute described in the link
Physical BW	Actual bandwidth of the link
Reservable BW	Reserved bandwidth of the link
BW Unreserved	Reserved bandwidth for current priority

Notifications

N/A

Platform Description

N/A

1.77 show isis graceful-restart

Function

Run the **show isis graceful-restart** command to display the state information about IS-IS GR.

Syntax

```
show isis [ tag ] graceful-restart
```

Parameter Description

tag: Name of an IS-IS instance.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the state information about IS-IS GR.

```
Hostname> enable
Hostname# show isis graceful-restart
Area (null):
  Graceful-restart Helper: enabled
  Level 1:
    TenGigabitEthernet 0/1: RR received: 0
  Level 2:
    TenGigabitEthernet 0/1: RR received: 0
Graceful-restart: enabled
Graceful-period: 400s, Level timer: 60s, Interface timer: 3s
Instance GR status: not restarting
```

Table 1-1 Output Fields of the show isis graceful-restart Command

Field	Description
Graceful-restart	Configuration state of the GR Restarter
Graceful-period	GR timer time
Level timer	Level-based timer time
Interface timer	Interface-based timer time
Graceful-restart Helper	Configuration state of the GR Helper
RR received	Statistics on received hello packets with the RR field
Instance GR status	GR state of the IS-IS instance

Notifications

N/A

Platform Description

N/A

1.78 show isis hostname**Function**

Run the **show isis hostname** command to display the mapping of a host name to a system ID.

Syntax

```
show isis [ tag ] hostname
```

Parameter Description

tag: Name of a specified IS-IS instance.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the mapping of a host name to a system ID.

```
Hostname> enable
Hostname# show isis hostname
```

```

System ID      Dynamic Hostname      Area (null)
* 5555.5555.5555 Hostname
1111.1111.1111 R1
System ID      Dynamic Hostname      Area 1
* 4444.4444.4444 Hostname
2222.2222.2222 R2

```

Table 1-1 Output Fields of the show isis hostname Command

Field	Description
System ID	System ID <ul style="list-style-type: none"> ● If the system ID is marked with an asterisk (*), the mapping of the local host name to a system ID is learned. ● If the system ID is not marked with an asterisk (*), the mapping of a non-local host name to a system ID is learned.
Dynamic Hostname	Host name
Area	Instance tag

Notifications

N/A

Platform Description

N/A

1.79 show isis interface**Function**

Run the **show isis interface** command to display details of an IS-IS interface.

Syntax

```
show isis [ tag ] interface [ interface-type interface-number ] [ counter ]
```

Parameter Description

tag: Name of a specified IS-IS instance.

interface-type interface-number: Interface type and interface number.

counter: Specifies the number of packet sending and receiving trigger times.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the details of an IS-IS interface.

```

Hostname> enable
Hostname# show isis interface
Area (null):
TenGigabitEthernet 0/1 is up, line protocol is up
  Routing Protocol: IS-IS ((null))
    Network Type: Broadcast
    Circuit Type: level-2
    Local circuit ID: 0x01
    Extended Local circuit ID: 0x00000001
    Local SNPA: 00d0.f822.33ab
    IP interface address:
      1.0.0.1/24
    Level-1 MTID: Standard
Level-2 MTID: Standard
Level-1 Metric: 10/10, Priority: 64, Circuit ID: r1.01
Level-1 Timer intervals configured, Hello: 10s, Lsp: 33ms, Psnp: 2s, Csnp:10s,
Retransmit:5s
Level-1 LSPs in queue: 0
Level-1 LSPs flood: 5
  Number of active level-1 adjacencies: 1
Level-2 Metric: 10/10, Priority: 64, Circuit ID: r1.01
Level-2 Timer intervals configured, Hello: 10s, Lsp: 33ms, Psnp: 2s, Csnp:10s,
Retransmit:5s
Level-2 LSPs in queue: 0
Level-2 LSPs flood: 5
  Number of active level-2 adjacencies: 1
  Next IS-IS LAN Level-1 Hello in 5 seconds
Next IS-IS LAN Level-2 Hello in 5 seconds
IS-IS TE: Enable
BFD Enabled (Anti-congestion)

```

Table 1-1 Output Fields of the show isis interface Command

Field	Description
Area	Instance tag
Routing Protocol	Routing protocol running on the interface
Network Type	Network type
Circuit Type	Link type
Local circuit ID	Local link ID

Field	Description
Extended Local circuit ID	ID of extended local link
Local SNPA	Local SNPA address
IP interface address	IP address of the interface
Level-1 MTID	Topology mode of the interface at Level-1
Level-2 MTID	Topology mode of the interface at Level-2
Level-1 Metric	Level-1 metric
Priority	Priority
Circuit ID	Link ID
Hello	Hello timer configuration on the interface
Lsp	LSP timer configuration on the interface
Psnp	PSNP timer configuration on the interface
Csnp	CSNP timer configuration on the interface
Retransmit	LSP retransmission timer configuration on the interface
Level-1 LSPs in queue	Number of LSPs in Level-1 queue
Level-1 LSPs flood	Number of LSPs sent at a time at Level-1
Number of active level-1 adjacencies	Number of Level-1 neighbors
Level-2 Metric	Level-2 metric
Level-2 LSPs in queue	Number of LSPs in Level-2 queue
Level-2 LSPs flood	Number of LSPs sent at a time at Level-2
Number of active level-2 adjacencies	Number of Level-2 neighbors
Next IS-IS LAN Level-1 Hello in 5 seconds	Next Level-1 hello packet sending time
Next IS-IS LAN Level-2 Hello in 5 seconds	Next Level-2 hello packet sending time
BFD Enabled(Anti-congestion)	BFD session state. If Anti-congestion is included, the BFD anti-congestion function is enabled. Otherwise, the anti-congestion function is not enabled.

The following example displays the statistical information of an IS-IS interface.

```

Hostname> enable
Hostname# show isis interface counter
Area (null):
TenGigabitEthernet 0/1:
  IS-IS LAN Level-1 isisCircuitCounterEntry:
    isisCircAdjChanges: 4
    isisCircNumAdj: 2
    isisCircInitFails: 0
    isisCircRejAdjs: 0
    isisCircIDFieldLenMismatches: 0
    isisCircMaxAreaAddrMismatches: 0
    isisCircAuthTypeFails: 0
    isisCircAuthFails: 0
    isisCircLanDesISChanges: 1
  IS-IS LAN Level-2 isisCircuitCounterEntry:
    isisCircAdjChanges: 4
    isisCircNumAdj: 2
    isisCircInitFails: 0
    isisCircRejAdjs: 0
    isisCircIDFieldLenMismatches: 0
    isisCircMaxAreaAddrMismatches: 0
    isisCircAuthTypeFails: 0
    isisCircAuthFails: 0
    isisCircLanDesISChanges: 1
  IS-IS Level-1 isisPacketCounterEntry:
    isisPacketCountIIHello in/out: 187/278
    isisPacketCountLSP in/out: 10/7
    isisPacketCountCSNP in/out: 0/92
    isisPacketCountPSNP in/out: 0/0
    isisPacketCountUnknown in/out: 0/0
  IS-IS Level-2 isisPacketCounterEntry:
    isisPacketCountIIHello in/out: 186/286
    isisPacketCountLSP in/out: 17/9
    isisPacketCountCSNP in/out: 1/91
    isisPacketCountPSNP in/out: 0/0
    isisPacketCountUnknown in/out: 0/0

```

Table 1-2Output Fields of the show isis interface counter Command

Field	Description
IS-IS LAN Level-1 isisCircuitCounterEntry	Statistics of local Level-1 link
isisCircAdjChanges	Number of adjacency state change times on the local link

Field	Description
isisCircNumAdj	Number of adjacency times on the local link
isisCircInitFails	Number of initialization failure times on the local link
isisCircRejAdjs	Number of adjacency rejection times on the local link
isisCircIDFieldLenMismatches	Number of mismatches between the system ID in the received PDU and that in local system on the local link
isisCircMaxAreaAddrMismatches	Number of mismatches between the maximum number of area addresses in the received PDU and that in local system on the local link
isisCircAuthTypeFails	Number of mismatches between the authentication type in the received PDU and that in local system on the local link
isisCircAuthFails	Number of authentication failures due to mismatch of authentication passwords in the received PDU on the local link (authentication types match)
isisCircLanDeslSChanges	Number of DIS changes at this level on the broadcast link
IS-IS LAN Level-2 isisCircuitCounterEntry	Statistics of the local Level-2 link
IS-IS Level-1 isisPacketCounterEntry	Packet statistics of the local Level-1 link
isisPacketCountIIHello in/out	Statistics about hello packet sending and receiving on the local link
isisPacketCountLSP in/out	Statistics about LSP packet sending and receiving on the local link
isisPacketCountCSNP in/out	Statistics about CSNP packet sending and receiving on the local link
isisPacketCountPSNP in/out	Statistics about PSNP packet sending and receiving on the local link
isisPacketCountUnknown in/out	Statistics about unknown packet sending and receiving on the local link
IS-IS Level-2 isisPacketCounterEntry	Packet statistics of the local Level-2 link

Notifications

N/A

Platform Description

N/A

1.80 show isis ipv6 topology

Function

Run the **show isis ipv6 topology** command to display the IPv6 unicast topology information of an IS-IS device.

Syntax

```
show isis [ tag ] ipv6 topology [ I1 | I2 | level-1 | level-2 ]
```

Parameter Description

tag: Name of a specified IS-IS instance.

I1: Specifies Level-1 topology.

level-1: Specifies Level-1 topology.

I2: Specifies Level-2 topology.

level-2: Specifies Level-2 topology.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the IPv6 unicast topology information.

```

Hostname> enable
Hostname# show isis ipv6 topology
Area (null):
IS-IS paths to level-1 routers
System Id      Metric  Next-Hop  SNPA          Interface
r1              10      r1        00d0.f822.33ad  TenGigabitEthernet 0/1
Hostname       -N/A
IS-IS paths to level-2 routers
System Id      Metric  Next-Hop  SNPA          Interface
r1              10      r1        00d0.f822.33ad  TenGigabitEthernet 0/1
Hostname       -N/A

```

Table 1-1 Output Fields of the show isis ipv6 topology Command

Field	Description
Area	Instance tag
System Id	System ID

Field	Description
Metric	Metric
Next-Hop	Next hop
SNPA	SNPA address
Interface	Interface name

Notifications

N/A

Platform Description

N/A

1.81 show isis mesh-groups

Function

Run the **show isis mesh-groups** command to display the mesh group configuration of interfaces.

Syntax

```
show isis [ tag ] mesh-groups
```

Parameter Description

tag: Name of a specified IS-IS instance.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the mesh group configuration of all interfaces.

```
Hostname> enable
Hostname# show isis mesh-groups
Mesh group (blocked)
TenGigabitEthernet 0/1
Mesh group 1 :
TenGigabitEthernet 0/2
```

Table 1-1 Output Fields of the show isis mesh-groups Command

Field	Description
Mesh group (blocked) TenGigabitEthernet 0/1	Interface that blocks the mesh group
Mesh group 1 TenGigabitEthernet 0/2	Interface for mesh group 1

Notifications

-

Platform Description

N/A

1.82 show isis neighbors

Function

Run the **show isis neighbors** command to display neighbor information of IS-IS.

Syntax

```
show isis [ tag ] neighbors [ detail ]
```

Parameter Description

tag: Name of a specified IS-IS instance.

detail: Displays detailed information.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays detailed neighbor information of IS-IS.

```

Hostname> enable
Hostname# show isis neighbors detail
Area (null):
System Id  Type  IP Address      State  Holdtime  Circuit  Interface
r1         L1   1.0.0.2        Up     9         r1.01   TenGigabitEthernet 0/1
L2   1.0.0.2      Up     9         r1.01   TenGigabitEthernet 0/1

Adjacency ID: 1
Uptime: 00:06:25
Area Address(es): 49.1111

```

```

SNPA: 00d0.f8bc.de08
IPv6 Address(es): fe80::2a9:15ff:fe36:5413
Level-1 MTID: Standard
Level-2 MTID: Standard
  Level-1 Protocols Supported: IPv4, IPv6
  Level-2 Protocols Supported: IPv4, IPv6
BFD(IPv4) session state: Up
BFD(IPv6) session state: Up

```

Table 1-1 Output Fields of the show isis neighbors detail Command

Field	Description
Area	Instance tag
System Id	System ID
Type	Neighbor type
IP Address	IP address of the neighbor
State	State of the neighbor
Holdtime	Holdtime of the neighbor
Circuit	Link ID. When the network type is Broadcast, the circuit column describes the DIS considered by the neighbor r1.
Interface	Interface for neighbor establishment
Adjacency ID	Neighbor ID, arranged based on interface. The value range is from 1 to 255.
Uptime	Uptime of a neighbor connection
Area Address(es)	Area address
SNPA	SNPA address of the neighbor
Ipv6 Address(es)	IPv6 address of the neighbor
Level-1 MTID	Topology type supported by the Level-1 neighbor
Level-2 MTID	Topology type supported by the Level-2 neighbor
Level-1 Protocols Supported	IP protocol type supported by the Level-1 neighbor
Level-2 Protocols Supported	IP protocol type supported by the Level-2 neighbor
BFD (IPv4) session state	BFDv4 session status corresponding to the IS-IS neighbor

Field	Description
BFD (IPv6) session state	BFDv6 session status corresponding to the IS-IS neighbor

Notifications

N/A

Platform Description

N/A

1.83 show isis nsr

Function

Run the **show isis nsr** command to display NSR information of IS-IS.

Syntax

```
show isis [ tag ] nsr
```

Parameter Description

tag: Name of a specified IS-IS instance.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the NSR information of IS-IS.

```
Hostname> enable
Hostname# show isis nsr
NSR role: master
Area (null):
NSR: enable
NSR state: realtime
Area 1:
NSR: disable
```

Table 1-1 Output Fields of the show isis nsr Command

Field	Description
NSR role	NSR role
Area	Instance tag
NSR	Whether the instance is configured with the NSR
NSR state	NSR running state of an instance. It is displayed after the instance is configured with the NSR.

Notifications

N/A

Platform Description

N/A

1.84 show isis protocol

Function

Run the **show isis protocol** command to display protocol information of IS-IS.

Syntax

```
show isis [ tag ] protocol
```

Parameter Description

tag: Name of a specified IS-IS instance.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the protocol information of IS-IS.

```

Hostname> enable
Hostname# show isis protocol
IS-IS Router: (null)
  Binding VRF: vrf
  Mib-Binding: off
System ID: 0000.0000.0036   IS-type: level-2
Virtual System ID:

```



```

1111.1111.1111, 2222.2222.2222
Manual area address(es):
  49.0001, 49.0003
Interfaces supported by IS-IS:
  TenGigabitEthernet 0/1, TenGigabitEthernet 0/2
Redistributing IPv4:
isis 1, isis 2
Redistributing IPv6:
  isis 3, isis 4
Distance: 115
Generate narrow metrics: Level-2
Accept narrow metrics:   Level-2
Generate wide metrics:   none
Accept wide metrics:     none
NSR: enable
Two-way-maintain: enable
BGP-IS: Level-2

```

Table 1-1Output Fields of the show isis protocol Command

Field	Description
IS-IS Router	Instance tag
Binding VRF	VRF name bound to the IS-IS instance
Mib-Binding	Whether the instance is bound to SNMP operations
System ID	System ID
IS-type	Level type supported by the instance
Virtual System ID	Extended system ID
Manual area address(es)	Area ID
Interfaces supported by IS-IS	Interface associated with this instance
Redistributing IPv4	Source of the IPv4 redistributed route
Redistributing IPv6	Source of the IPv6 redistributed route
Distance	IS-IS management weight
Generate narrow metrics	Type of narrow metric generated
Accept narrow metrics	Type of narrow metric received
Generate wide metrics	Type of wide metric generated
Accept wide metrics	Type of wide metric received
NSR	Whether the instance is configured with the NSR. It is displayed when the

Field	Description
	instance is configured with the NSR.
Two-way-maintain	Whether the instance is configured with the two-way-maintain function
BGP-LS	Level type of the BGP-LS configured for the instance

Notifications

N/A

Platform Description

N/A

1.85 show isis topology

Function

Run the **show isis topology** command to display the topology information of connected IS-IS devices.

Syntax

```
show isis [ tag ] topology [ I1 | I2 | level-1 | level-2 ]
```

Parameter Description

tag: Name of a specified IS-IS instance.

I1: Specifies Level-1 topology.

level-1: Specifies Level-1 topology.

I2: Specifies Level-2 topology.

level-2: Specifies Level-2 topology.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the topology information of connected IS-IS devices.

```
Hostname> enable
Hostname# show isis topology
Area (null):
IS-IS paths to level-1 routers
```

```

System Id      Metric  Next-Hop  SNPA          Interface
r1             10      r1        00d0.f822.33ad  TenGigabitEthernet 0/1
Hostname
IS-IS paths to level-2 routers
System Id      Metric  Next-Hop  SNPA          Interface
r1             10      r1        00d0.f822.33ad  TenGigabitEthernet 0/1
Hostname

```

Table 1-1 Output Fields of the show isis protocol Command

Field	Description
Area	Instance tag
System Id	System ID
Metric	Metric
Next-Hop	Next hop
SNPA	SNPA address
Interface	Interface of next hop

Notifications

N/A

Platform Description

N/A

1.86 show isis virtual-neighbors**Function**

Run the **show isis virtual-neighbors** command to display virtual system neighbor information of IS-IS.

Syntax

```
show isis [ tag ] virtual-neighbors
```

Parameter Description

tag: Name of a specified IS-IS instance.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays virtual system neighbor information of IS-IS.

```

Hostname> enable
Hostname# show isis virtual-neighbors
Area (null):
Virtual System Id          Type          State
1111.1111.1111            L1            DOWN
                          L2            UP
2222.2222.2222            L1            DOWN
                          L2            UP

```

Table 1-1 Output Fields of the show isis virtual-neighbors Command

Field	Description
Area	Instance tag
Virtual System Id	Virtual system ID
Type	Neighbor type
State	State of the neighbor. The value Up indicates that LSP fragments are created at the corresponding level.

Notifications

N/A

Platform Description

N/A

1.87 spf-interval**Function**

Run the **spf-interval** command to configure the exponential backoff algorithm of SPF calculation.

Run the **no** form of this command to restore the default configuration.

The default 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.

Syntax

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

no spf-interval [**level-1** | **level-2**]

Parameter Description

level-1: Takes effect for Level-1 IS-IS.

level-2: Takes effect for Level-2 IS-IS.

maximum-interval: Maximum interval for performing two consecutive SPF calculations, in seconds. The value range is from 1 to 120.

initial-interval: Wait time for performing the SPF calculation for the first time, in milliseconds. The value range is from 0 to 60000.

hold-interval: Minimum interval for performing the SPF calculation for the first and second times, in milliseconds. The value range is 10 to 60000.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

If the **level-1** or **level-2** parameter is not specified when the command is configured, the interval configuration takes effect for Level-1 and Level-2 LSPs.

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

The wait time for performing the SPF calculation for the first time is the *initial-interval*. If the network becomes unstable, the SPF calculation interval is less than the *maximum-interval*, and the interval for performing the SPF calculation for the second time becomes the *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*.

Link changes have high requirements for convergence. The initial interval can be set to a small value. You can also appropriately increase the values of the preceding parameters to reduce the CPU usage.

Note

- 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*.
-

Examples

The following example configures an exponential backoff algorithm of SPF calculation, and sets the maximum interval of two SPF calculations to **5** seconds, the wait time of SPF calculation for the first time to **100** ms, and the interval for the first and SPF calculation to **200** ms.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# spf-interval 5 100 200
```

The following example configures an exponential backoff algorithm of SPF calculation, sets the maximum interval of two SPF calculations to **10** seconds, and uses the default values of other exponential backoff parameters.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# spf-interval 10
```

Notifications

If the configured value of *hold-interval* is greater than *maximum-interval* (for example, the configured value of *hold-interval* is **1500** ms, and the *maximum-interval* is **1** second), the following notification will be displayed:

```
% ISIS: hold_interval (1500ms) should be no more than maximum_interval (1s), set
to (1000ms).
```

If the configured value of *initial-interval* is greater than *hold-interval* (for example, the configured value of *initial-interval* is **20** ms, and the *hold-interval* is **10** ms), the following notification will be displayed:

```
% ISIS: initial_interval (20ms) should be no more than hold_interval (10ms), set
to (10ms).
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.88 summary-address

Function

Run the **summary-address** command to configure IPv4 summarized routes.

Run the **no** form of this command to remove this configuration.

The route summarization function is disabled by default.

Syntax

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

```
no summary-address ipv4-address net-mask
```

Parameter Description

ipv4-address: IPv4 address of the summarized route.

net-mask: Network mask of the summarized route.

level-1: Takes effect for Level-1 summarized routes.

level-1-2: Takes effect for Level-1 and Level-2 summarized routes.

level-2: Takes effect for Level-2 summarized routes.

metric-value: Metric of the summarized route. The value range is from 1 to 4294967295, and the default value is 0.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

If the configured summarized route contains routing information about a reachable address or network segment, the summarized route, instead of detailed routes, is advertised externally.

Examples

The following example sets the IPv4 summarized route to 10.10.0.0/24 on Level-2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# summary-address 10.10.0.0 255.255.255.0 level-2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip route** (IP routing basic)

1.89 summary-prefix

Function

Run the **summary-prefix** command to configure IPv6 summarized routes.

Run the **no** form of this command to remove this configuration.

The route summarization function is disabled by default.

Syntax

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

no summary-prefix *ipv6-prefix/prefix-length*

Parameter Description

ipv6-prefix/prefix-length: Network address of the summarized route and its IPv6 prefix length. It follows the X:X:X:X::X/<0-128> format.

level-1: Takes effect for Level-1 summarized routes.

level-1-2: Takes effect for Level-1 and Level-2 summarized routes.

level-2: Takes effect for Level-2 summarized routes. By default, the setting takes effect for Level-2.

Command Modes

IS-IS IPv6 address family configuration mode

Default Level

14

Usage Guidelines

If the configured summarized route contains routing information about a reachable address or network segment, the summarized route, instead of detailed routes, is advertised externally.

Examples

The following example sets the IPv6 summarized route to 1000::/96 on Level-2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# address-family ipv6
Hostname(config-router-af)# summary-prefix 1000::/96 level-2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 route** (IP routing basic)

1.90 two-way-maintain

Function

Run the **two-way-maintain** command to enable the two-way maintenance function of IS-IS.

Run the **no** form of this command to disable this function.

The two-way maintenance function is enabled by default.

Syntax

two-way-maintain

no two-way-maintain

Parameter Description

N/A

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

In a large network, a lot of packets may be sent or received, occupying a great proportion of CPU and memory. As a result, some packets are delayed or discarded. If the time required for processing hello packets exceeds the neighbor holdtime, the corresponding adjacency 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.

Examples

The following example enables the two-way maintenance function of IS-IS.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis 1
Hostname(config-router)# no two-way-maintain
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- [show isis protocol](#)

1.91 virtual-system

Function

Run the **virtual-system** command to configure an additional system ID for fragment extension.

Run the **no** form of this command to disable this function.

The fragment extension function is disabled by default.

Syntax

virtual-system *system-id*

no virtual-system *system-id*

Parameter Description

system-id: ID of an additional system, six bytes.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

Use this command to configure the additional system ID of an IS-IS routing process, which is used by the extended LSP that is generated after the 256 fragments of the original LSP are used up. To enable fragment extension, run this command to configure an additional system ID and run the **lsp-fragments-extend** command to configure fragment extension.

Examples

The following example sets the Additional system ID to 0000.0000.0034 for fragment extension.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# router isis
Hostname(config-router)# virtual-system 0000.0000.0034
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.92 vrf

Function

Run the **vrf** command to bind an IS-IS instance to a VRF table.

Run the **no** form of this command to remove this configuration.

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

Syntax

vrf *vrf-name*

no vrf *vrf-name*

Parameter Description

vrf-name: Name of a configured VRF.

Command Modes

IS-IS routing process configuration mode

Default Level

14

Usage Guidelines

Before you bind an IS-IS instance to a VRF table, ensure that the VRF table has been configured. If you need to establish an IS-IS IPv6 neighbor relationship, enable IPv6 and ensure that the table to be bound is a multiprotocol VRF table.

Note the following constraints or conventions for the binding operation:

- The IS-IS instances bound with the same non-default 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** (or **ipv6**) **router isis [tag]** interface configuration and the redistribution configuration in routing process configuration mode will be deleted.

Examples

The following example binds an IS-IS instance to vrf_1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vrf definition vrf_1
Hostname(config-vrf)# address-family ipv4
Hostname(config-vrf-af)# exit-address-family
Hostname(config)# router isis
Hostname(config-router)# vrf vrf_1
```

Notifications

If the VRF bound does not exist, the following notification will be displayed:

```
% The VRF does not exist
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- [show isis protocol](#)