1 OSPFv3 Commands

Command	Function
area authentication	Enable OSPFv3 area authentication.
area default-cost	Configure the cost of the default route in a stub area or not-so-stubby area (NSSA) on the ABR that resides in the stub area or NSSA.
area encryption	Enable OSPFv3 area encryption and authentication.
area nssa	Configure an OSPFv3 area as NSSA.
area range	Configure a range of summarized inter-area routes.
area stub	Configure an area as a stub or totally stub area.
area virtual-link	Create a virtual link or set virtual link parameters.
asbr enable	Configure a device as an ASBR.
auto-cost reference-bandwidth	Enable metric computation or reference bandwidth value modification for an interface based on bandwidth.
bfd all-interfaces	Enable bidirectional forwarding detection (BFD) on all OSPFv3 interfaces for link detection.
clear ipv6 ospf process	Clear and reset an OSPFv3 process.
default-information originate	Generate a default route and inject the route to an OSPFv3 routing domain.
default-metric	Configure the default metric of a redistributed route.
distance	Configure the administrative distances corresponding to different types of OSPFv3 routes.
distribute-list in	Enable the function of filtering routes that are computed based on the received LSAs.
distribute-list out	Enable the function of filtering redistributed routes.
enable mib-binding	Bind an MIB to a specified OSPFv3 process.
enable traps	Enable sending of the specified trap message.
graceful-restart	Enable the OSPFv3 GR capability.

graceful-restart helper	Enable the OSPFv3 GR helper function and configure a topology detection method of the OSPFv3 GR helper.
ipv6 ospf area	Enable an interface to join in an OSPFv3 routing process.
ipv6 ospf authentication	Enable OSPFv3 authentication on an interface.
ipv6 ospf bfd	Enable BFD on a specified OSPFv3 interface for link detection.
ipv6 ospf cost	Configure cost of an interface.
ipv6 ospf dead-interval	Configure the neighbor dead interval of an interface.
ipv6 ospf encryption	Enable OSPFv3 encryption on an interface.
ipv6 ospf hello-interval	Configure the hello packet sending interval on an interface.
ipv6 ospf mtu-ignore	Disable MTU verification for an interface that receives database description packets.
ipv6 ospf neighbor	Configure OSPFv3 neighbors.
ipv6 ospf network	Configure an OSPF network type of an interface.
ipv6 ospf priority	Configure the priority of an interface.
ipv6 ospf retransmit-interval	Configure the LSA retransmission interval on an interface.
ipv6 ospf subvlan	Enable the OSPFv3 function in a super VLAN.
ipv6 ospf transmit-delay	Configure the LSU transmission delay on an interface.
ipv6 router ospf	Enable an OSPFv3 routing process.
ipv6 router ospf max-concurrent-dd	Configure the maximum number of neighbors with which all the OSPFv3 routing processes can concurrently initiate or accept interaction.
log-adj-changes	Record the log of adjacency state changes.
max-concurrent-dd	Configure the maximum number of neighbors with which the current OSPFv3 instance can concurrently initiate or accept interaction.
nsr	Enable the nonstop routing (NSR) function.
passive-interface	Configure a passive interface.
redistribute	Enable route redistribution and inject routing

	information of other routing protocols to an OSPFv3 routing process.
router-id	Configure the ID of a router.
show ipv6 ospf	Display information of an OSPFv3 process.
show ipv6 ospf database	Display the database information of an OSPFv3 process.
show ipv6 ospf interface	Display the information of an OSPFv3 interface.
show ipv6 ospf neighbor	Display neighbor information of an OSPFv3 process.
show ipv6 ospf restart	Display the information related to OSPFv3 GR.
show ipv6 ospf route	Display the routing information of OSPFv3.
show ipv6 ospf summary-prefix	Display external route summarization information of OSPFv3.
show ipv6 ospf topology	Display the topological information of an OSPFv3 area.
show ipv6 ospf virtual-links	Display virtual link information of an OSPFv3 process.
summary-prefix	Configure a summarized route for the external routes of an OSPFv3 routing domain.
timers lsa arrival	Configure the delay for receiving same LSAs.
timers pacing lsa-group	Configure a group update time of LSAs.
timers pacing lsa-transmit	Configure the LSA group sending interval.
timers spf	Configure the delay time for SPF computation after an OSPFv3 process receives the topological change information and the interval between two SPF computations.
timers throttle lsa all	Configure an exponential backoff algorithm of LSA packet generation.
timers throttle route	Configure the delay time for route computation when an OSPFv3 process receives changed inter-area and external LSAs.
timers throttle spf	Configure the delay time for SPF computation when an OSPFv3 process receives topological change information, and the minimum and maximum intervals for two SPF computations.

1.1 area authentication

Function

Run the **area authentication** command to enable OSPFv3 area authentication.

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

The OSPFv3 area authentication function is disabled by default.

Syntax

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

no area *area-id* **authentication**

Parameter Description

area-id: Area ID, which can be a decimal integer or an IP address. The value range is from 0 to 4294967295.

spi *spi*: Specifies a security parameter index. The value range is from 256 to 4294967295.

md5: Enables the MD5 authentication mode.

string-key: Specifies to use a string as an authentication key.

sha1: Enables the SHA1 authentication mode.

0: Indicates that the key is displayed in plaintext.

7: Indicates that the key is displayed in ciphertext.

key: Authentication key.

Command Modes

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.

Enabling authentication can improve interaction security of OSPFv3 packets. A device supports four types of authentication:

- No authentication (when authentication is not configured)
- MD5
- SHA1

After an OSPFv3 area is configured with authentication, the configuration takes effect on all interfaces (except virtual links) in the area. If the interface authentication configuration is different from area authentication configuration, interface authentication configuration takes precedence over the area authentication configuration.

OSPFv3 area authentication and area associated SA authentication are mutually exclusive.

Examples

The following example configures MD5 for Area 1 in the OSPFv3 routing process, and sets the security parameter index to 300 and the password to aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.

The following example configures MD5 for Area 0 in the OSPFv3 routing process, and sets the security parameter index to 606 and the key to psw@123.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# area 1 authentication ipsec spi 300 md5
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
Hostname(config-router)# area 0 authentication ipsec spi 606 md5 string-key
psw@123
```

Notifications

If this SPI has been used in this module, the following notification will be displayed:

```
% OSPFv3: SPI is already in use.
```

If this SPI has been used in another module, the following notification will be displayed:

```
% OSPFv3: SPI is already in use by others.
```

If this SPI has been configured in the local area, the following notification will be displayed:

```
% OSPFv3: Area is already configured with the same SPI.
```

If authentication is configured for an area with encryption configuration, the following notification will be displayed:

```
% OSPFv3: Area is already configured with encryption so cannot configure
authentication.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 router ospf**

1.2 area default-cost

Function

Run the **area default-cost** command to configure the cost of the default route in a stub area or not-so-stubby area (NSSA) on the ABR that resides in the stub area or NSSA.

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

The default cost value of the default route is **1**.

Syntax

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

no area *area-id* **default-cost**

Parameter Description

area-id: ID of a stub area or an NSSA, which can be a decimal integer or an IP address. The value range is from 0 to 4294967295.

cost: Cost of the default summarized route injected to the stub area or NSSA. The value range is from 0 to 16777215.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

The ABR in the stub area or NSSA will advertise the default route to the devices in the area. The default cost value of the default route is **1**. To lower the routing priority of the default route, you can use this command to set the cost to a greater value.

Examples

The following example sets the cost of the default route in a stub area to 100 on the ABR that resides in the stub area.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# area 50 stub
Hostname(config-router)# area 50 default-cost 100
```

Notifications

When this command is configured in the backbone area, the following notification will be displayed:

```
% You can't configure default-cost to backbone
```

When this command is configured in a non-stub area or non-NSSA, the following notification will be displayed:

```
% The area is neither stub, nor NSSA
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- ipv6 router ospf

1.3 area encryption

Function

Run the **area encryption** command to enable OSPFv3 area encryption and authentication.

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

The encryption and authentication function is disabled by default.

Syntax

area *area-id* **encryption ipsec spi** *spi* **esp** { { **3des** | **aes-cbc** { **128** | **192** | **256** } | **des** } [**0** | **7**] *des-key* | **null** } { **md5** | **sha1** } [**0** | **7**] *key*
no area *area-id* **encryption**

Parameter Description

Area-id: Area ID, which can be a decimal integer or an IP address. The value range is from 0 to 4294967295.

spi *spi*: Specifies a security parameter index. The value range is from 256 to 4294967295.

esp: Enables the ESP encryption mode.

3des: Enables the 3DES encryption mode.

aes-cbc [**128** | **192** | **256**]: Enables the Advanced Encryption Standard-Cipher Block Chaining (AES-CBC) encryption mode. The encryption key length is 128, 192, or 256 bits.

des: Enables the Data Encryption Standard (DES) mode.

0: Indicates that the key is displayed in plaintext.

7: Indicates that the key is displayed in ciphertext.

des-key: Encryption key.

null: Indicates that no encryption mode is used.

md5: Enables the MD5 authentication mode.

sha1: Enables the SHA1 authentication mode.

key: Authentication key.

Command Modes

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.

Enabling encryption and authentication can improve interaction security of OSPFv3 packets. A device supports the following types of encryption and authentication:

- Encryption modes: DES, 3DES, and AES-CBC.
- Authentication modes: MD5 and SHA1

After an OSPFv3 area is configured with encryption and authentication, the configuration takes effect on all interfaces (except virtual links) in the area, but the interface encryption and authentication configuration takes precedence over the area configuration.

Examples

The following example enables the OSPFv3 encryption and authentication function for Area 1, configures Area 1 with null encryption and MD5 authentication, and sets the password to aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# area 1 encryption ipsec spi 300 esp null md5
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Notifications

If this SPI has been used in this module, the following notification will be displayed:

```
% OSPFv3: SPI is already in use.
```

If this SPI has been used in another module, the following notification will be displayed:

```
% OSPFv3: SPI is already in use by others.
```

If this SPI has been configured in the local area, the following notification will be displayed:

```
% OSPFv3: Area is already configured with the same SPI.
```

If encryption and authentication is re-configured for an area with authentication configuration, the following notification will be displayed:

```
% OSPFv3: Area is already configured with authentication so cannot configure
encryption.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- ipv6 router ospf

1.4 area nssa

Function

Run the **area nssa** command to configure an OSPFv3 area as NSSA.

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

The NSSA function is disabled by default.

Syntax

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

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

Parameter Description

area-id: ID of the NSSA, which can be a decimal integer or an IP address. The value range is from 0 to 4294967295.

default-information-originate: Indicates that generated default Type 7 LSAs are introduced to the NSSA. This option takes effect only on an NSSA ABR or ASBR.

metric *metric*: Indicates the metric of the generated default LSA. The value range is from 0 to 16777214, and the default value is **1**.

metric-type *metric-type*: Indicates the route type of the generated default LSA. *metric-type*: The value is **1** or **2**: **1** represents N-1, and **2** represents N-2. The default value is **2**.

no-redistribution: Select this option if the router is an NSSA ABR and you want to use the **redistribute** command to introduce the routing information only to a common area instead of an NSSA.

no-summary: Prohibits the ABR in the NSSA from sending Summary LSAs (Type 3 LSAs).

translator: Configures an ABR translator in an NSSA.

always: Enables the current NSSA ABR to always act as a translator. The default value is the standby translator.

stability-interval *stability-interval*: Configures the stability interval after the NSSA ABR is changed from a translator to a non-translator, in seconds. The value range is from 0 to 2147483647, and the default value is **40**.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

If you expect to reduce the LSA number in an area and to redistribute external routes, you can configure this area as an NSSA.

Parameter configurations are used as follows:

- The **default-information-originate** parameter is used to generate a default Type 7 LSA. This parameter has different functions on the ABR and the ASBR in the NSSA. On the ABR, a Type 7 LSA default route is generated regardless of whether the default route exists in the routing table. On the ASBR (not an ABR), a Type 7 LSA default route is generated only when the default route exists in the routing table.
- If the **no-redistribution** parameter is configured on the ASBR, other external routes introduced by OSPF through the **redistribute** command cannot be distributed to the NSSA. This parameter is generally used when a router in the NSSA acts both as an ASBR and an ABR. It prevents external routing information from

entering the NSSA.

- The **no-summary** parameter is used to further reduce the number of LSAs sent to the NSSA and prevent the ABR from sending Summary LSAs (Type 3 LSAs) to the NSSA.
- The **area default-cost** parameter is used on an ABR/ASBR in this NSSA. This command configures the cost of the default route sent from the ABR/ASBR to the NSSA. The default cost of the default route sent to the NSSA is 1.
- If an NSSA has two or more ABRs, the ABR with the largest router ID is elected by default as the translator for translating Type 7 LSAs to Type 5 LSAs. If you expect that the current device is always the translator ABR for translating Type 7 LSAs to Type 5 LSAs, use the **translator always** parameter.
- If the translator role of the current device is replaced by another ABR, the translation capability of the device is retained during the time specified by **stability-interval**. If the device does not become a translator again during the time, LSAs that are translated from Type 7 to Type 5 will be deleted from the AS after **stability-interval** expires.
- To prevent a routing loop, LSAs that are translated from Type 7 to Type 5 are deleted from the AS immediately after the current device loses the translator role even if **stability-interval** does not expire.
- In the same NSSA, it is recommended that **translator always** be configured on only one ABR.

Examples

The following example configures OSPFv3 Area 1 as an NSSA.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# area 1 nssa
```

Notifications

If the backbone area is configured as an NSSA, the following notification will be displayed:

```
% You can't configure NSSA to backbone
```

If a stub area is configured as an NSSA, the following notification will be displayed:

```
% The area is configured as stub area already
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 ospf**
- **ipv6 router ospf**

1.5 area range

Function

Run the **area range** command to configure a range of summarized inter-area routes.

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

Inter-area route summarization is not performed by default.

Syntax

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

no area *area-id* **range** *ipv6-prefix*/*prefix-length*

Parameter Description

area-id: ID of the OSPF area to which the summarized routes will be injected, which can be a decimal integer or an IP address. The value range is from 0 to 4294967295.

ipv6-prefix/prefix-length: Range of IP addresses to be summarized.

advertise: Advertises the range of summarized routes.

not-advertise: Does not advertise the range of summarized routes.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

This command takes effect only on an ABR, and is used to summarize multiple routes in an area as a route and advertise this route to other areas. Combination of the routing information occurs only on the boundary of an area. Routers inside the area can learn specific routing information, whereas routers in other areas can learn only one summarized route. You can configure **advertise** or **not-advertise** to determine whether to advertise the range of summarized routes, which helps shield and filter routes. By default, the summarized routes are advertised.

You can configure the route summarization command for multiple areas to simplify the entire OSPF routing domain, and improve the network forwarding performance, especially for a large-sized network.

When multiple summarized routes are configured and have an inclusive relationship with each other, the range of routes to be summarized is determined based on the longest match principle.

Examples

The following example sets the IP address of the inter-area route summarization in Area 1 to 2001:DB8:1:2::/64.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# area 1 range 2001:db8:1:2::/64
```

Notifications

If an inexistent summarization entry is deleted, the following notification will be displayed:

```
% Can't find specified area range.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- ipv6 router ospf

1.6 area stub

Function

Run the **area stub** command to configure an area as a stub or totally stub area.

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

The stub area function is disabled by default.

Syntax

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

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

Parameter Description

area-id: ID of a stub area, which can be a decimal integer or an IP address. The value range is from 0 to 4294967295.

no-summary: This option is valid only on the ABR in a stub area. If this option is specified, the ABR only advertises one Type 3 LSA indicating the default route to the stub area, and does not advertise other Type 3 LSAs.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

An area located on the stub of a network can be configured as a stub area. You must run the **area stub** command on all routers in the stub area. Devices in a stub area cannot learn external routes (Type 5 LSAs) of the AS. In actual application, external routes take up a large proportion of the LSDB. Therefore, devices in a stub area can learn only a small amount of routing information, which reduces the amount of system resources required to run the OSPFv3 protocol.

By default, an ABR in a stub area will generate a Type 3 LSA indicating the default fault and advertise the LSA to the stub area. In this way, devices in the stub area can access devices outside the AS.

To configure a totally stub area, add the **no-summary** keyword when you are running the **area stub** command on the ABR.

Examples

The following example creates a stub area 10 and enables the ABRs in stub area 10 to advertise only default routes to the stub area.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# area 10 stub
Hostname(config-router)# area 10 stub no-summary
```

Notifications

If the backbone area is configured as a stub area, the following notification will be displayed:

```
% You can't configure stub to backbone
```

If an NSSA is configured as a stub area, the following notification will be displayed:

```
% The area is configured as NSSA area already
```

If a stub area is configured with a virtual link, the following notification will be displayed, indicating that the virtual link must be deleted to validate the configuration:

```
% First deconfigure all virtual link through this area
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- show ipv6 ospf
- ipv6 router ospf

1.7 area virtual-link

Function

Run the **area virtual-link** command to create a virtual link or set virtual link parameters.

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

No virtual link is configured by default.

Syntax

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

no area *area-id* **virtual-link** *router-id* [**dead-interval** | **hello-interval** | **instance** | **retransmit-interval** | **transmit-delay**] * [**authentication** | **encryption**]

Parameter Description

area-id: ID of an area where a virtual link exists, which can be a decimal integer or an IP address. The value range is from 0 to 4294967295.

router-id: ID of a neighboring router of the virtual link.

dead-interval *dead-interval*: Indicates the time that the local interface of the virtual link detects the failure of the neighbor, in seconds. The value range is from 0 to 2147483647, and the default value is **40**.

hello-interval *hello-interval*: Indicates the time consumed to send a Hello packet on the local interface of the virtual link, in seconds. The value range is from 1 to 65535, and the default value is **10**.

instance *instance-id*: Specifies the instance of a virtual link. The value range is from 0 to 255.

retransmit-interval *retransmit-interval*: Indicates the retransmission time of an LSA on the local interface of the virtual link, in seconds. The value range is from 0 to 65535, and the default value is **5**.

transmit-delay *transmit-delay*: Indicates the delay after which the LSA is sent on the local interface of the virtual link, in seconds. The value range is from 0 to 65535, and the default value is **1**.

authentication ipsec spi *spi* { **md5** | **sha1** | **sha2-256** } [**0** | **7**] *key*: Defines OSPFv3 authentication.

Note

Authentication between neighbors must be consistent. The **service password-encryption** command enables a configured key to be displayed in ciphertext mode.

spi *spi*: Specifies a security parameter index. The value range is from 256 to 4294967295.

md5: Specifies the MD5 authentication mode.

sha1: Specifies the SHA1 authentication mode.

sha2-256: Specifies the sha2-256 authentication mode.

0: Indicates that the key is displayed in plaintext.

7: Indicates that the key is displayed in ciphertext.

key: Authentication key.

encryption ipsec spi *spi* **esp** [**3des** | **aes-cbc** { **128** | **192** | **256** } [**0** | **7**] *des-key* | **des** [**0** | **7**] *des-key* | **null**] { **md5** | **sha1** } [**0** | **7**] *key*: Defines OSPFv3 encryption and authentication.

Note

Encryption and authentication between neighbors must be consistent. The **service password-encryption** command enables a configured key to be displayed in ciphertext mode.

spi *spi*: Specifies a security parameter index. The value range is from 256 to 4294967295.

3des: Specifies the 3DES encryption mode.

aes-cbc 128: Specifies 128-bit AES-CBC authentication mode.

aes-cbc 192: Specifies 192-bit AES-CBC authentication mode.

aes-cbc 256: Specifies 256-bit AES-CBC authentication mode.

0: Indicates that the key is displayed in plaintext.

7: Indicates that the key is displayed in ciphertext.

des-key: Encryption key.

des: Specifies the DES encryption mode.

null: Indicates that no encryption mode is used.

md5: Specifies the MD5 authentication mode.

sha1: Specifies the SHA1 authentication mode.

key: Authentication key.

Command Modes

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.

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

The area where the virtual link is located cannot be a stub area or NSSA.

The **hello-interval**, **dead-interval**, and **instance** parameters configured for neighbors connected by a virtual link must be consistent; otherwise, the adjacency cannot be set up properly.

Examples

The following example creates a virtual link and sets the router ID of the virtual link to 192.1.1.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# area 1 virtual-link 192.1.1.1
```

Notifications

If a virtual link is configured in the backbone area, the following notification will be displayed:

```
% You can't configure virtual-link transit to backbone
```

If a virtual link is configured in a stub area or an NSSA, the following notification will be displayed:

```
% Area is a stub or NSSA so virtual links are not allowed
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- ipv6 router ospf
- show ipv6 ospf virtual-links

1.8 asbr enable

Function

Run the **asbr enable** command to configure a device as an ASBR.

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

No device is an ASBR by default.

Syntax

asbr enable

no asbr enable

Parameter Description

N/A

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

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

Examples

The following example configures a device as an ASBR.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# asbr enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 router ospf**
- **show ipv6 ospf database**

1.9 auto-cost reference-bandwidth

Function

Run the **auto-cost reference-bandwidth** command to enable metric computation or reference bandwidth value modification for an interface based on bandwidth.

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

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

Syntax

auto-cost reference-bandwidth *ref-bw*

no auto-cost reference-bandwidth

Parameter Description

reference-bandwidth *reference-bandwidth*: Specifies the reference bandwidth value, in Kbps. The value range is from 1 to 4294967.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

The cost value of an OSPFv3 interface is equal to the reference bandwidth value/interface bandwidth. To enable OSPFv3 on a 100M link, it is recommended that the *ref-bw* value be adjusted to a greater value based on actual network bandwidth. For a 1000M network, the reference bandwidth value can be set to a value greater than 1000; for a 10G network, the reference bandwidth value can be set to a value greater than 10000.

You can run the **ipv6 ospf cost** command in interface configuration mode to specify the cost of the specified interface. The priority of this cost is higher than that of the metric computed based on the reference bandwidth value.

Examples

The following example sets the reference bandwidth value to 10 Mbps.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# auto-cost reference-bandwidth 10
```

Notifications

If the reference bandwidth value is modified, the following notification will be displayed:

```
% OSPFv3: Reference bandwidth is changed.
Please ensure reference bandwidth is consistent across all routers
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- ipv6 router ospf
- show ipv6 ospf interface

1.10 bfd all-interfaces

Function

Run the **bfd all-interfaces** command to enable bidirectional forwarding detection (BFD) on all OSPFv3 interfaces for link detection.

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

The BFD function is disabled on all interfaces by default.

Syntax

bfd all-interfaces

no bfd all-interfaces

Parameter Description

N/A

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

The OSPFv3 protocol dynamically discovers a neighbor by using hello packets. After BFD is enabled, OSPFv3 establishes a BFD session with a neighbor in the full neighbor relationship. The neighbor state is detected using the BFD mechanism. When the BFD neighbor fails, OSFPv3 immediately performs network convergence.

You can also run the **ipv6 ospf bfd** [**disable**] command in interface configuration mode to enable or disable the BFD function on a specified interface, and this configuration takes precedence over the configuration made using the **bfd all-interfaces** command in process configuration mode.

Examples

The following example enables BFD on all OSPFv3 interfaces for link detection.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# bfd all-interfaces
```

Notifications

If BFD is enabled on all interfaces for link detection, the following notification will be displayed:

```
% Warning: The BFD for OSPFv3 neighbor shall be enabled, or it would affect the
route learning.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 router ospf**
- **show ipv6 ospf**

1.11 clear ipv6 ospf process

Function

Run the **clear ipv6 ospf process** command to clear and reset an OSPFv3 process.

Syntax

clear ipv6 ospf [*process-id*] **process**

Parameter Description

process-id: OSPFv3 process ID. The value range is from 1 to 65535. When this parameter is specified, the specified OSPF process will be cleared and reset. When this parameter is not specified, all the running OSPF processes will be cleared and reset.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

Resetting the whole OSPFv3 process will reestablish all the neighbors, which has a great impact on the entire protocol.

When running this command, you need to make confirmation.

Use the *process-id* parameter to specify to clear an OSPFv3 instance. If the *process-id* parameter is not specified, all OSPFv3 instances are cleared.

Examples

The following example clears and resets an OSPFv3 instance.

```
Hostname> enable
Hostname# clear ipv6 ospf process
```

Notifications

If the specified process ID is incorrect, the following notification will be displayed:

```
% OSPFv3: No router process 1.
```

Platform Description

N/A

Related Commands

N/A

1.12 default-information originate

Function

Run the **default-information originate** command to generate a default route and inject the route to an OSPFv3 routing domain.

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

No default route is generated by default.

Syntax

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

no default-information originate [**always** | **metric** | **metric-type** | **route-map** *map*] *

Parameter Description

always: Enables OSPFv3 to generate a default route even if a default route exists locally.

metric *metric*: Indicates the initial metric of the default route. The value range is from 0 to 16777214, and the default value is **1**.

metric-type type: Indicates the type of the default route. The value is 1 or 2, and the default value is **2**.

route-map *map*: Indicates the name of the associated route map. No route map is associated by default.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

When the **redistribute** or **default-information** command is executed, an OSPFv3 router automatically becomes an ASBR. The ASBR, however, does not automatically generate or advertise a default route to all routers in the OSPF routing domain. To enable an ASBR to generate a default route, run the **default-information originate** command.

If the **always** parameter is specified, the OSPFv3 process advertises an external default route to neighbors no matter whether a default route exists in the core routing table. This default route, however, is not displayed on the local router. To confirm whether the default route is generated, run the **show ipv6 ospf database** command to display the OSPFv3 LSDB. On an OSPFv3 neighbor, you can run the **show ipv6 route** command to display the default route.

The metric of the external default route can be defined only by the **default-information originate** command, instead of the **default-metric** command.

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

This command generates a default route of Type 5 LSA, which will not be flooded to an NSSA. If you want to generate a default route in the NSSA, use the **area nssa default-information-originate** command. A router in the stub area cannot generate an external default route.

Examples

The following example generates a default route and injects the route to an OSPFv3 routing domain.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# default-information originate always
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- ipv6 router ospf
- show ipv6 ospf database

1.13 default-metric

Function

Run the **default-metric** command to configure the default metric of a redistributed route.

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

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

Syntax

default-metric *metric-value*

no default-metric

Parameter Description

metric-value: Default metric of a redistributed route. The value range is from 1 to 16777214.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

This command is used with the **redistribute** command to configure the default metric of a redistributed route. This command does not take effect to two types of routes:

- Default route generated by the **default-information originate** command.
- Redistributed direct route. The default metric of a redistributed direct route is always **20**.

Examples

The following example sets the default metric of a redistributed route to **10**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# default-metric 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 router ospf**

1.14 distance

Function

Run the **distance** command to configure the administrative distances corresponding to different types of OSPFv3 routes.

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

The default administrative distance is **110** for all the OSPF routes.

Syntax

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

no distance [**ospf**]

Parameter Description

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

distance: Configures an administrative distance of OSPFv3.

external *distance*: Indicates the administrative distance of an external route. The value range is from 1 to 255.

inter-area *distance*: Indicates the administrative distance of an inter-area route. The value range is from 1 to 255.

intra-area *distance*: Indicates the administrative distance of an internal route. The value range is from 1 to 255.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

To compare the priorities of routes generated by different OSPF processes, use this command to specify the administrative distances corresponding to different types of OSPF routes.

The administrative distances of routes allow different routing protocols to compare route priorities. A smaller administrative distance indicates a higher route priority.

If the administrative distance of a route entry is set to 255, the route entry is not trustworthy and does not participate in packet forwarding.

Examples

The following example sets the administrative distance of an OSPFv3 external route to **160**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# distance ospf external 160
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- ipv6 router ospf

1.15 distribute-list in

Function

Run the **distribute-list in** command to enable the function of filtering routes that are computed based on the received LSAs.

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

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

Syntax

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

no distribute-list { *acl-name* | **prefix-list** *prefix-list-name* } **in** [*interface-type interface-number*]

Parameter Description

acl-name: Name of an ACL. The value is a case-sensitive string of 1 to 99 characters.

prefix-list *prefix-list-name*: Uses a prefix list for filtering.

interface-type interface-number: Type and number of an interface on which LSA routes are filtered.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

This command filters the routes that are computed based on received LSAs. Only the routes meeting the filtering conditions can be forwarded. The command does not affect the LSDB or the routing tables of neighbors. The ACL and prefix list filtering rules are mutually exclusive in the configuration. In other words, if an ACL is used for filtering routes of a specified interface, prefix list cannot be configured for the same interface.

This command affects forwarding of local routes, but does not affect route computation based on LSAs. Therefore, if route filtering is configured on the ABR, Type 3 LSAs will still be generated and advertised to other areas because routes can still be computed based on LSAs. As a result, black-hole routes are generated. In this case, you can run the **area range** (containing the **not-advertise** parameter) command on the ABR to prevent generation of black-hole routes.

Examples

The following example filters routes (that are computed based on the received LSAs) based on the prefix list aaa.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 prefix-list aaa seq 10 permit 2001::/64
Hostname(config)# ipv6 router ospf 25
Hostname(config-router)# redistribute rip metric 100
Hostname(config-router)# distribute-list prefix-list aaa in gigabitethernet 0/1
```

Notifications

If the configured interface is invalid, the following notification will be displayed:

```
% Interface is invalid.
```

If the configured ACL name is invalid, the following notification will be displayed:

```
% ACL name abc-acl is invalid
```

If routes imported by this instance are filtered, the following notification will be displayed:

```
% Distribute-list of "ospf 1" via "ospf 1" not allowed
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 router ospf**

1.16 distribute-list out

Function

Run the **distribute-list out** command to enable the function of filtering redistributed routes.

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

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

Syntax

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

no distribute-list { *name* | **prefix-list** *prefix-list-name* } **out** [**bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **rip** | **static**]

Parameter Description

acl-name: Name of an ACL. The value is a case-sensitive string of 1 to 99 characters.

prefix-list prefix-*list-name*: Uses a prefix list for filtering.

bgp: Filters BGP routes.

connected: Filters direct routes.

isis [*area-tag*]: Filters IS-IS routes.

ospf *process-id*: Filters OSPF routes.

rip: Filters RIP routes.

static: Filters static routes.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

As with the **redistribute route-map** command, the **distribute-list out** command filters routes that are redistributed from other protocols to OSPFv3. The **distribute-list out** command does not redistribute routes, and is generally used together with the **redistribute** command. The ACL and prefix list are mutually exclusive in the configuration. In other words, if an ACL is used for filtering routes of a source, prefix list cannot be configured for the same source.

Examples

The following example filters redistributed static routes based on the prefix list jjj.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# redistribute static
Hostname(config-router)# distribute-list prefix-list jjj out static
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- ipv6 router ospf

1.17 enable mib-binding

Function

Run the **enable mib-binding** command to bind an MIB to a specified OSPFv3 process.

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

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

Syntax

enable mib-binding

no enable mib-binding

Parameter Description

N/A

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

The OSPFv3 MIB does not contain OSPFv3 process information. Therefore, SNMP operations take effect on one OSPFv3 process only.

If you wish to perform operations on a specified OSPFv3 process through SNMP, run this command to bind the MIB with the process.

Examples

The following example binds an MIB to a specified OSPFv3 process.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 100
Hostname(config-router)# enable mib-binding
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 router ospf**

1.18 enable traps

Function

Run the **enable traps** command to enable sending of the specified trap message.

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

The trap function is disabled by default.

Syntax

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

no enable traps [**error** [**IfConfigError** | **IfRxBadPacket** | **VirtIfConfigError** | **VirtIfRxBadPacket**] * | **state-change** [**IfStateChange** | **NbrStateChange** | **NssaTranslatorStatusChange** | **VirtIfStateChange** | **VirtNbrStateChange** | **RestartStatusChange** | **NbrRestartHelperStatusChange** | **VirtNbrRestartHelperStatusChange**] *]

Parameter Description

error: Configures all the trap switches related to Error. This parameter can also configure the following specific error trap switches:

IfConfigError: Indicates interface parameter configuration error.

IfRxBadPacket: Indicates that the interface receives an error packet.

VirtIfConfigError: Indicates virtual interface parameter configuration error.

VirtIfRxBadPacket: Indicates that the virtual interface receives an error packet.

state-change: Configures all the trap switches related to State-change. This parameter can also configure the following specific state-change trap switches:

IfStateChange: Indicates that the interface state changes.

NbrStateChange: Indicates that the neighbor state changes.

NssaTranslatorStatusChange: Indicates that the NSSA translator state changes.

VirtIfStateChange: Indicates that the virtual interface state changes.

VirtNbrStateChange: Indicates that the virtual neighbor state changes.

RestartStatusChange: Indicates that the local GR state changes.

NbrRestartHelperStatusChange: Indicates that the neighbor GR process state changes.

VirtNbrRestartHelperStatusChange: Indicates that the status of the virtual neighbor GR process changes.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

The function of this command is restricted by the **snmp-server** command. The **snmp-server enable traps ospf** command must be run prior to the **enable traps** command so that OSPFv3 Trap messages can be sent correctly.

This command is not restricted by the MIB bound to the process. The trap switch can be enabled concurrently for different processes.

Examples

The following example enables sending of the specified trap message.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 100
Hostname(config-router)# enable traps
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- ipv6 router ospf
- **snmp-server enable traps ospf** (network management and monitoring/SNMP)

1.19 graceful-restart

Function

Run the **graceful-restart** command to enable the OSPFv3 GR capability.

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

The OSPFv3 GR function is enabled by default.

Syntax

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

no graceful-restart [**grace-period** | **inconsistent-lsa-checking**]

Parameter Description

grace-period *grace-period*: Configures the GR time (in seconds), which starts at the time when OSPFv3 fails and ends at the time when OSPFv3 is restarted and GR is completed. The value range is from 1 to 1800, and the default value is **120**.

inconsistent-lsa-checking: Enables topology change detection. If any topology change is detected, OSPF exits the GR process to complete convergence.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

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

The GR function is based on OSPFv3 instance configuration, and different instances can be configured with different parameters based on actual situation.

This command is used to configure the GR restarter capability of a router. In the GR period, link state reestablishment enables OSPFv3 to restore to the original state. When a GR period expires, OSPFv3 exits the GR state and executes normal OSPFv3 operations.

Run the **graceful-restart** command to set the GR period to 120s. The **graceful-restart grace-period** command allows you to modify the GR period explicitly.

If the Fast Hello function is enabled, the GR function cannot be enabled.

The precondition for successful execution of GR and uninterrupted forwarding is that the topology remains stable. In case of a topology change, OSPFv3 converges as soon as possible and does not wait for GR execution to avoid longtime forwarding black-hole.

- Disabling topology detection: If OSPFv3 cannot converge in time when the topology changes during the hot standby process, forwarding black-hole may appear in a long time.
- Enabling topology detection: Forwarding interruption may occur, but the interruption time is far less than the forwarding black-hole time when topology detection is disabled.

In most cases, it is recommended that topology detection be enabled. In special scenarios, topology detection can be disabled if the topology changes after the hot standby process, but it can be ensured that the forwarding black-hole will not appear in a long time. This can minimize the forwarding interruption time during the hot standby process.

Examples

The following example enables the OSPFv3 restarter capability and sets the GR period to **60** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# graceful-restart
Hostname(config-router)# graceful-restart grace-period 60
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 router ospf**
- **show ipv6 ospf**

1.20 graceful-restart helper

Function

Run the **graceful-restart helper** command to enable the OSPFv3 GR helper function and configure a topology detection method of the OSPFv3 GR helper.

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

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

Syntax

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

no graceful-restart helper { **disable** | **internal-lsa-checking** | **strict-lsa-checking** }

Parameter Description

disable: Disables a device to act as a GR helper for other devices.

internal-lsa-checking: Indicates that changes in Type 1 to Type 3 LSAs will be checked during the period that the device acts as a GR helper to determine whether the network changes. If the network changes, the device will stop acting as a GR helper.

strict-lsa-checking: Indicates that changes in Type 1 to Type 5 and Type 7 LSAs will be checked during the period that the device acts as a GR helper to determine whether the network changes. If the network changes, the device will stop acting as a GR helper.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

This command is used to configure the GR help capability of a device. When a device performs GR, it sends a Grace-LSA to notify all its neighbor devices. If the GR help capability is enabled on the local device, the local device becomes a GR helper upon receiving the Grace-LSA to help the former device complete GR. The **disable** option indicates that the GR helper is not provided for any device that implements GR.

After a device becomes a GR helper, the network changes are not detected by default. If any change takes place in the network, the network topology converges after GR is completed. If you expect that network change can be detected quickly during GR, configure the **strict-lsa-checking** or **internal-lsa-checking** option to enable detection. The former option detects any LSA (Type 1 to Type 5 and Type 7 LSAs) that indicates network information, and the latter option detects any LSA (Type 1 to Type 3 LSAs) that indicates routes in an AS domain. When the network scale is large, it is recommended that you disable the LSA checking options because regional network changes may trigger termination of GR and consequently reduce the convergence of the entire network.

Examples

The following example disables the OSPFv3 GR helper function and configures the topology detection method as **strict-lsa-checking**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# graceful-restart helper disable
Hostname(config-router)# no graceful-restart helper disable
Hostname(config-router)# graceful-restart helper strict-lsa-checking
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- ipv6 router ospf
- show ipv6 ospf

1.21 ipv6 ospf area

Function

Run the **ipv6 ospf area** command to enable an interface to join in an OSPFv3 routing process.

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

No interface joins in an OSPFv3 routing process by default.

Syntax

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

no ipv6 ospf *process-id* **area** [**instance** *instance-id*]

Parameter Description

process-id: OSPF process ID. The value range is from 1 to 65535.

area *area-id*: Specifies an OSPFv3 area that an interface joins in. The area ID can be a decimal integer or an IP address. The value range is from 0 to 4294967295.

instance *instance-id*: Configures a specified OSPFv3 instance of the interface. The value range is from 0 to 255.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Run this command in interface configuration mode to enable an interface to join in OSPFv3, and then run the **ipv6 router ospf** command to configure an OSPFv3 process. After the OSPFv3 process is configured, the interface will automatically join in the process. The adjacency can be set up only between devices with the same *instance ID*. After this command is configured, all prefix information on the interface will be used to participate in the OSPFv3 process.

The following methods can be used to disable an interface from joining in an OSPFv3 process.

- Run the **no** form of this command to disable an interface from joining an OSPFv3 process.
- Run the **no ipv6 router ospf** command to disable all interfaces from joining in an OSPFv3 process.

Examples

The following example enables an OSPFv3 process on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1))# ipv6 ospf 1 area 2 instance 2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- show ipv6 ospf interface

1.22 ipv6 ospf authentication

Function

Run the **ipv6 ospf authentication** command to enable OSPFv3 authentication on an interface.

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

By default, no authentication mode is configured on an interface. In this case, the authentication type of the area where the interface resides is used on the interface.

Syntax

ipv6 ospf authentication { **ipsec spi** *spi* { **md5** [**string-key**] | **sha1** } [**0** | **7**] *key* | **null** } [**instance** *instance-id*]

no ipv6 ospf authentication [**instance** *instance-id*]

Parameter Description

spi *spi*: Specifies a security parameter index. The value range is from 256 to 4294967295.

md5: Enables the MD5 authentication mode.

string-key: Specifies to use a string as an authentication key.

sha1: Enables the SHA1 authentication mode.

0: Indicates that the key is displayed in plaintext.

7: Indicates that the key is displayed in ciphertext.

key: Authentication key.

null: Indicates that no authentication mode is enabled.

instance *instance-id*: Configures a specified OSPFv3 instance of the interface. The value range is from 0 to 255.

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 enable OSPFv3 authentication on an interface.

The device supports four authentication types:

- No authentication (when authentication is not configured)
- MD5
- SHA1

After an OSPFv3 area is configured with authentication, the configuration takes effect on all interfaces (except virtual links) in the area. If the interface authentication configuration is different from area authentication configuration, interface authentication configuration takes precedence over the area authentication configuration.

OSPFv3 interface authentication and interface associated SA authentication are mutually exclusive.

Note

OSPFv3 authentication parameters configured on interconnected interfaces must be consistent.

Examples

The following example configures an OSPFv3 interface with MD5 authentication mode and sets the password to aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 ospf authentication ipsec spi 300
md5 aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Notifications

If this SPI has been used in this module, the following notification will be displayed:

```
% OSPFv3: SPI is already in use.
```

If this SPI has been used in another module, the following notification will be displayed:

```
% OSPFv3: SPI is already in use by others.
```

If this SPI has been configured on the local Interface, the following notification will be displayed:

```
% OSPFv3: Interface is already configured with the same SPI.
```

If authentication is configured on an interface with encryption configuration, the following notification will be displayed:

```
% OSPFv3: Interface is already configured with encryption so cannot configure
authentication.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.23 ipv6 ospf bfd

Function

Run the **ipv6 ospf bfd** command to enable BFD on a specified OSPFv3 interface for link detection.

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

The BFD function is disabled on an interface by default, and the BFD configuration is subject to the configuration in the OSFPv3 process configuration mode.

Syntax

ipv6 ospf bfd [**disable**] [**instance** *instance-id*]

no ipv6 ospf bfd [**instance** *instance-id*]

Parameter Description

disable: Disables BFD on a specified OSPF interface for link detection.

instance *instance-id*: Configures a specified OSPFv3 instance of the interface. The value range is from 0 to 255.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

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

The BFD priority configured on an interface takes precedence over that configured in process configuration mode.

In light of the actual environment, you can run the **ipv6 ospf bfd** command to enable BFD on a specified OSPF interface for link detection, or run the **bfd all-interfaces** command in OSPFv3 process configuration mode to enable BFD on all OSPFv3 interfaces for link detection. Run the **ipv6 ospf bfd disable** command to disable BFD on a specified OSPF interface for link detection.

Examples

The following example enables BFD for link detection.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 ospf bfd
```

Notifications

If BFD is enabled for link detection on an interface, the following notification will be displayed:

```
% Warning: The BFD for OSPFv3 neighbor shall be enabled, or it would affect the
route learning.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- show ipv6 ospf interface

1.24 ipv6 ospf cost

Function

Run the **ipv6 ospf cost** command to configure cost of an interface.

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

The default cost of an interface is the reference bandwidth value/Bandwidth (the default reference bandwidth value is 100 Mbps).

Syntax

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

no ipv6 ospf *cost* [**instance** *instance-id*]

Parameter Description

cost: Cost of an OSPFv3 interface. The value range is from 0 to 65535.

instance *instance-id*: Configures a specified OSPFv3 instance of the interface. The value range is from 0 to 255.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

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

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

- For the 64 Kbps serial line, the cost is 1562.
- For the E1 line, the cost is 48.
- For the 10 Mbps Ethernet, the cost is 10.
- For the 100 Mbps Ethernet, the cost is 1.

The OSPFv3 cost configured through the **ipv6 ospf cost** command will overwrite the default configuration.

Examples

The following example sets the cost of an interface to **1**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 ospf cost 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 ospf interface**

1.25 ipv6 ospf dead-interval

Function

Run the **ipv6 ospf dead-interval** command to configure the neighbor dead interval of an interface.

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

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

Syntax

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

no ipv6 ospf dead-interval [**instance** *instance-id*]

Parameter Description

Dead-interval: Neighbor dead interval, in seconds. The value range is from 0 to 2147483647.

minimal hello-multiplier: Enables the fast hello function and sets the neighbor dead interval to **1** second.

multiplier: Hello packet sending times per second. The value range is from 3 to 20.

instance *instance-id*: Configures a specified OSPFv3 instance of the interface. The value range is from 0 to 255.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The OSPFv3 neighbor dead interval is contained in hello packets. If OSPF does not receive a hello packet from a neighbor within the neighbor dead interval, it declares that the neighbor is invalid and deletes this neighbor record from the neighbor list. By default, the neighbor dead interval is four times the hello packet sending interval. If the hello packet sending interval is modified, the neighbor dead interval is modified automatically.

This command can be used to manually modify the neighbor dead interval. However, the configuration must be made with caution. Pay attention to the following two issues:

(1) The dead interval cannot be smaller than the hello packet sending interval.

(2) The dead interval must be the same on all routers in the same network segment.

OSPFv3 supports the fast hello function:

Enabling the OSPFv3 fast hello function allows OSPFv3 to find neighbors more quickly and detect neighbor failures faster. You can enable the OSPFv3 fast hello function by specifying the **minimal hello-multiplier** keyword and the *multiplier* parameter. The **minimal** keyword sets the dead interval to 1s, and the value of **hello-multiplier** specifies the hello packet sending times per second. In this way, the hello packet sending interval drops to less than 1s.

If the fast hello function is enabled on an interface, the hello-interval field of the hello packets advertised on the interface is set to 0, and the hello-interval field of the hello packets received on this interface is ignored.

Note

The *dead-interval*, *minimal hello-multiplier*, and *hello-interval* parameters introduced for the fast hello function cannot be configured simultaneously.

No matter whether the fast hello function is enabled, the neighbor dead interval must be consistent among neighbor interfaces. The **hello-multiplier** value can be inconsistent provided that at least one hello packet can be received within the neighbor dead interval.

Run the **show ipv6 ospf interface** command to display the dead interval and fast hello interval configured for an interface.

Examples

The following example sets the neighbor dead interval of an interface to **60** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 ospf dead-interval 60
```

Notifications

If the neighbor dead interval is smaller than the hello packet sending interval, the following notification will be displayed:

```
% Warning: OSPFv3 dead interval should be higher than hello interval
```

If the hello packet sending interval is configured prior to the fast hello function, the following notification will be displayed:

```
% OSPFv3: Hello interval configured with hello-interval.
```

Common Errors

- The neighbor dead intervals configured on different ports in the same area are inconsistent.

Platform Description

N/A

Related Commands

- show ipv6 ospf interface

1.26 ipv6 ospf encryption

Function

Run the **ipv6 ospf encryption** command to enable OSPFv3 encryption on an interface.

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

Encryption is disabled by default.

Syntax

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

no ipv6 ospf encryption [**instance** *instance-id*]

Parameter Description

spi *spi*: Specifies a security parameter index. The value range is from 256 to 4294967295.

esp: Enables the ESP encryption mode.

des: Enables the DES encryption mode.

3des: Enables the 3DES encryption mode.

aes-cbc [**128** | **192** | **256**]: Enables the Advanced Encryption Standard-Cipher Block Chaining (AES-CBC) encryption mode. The encryption key length is 128, 192, or 256 bits.

des: Enables the DES encryption mode.

0: Indicates that the key is displayed in plaintext.

7: Indicates that the key is displayed in ciphertext.

des-key: Encryption key.

null: Indicates that no encryption mode is used.

md5: Enables the MD5 authentication mode.

sha1: Enables the SHA1 authentication mode.

key: Authentication key.

null: Indicates that no authentication mode is enabled.

instance *instance-id*: Configures a specified OSPFv3 instance of the interface. The value range is from 0 to 255.

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.

The device supports the following types of encryption and authentication:

Encryption modes: DES, 3DES, and AES-CBC.

Authentication modes: MD5 and SHA1

Note

OSPFv3 encryption and authentication parameters configured on the interconnected interfaces must be consistent.

Examples

The following example enables OSPFv3 encryption and authentication for an interface, configures the interface with null encryption and MD5 authentication, and sets the password to aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 ospf encryption ipsec spi 300 esp
null md5 aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Notifications

If this SPI has been used in this module, the following notification will be displayed:

```
% OSPFv3: SPI is already in use.
```

If this SPI has been used in another module, the following notification will be displayed:

```
% OSPFv3: SPI is already in use by others.
```

If this SPI has been configured on the local Interface, the following notification will be displayed:

```
% OSPFv3: Interface is already configured with the same SPI.
```

If encryption and authentication is re-configured for an interface with authentication configuration, the following notification will be displayed:

```
% OSPFv3: Interface is already configured with authentication so cannot configure
encryption.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 ospf interface**

1.27 ipv6 ospf hello-interval

Function

Run the **ipv6 ospf 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.

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

Syntax

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

no ipv6 ospf hello-interval [**instance** *instance-id*]

Parameter Description

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

instance *instance-id*: Configures a specified OSPFv3 instance of the interface. The value range is from 0 to 255.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The hello packet sending interval is contained in hello packets. A shorter interval indicates that OSPFv3 can detect topology changes more quickly, but the network traffic increases. The hello packet sending interval must be the same on all routers in the same network segment. If you want to manually modify the neighbor dead interval, ensure that the neighbor dead interval is longer than the hello packet sending interval.

Note

The *dead-interval minimal hello-multiplier* and *hello-interval* parameters introduced for the fast hello function cannot be configured simultaneously.

Examples

The following example sets the hello packet sending interval to **20** seconds on the interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 ospf hello-interval 20
```

Notifications

If the hello packet sending interval is configured on an interface that is configured with the *dead-interval minimal hello-multiplier* parameter of the fast hello function, the following notification will be displayed:

```
% OSPFv3: Hello interval configured with hello-multiplier.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- show ipv6 ospf interface

1.28 ipv6 ospf mtu-ignore

Function

Run the **ipv6 ospf mtu-ignore** command to disable MTU verification for an interface that receives database description packets.

Run the **no** form of this command to enable MTU verification for an interface that receives database description packets.

The MTU verification function is disabled by default.

Syntax

ipv6 ospf mtu-ignore [**instance** *instance-id*]

no ipv6 ospf mtu-ignore [**instance** *instance-id*]

Parameter Description

instance *instance-id*: Configures a specified OSPFv3 instance of the interface. The value range is from 0 to 255.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

On receiving a database description packet, OSPFv3 checks whether the MTU of the neighbor interface in the database description packet is the same as the MTU of the local interface. If the interface MTU specified in the received database description packet is greater than the MTU of the local interface, the adjacency fails to be set up. To resolve this problem, you can disable MTU verification.

Examples

The following example disables MTU verification for an interface that receives database description packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 ospf mtu-ignore
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.29 ipv6 ospf neighbor

Function

Run the **ipv6 ospf neighbor** command to configure OSPFv3 neighbors.

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

No neighbor is configured by default.

Syntax

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

no ipv6 ospf neighbor *ipv6-address* [**cost** *cost* | [**poll-interval** *poll-interval* | **priority** *value*] *] [**instance** *instance-id*]

Parameter Description

cost *cost*: Configures costs required to reach each neighbor in the P2MP network. This parameter is not defined by default and applicable only to the P2MP network. The value range is from 0 to 65535.

poll-interval *poll-interval*: Indicates the neighbor polling interval, in seconds. This parameter is applicable only to the NBMA network. The value range is from 0 to 2147483647, and the default value is **120**.

priority *priority*: Configures the priority of a neighbor in the NBMA network. This parameter is applicable only to the NBMA network. The value range is from 0 to 255, and the default value is **0**.

instance *instance-id*: Configures a specified OSPFv3 instance of the interface. The value range is from 0 to 255.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the IPv6 address of an OSPFv3 neighbor to FE80::2D0:F8FF:FE22:3533, priority value to **1**, and polling interval to **150** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 ospf network non-broadcast
Hostname(config-if-GigabitEthernet 0/1)# ipv6 ospf neighbor
fe80::2d0:f8ff:fe22:3533 priority 1 poll-interval 150
```

Notifications

If a neighbor is configured in the NBMA and P2MP networks, the following notification will be displayed:

```
% Neighbor command is allowed only on NBMA and point-to-multipoint networks.
```

If the IP address of a specified neighbor is not an IPv6 address, the following notification will be displayed:

```
% OSPFv3: Neighbor address needs to be a link-local address.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.30 ipv6 ospf network

Function

Run the **ipv6 ospf network** command to configure an OSPF network type of an interface.

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

By default, the interface type of OSPF is not configured. No interface is set to P2MP type by default.

Syntax

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

no ipv6 ospf network [**broadcast** | **non-broadcast** | **point-to-multipoint** [**non-broadcast**] | **point-to-point**] [**instance** *instance-id*]

Parameter Description

broadcast: Configures the broadcast network type for an interface.

non-broadcast: Configures the non-broadcast network type for an interface.

point-to-multipoint: Configures the P2MP network type for an interface.

point-to-multipoint non-broadcast: Configures the P2MP non-broadcast network type for an interface.

point-to-point: Configures the P2P network type for an interface.

instance *instance-id*: Configures a specified OSPFv3 instance of the interface. The value range is from 0 to 255.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

OSPFv3 network types are configured based on the network architecture. Ethernet and FDDI belong to the broadcast type. X.25, frame relay, and ATM belong to the NBMA type. PPP, HDLC, and LAPB belong to the P2P type. Each network type is restricted as follows:

- The broadcast type requires that the interfaces must have the broadcast capability.
- The P2P type requires that the interfaces are interconnected in one-to-one manner.
- The NBMA type requires full-meshed connections, and all interconnected routers can directly communicate with each other.
- The P2MP type does not raise any requirement.

Examples

The following example configures the OSPF network type of an interface as P2P.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 ospf network point-to-point
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- show ipv6 ospf interface

1.31 ipv6 ospf priority

Function

Run the **ipv6 ospf priority** command to configure the priority of an interface.

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

The priority value is **1** by default.

Syntax

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

no ipv6 ospf priority [**instance** *instance-id*]

Parameter Description

priority: Priority of an interface. The value range is from 0 to 255.

instance *instance-id*: Configures a specified OSPFv3 instance of the interface. The value range is from 0 to 255.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

In a broadcast network, a DR or BDR must be elected. During the DR or BDR election, the device with a higher priority will be preferentially elected as a DR or BDR. If the priority is the same, the device with a larger router ID will be preferentially elected as a DR or BDR.

A device with the priority 0 does not participate in the DR or BDR election.

Examples

The following example sets the priority of an interface to **0** so that the interface does not participate in the DR or BDR election.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 ospf priority 0
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- show ipv6 ospf interface

1.32 ipv6 ospf retransmit-interval

Function

Run the **ipv6 ospf retransmit-interval** command to configure the LSA retransmission interval on an interface.

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

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

Syntax

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

no ipv6 ospf retransmit-interval [**instance** *instance-id*]

Parameter Description

retransmit-interval: LSU retransmission interval, in seconds. The value range is from 1 to 65535.

instance *instance-id*: Configures a specified OSPFv3 instance of the interface. The value range is from 0 to 255.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

To ensure transmission reliability of the routing information, a router must get confirmation from a neighbor when sending LSAs to the neighbor. Users can use this command to configure the interval of waiting for confirmation from a neighbor based on the actual running environment. If no confirmation is received within the specified interval, the router retransmits LSAs.

The LSU retransmission interval must be longer than the round-trip transmission delay of data packets between two neighbors.

Examples

The following example sets the LSA transmission interval on an interface to **10** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 ospf retransmit-interval 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- show ipv6 ospf interface

1.33 ipv6 ospf subvlan

Function

Run the **ipv6 ospf subvlan** command to enable the OSPFv3 function in a super VLAN.

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

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

Syntax

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

no ipv6 ospf 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. The multicast packets corresponding to a super VLAN are also sent to its sub VLANs. OSPFv3 multicast packets will be replicated when they are sent in a super VLAN. If the super VLAN contains many sub VLANs, a great number of OSPF multicast packets are replicated, exceeding the processing capability of the device. This results in discarding of many packets and causes protocol flapping.

In most scenarios, the OSPFv3 function does not need to be enabled in a super VLAN, and it is disabled by default. In some other scenarios, OSPFv3 needs to be run in a super VLAN. In this case, you can decide to send multicast packets to a certain sub VLAN or to all sub VLANs as actually needed. Usually, packets need to be sent to only one sub VLAN. You can run this command to specify a 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 OSPFv3 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)# ipv6 ospf 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

1.34 ipv6 ospf transmit-delay

Function

Run the **ipv6 ospf transmit-delay** command to configure the LSU transmission delay on an interface.

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

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

Syntax

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

no ipv6 ospf transmit-delay [**instance** *instance-id*]

Parameter Description

transmit-delay: Delay for an OSPF interface to transmit LSU packets, in seconds. The value range is from 1 to 65535.

instance *instance-id*: Configures a specified OSPFv3 instance of the interface. The value range is from 0 to 255.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The sending delay and line transmission delay of the interface must be considered when *transmit-delay* is configured. For a low-speed line, the transmission delay of the interface must be set to a value greater than the default value.

Examples

The following example sets the LSU transmission delay on an interface to **2** seconds.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 ospf transmit-delay 2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- show ipv6 ospf interface

1.35 ipv6 router ospf

Function

Run the **ipv6 router ospf** command to enable an OSPFv3 routing process.

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

No OSPFv3 routing process is enabled by default.

Syntax

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

no ipv6 router ospf *process-id*

Parameter Description

process-id: OSPFv3 process ID. The value range is from 1 to 65535, and the default value is **1**.

vrf-name: VRF to which the OSPFv3 process belongs.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Run this command to enable an OSPFv3 routing process, and the device enters the routing process configuration mode.

A maximum of 32 OSPFv3 processes can be configured.

Examples

The following example enables an OSPFv3 process in vrf:vpn_1.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1 vrf vpn_1
```

Notifications

When an OSPFv3 process fails to be configured because **ipv6 unicast-routing** is not enabled, the following notification will be displayed:

```
IPv6 unicast-routing not enabled, OSPFv3 process can't configure
```

When the corresponding OSPFv3 process cannot be enabled because it is not allocated a router ID, the following notification will be displayed:

```
%OSPFV3-NORTRID: OSPFv3 process 1 failed to allocate unique router-id and cannot
start.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- show ipv6 ospf

1.36 ipv6 router ospf max-concurrent-dd

Function

Run the **ipv6 router ospf max-concurrent-dd** command to configure the maximum number of neighbors with which all the OSPFv3 routing processes can concurrently initiate or accept interaction.

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

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

Syntax

ipv6 router ospf max-concurrent-dd *max-neighbor*

no ipv6 router ospf max-concurrent-dd

Parameter Description

max-neighbor: Maximum number of neighbors that concurrently interact with the OSPF process. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When the performance of a router is affected because the router exchanges data with multiple neighbors, you can run this command to restrict the maximum of neighbors with which all OSPFv3 processes can concurrently initiate or accept interaction.

Examples

The following example sets the maximum number of neighbors with which all OSPFv3 processes can concurrently initiate or accept interaction to **4**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf max-concurrent-dd 4
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.37 log-adj-changes

Function

Run the **log-adj-changes** command to record the log of adjacency state changes.

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

The log record function is enabled by default.

Syntax

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

no log-adj-changes [**detail**]

Parameter Description

detail: Displays detailed information of neighbor state changes.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

The log records the log information of the following four types of events only:

The adjacency reaches the full state;

The adjacency leaves the full state;

The adjacency reaches the down state;

The adjacency leaves the down state.

Examples

The following example records the log of adjacency state changes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# log-adj-changes detail
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- ipv6 router ospf
- show ipv6 ospf

1.38 max-concurrent-dd

Function

Run the **max-concurrent-dd** command to configure the maximum number of neighbors with which the current OSPFv3 instance can concurrently initiate or accept interaction.

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

The maximum number of concurrent neighbors is **5** by default.

Syntax

max-concurrent-dd *neighbor-number*

no max-concurrent-dd

Parameter Description

neighbor- number: Maximum number of neighbors that concurrently interact with the OSPF instance. The value range is from 1 to 65535.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

When the performance of a router is affected because the router exchanges data with multiple neighbors, you can run this command to restrict the maximum number of neighbors with which each OSPFv3 instance can concurrently initiate or accept interaction.

Examples

The following example sets the maximum number of neighbors with which the current OSPFv3 instance can concurrently initiate or accept interaction to **4**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# max-concurrent-dd 4
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- ipv6 router ospf
- show ipv6 ospf

1.39 nsr

Function

Run the **nsr** command to enable the nonstop routing (NSR) function.

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

Routing process configuration mode

Default Level

14

Usage Guidelines

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

For the same OSPFv3 instance, either NSR or GR is enabled because they are mutually exclusive. Nevertheless, when NSR is enabled, the GR helper capability is supported.

The switchover of devices in distributed or VSU mode takes a period of time. If OSPFv3 neighbor keepalive duration is shorter than the switchover duration, the OSPFv3 neighbor relationship with the neighbor device is removed, and services are interrupted during the switchover. Therefore, you are advised to set the OSPFv3 neighbor keepalive duration not less than the default value when you are enabling the NSR function. When fast hello is enabled, the OSPFv3 neighbor keepalive duration is less than 1s and the OSPFv3 neighbor relationship times out during the switchover, causing NSR failures. Therefore, you are advised to disable fast hello when NSR is enabled.

Examples

The following example enables the NSR function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# nsr
```

Notifications

N/A

Common Errors

- The neighbor keepalive duration is short. When fast hello is enabled, the OSPFv3 neighbor relationship is removed during a switchover, causing forwarding interruption.

Platform Description

N/A

Related Commands

- ipv6 router ospf
- show ipv6 ospf

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

Syntax

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

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

Parameter Description

Default: Configures all interfaces as passive interfaces.

interface-type interface-number: Interface type and interface number.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

To prevent other routers in the network from learning the routing information of the local router, you can configure a specified network interface of the local router as the passive interface, or a specified IP address of a network interface as the passive address. The loopback interface and the interface that is not connected to any OSPF neighbor can be set to passive interfaces.

When an interface is configured as a passive interface, it no longer sends or receives hello packets.

This command takes effect only on an OSPFv3 interface, and not on a virtual link.

Examples

The following example configures all interfaces of the local router as passive interfaces and enables OSPFv3 on the interfaces of VLAN 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# passive-interface default
Hostname(config-router)# no passive-interface vlan 1
```

Notifications

If the specified interface is invalid, the following notification will be displayed:

```
% Interface is invalid.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- ipv6 router ospf
- show ipv6 ospf interface

1.41 redistribute

Function

Run the **redistribute** command to enable route redistribution and inject routing information of other routing protocols to an OSPFv3 routing process.

Run the **no** form of this command to disable this function or modify the redistribution parameters.

The route redistribution function is not enabled by default.

Syntax

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

no redistribute { **bgp** | **connected** | **isis** [*area-tag*] [**level-1** | **level-1-2** | **level-2**] * | **ospf** *process-id* [**match** { **external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**] } *] | **rip** | **static** } [**metric** | **metric-type** | **route-map** | **tag**] *

Parameter Description

bgp: Indicates redistribution from BGP.

connected: Indicates redistribution from direct routes.

isis [*area-tag*]: Indicates redistribution from IS-IS. Here, *area-tag* specifies an IS-IS instance.

level-1 | **level-2** | **level-1-2**: Redistributes IS-IS routes at the specified level.

ospf *process-id*: Indicates redistribution from OSPF. Here, *process-id* specifies an OSPF process. The value range is from 1 to 65535.

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.

metric *metric-value*: Configures a metric value of OSPFv3 external LSAs, which is specified based on *metric-value*. The value range is from 0 to 16777214.

metric-type { **1** | **2** }: Configures the metric type of external routes, which can be E-1 or E-2.

route-map *route-map-name*: Configures the redistribution route filtering rules. Here, the value of *route-map-name* cannot exceed 32 characters.

tag *tag-value*: Specifies the tag value of the route that is redistributed to an OSPFv3 routing domain. The value range is from 0 to 4294967295.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

When the device supports multiple routing protocols, collaboration between protocols is required. To run multiple routing protocols concurrently, the device must be able to redistribute routing information of a protocol to another protocol.

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

During redistribution of OSPFv3 routes, *match* can be configured to indicate that OSPFv3 routes of the specified sub-type are redistributed. By default, all types of OSPFv3 routes are redistributed.

For the **level** parameter configured for redistribution of IS-IS routes and the **match** parameter configured during redistribution of OSPFv3 routes, the routes are matched against the route map only when the sub-types of the routes are correct.

The **match** parameter in the route map rule used for route redistribution is matched based on the original information of the routes. The priority of the **tag**, **metric**, and **metric-type** parameters configured for route redistribution is lower than that of the **set** rule in the route map.

The **set metric** value of the associated route map should fall into the range of 0 to 16777214. If the value exceeds this range, routes cannot be introduced.

The configuration rules for the **no** form of the **redistribute** command are as follows:

- If some parameters are specified in the **no** form of this command, default values of these parameters will be restored.
- If no parameter is specified in the **no** form of this command, the entire command will be deleted.

For example, if **redistribute isis 112 level-2** is configured, you can run the **no redistribute isis 112 level-2** command to restore the default value of level-2. As **level-2** itself is the default value of the parameter, the configuration saved is still **redistribute isis 112 level-2** after the preceding **no** form of the command is executed. To delete the entire command, run the **no redistribute isis 112** command.

Examples

The following example redistributes a direct route and associates the route with the route map **test**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# redistribute connect metric 10 route-map test
```

The following example configures the route map **test** and changes the metric value of the matched routes from **20** to **30** and the metric value of other redistributed routes from **20** to **10**.

```
Hostname(config)# route-map test permit 10
Hostname(config-route-map)# match metric 20
Hostname(config-route-map)# set metric 30
```

Notifications

If routes of this instance are redistributed, the following notification will be displayed:

```
% Redistribution of "ospf 1" via "ospf 1" not allowed
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 router ospf**
- **show ipv6 ospf database**

1.42 router-id

Function

Run the **router-id** command to configure the ID of a router.

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

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

Syntax

router-id *router-id*

no router-id

Parameter Description

router-id: ID of a router, which is expressed in the IPv4 address.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

Every OSPFv3 router must be identified by using a router ID. You can configure an IPv4 address as the ID of the router, but ensure that the router ID is unique in an AS. If a router runs multiple OSPFv3 processes, ensure that the router ID of each process is unique.

After the router ID changes, OSPF performs a lot of internal processing. Therefore, you are not advised to change the router ID unless necessary. When an attempt is made to modify the router ID, a prompt is displayed, requesting you to confirm the modification. After an OSPFv3 process is enabled, you are advised to specify the router ID before configuring other parameters of the process.

Examples

The following example sets the router ID to 1.1.1.1.

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

Notifications

When you set the router ID to 0.0.0.0, which stops the OSPFv3 process, the following notification will be displayed:

```
% OSPFv3: router-id set to 0.0.0.0, process will not run.
```

When the configured router ID is duplicate with that of another process, the following notification will be displayed:

```
% OSPFv3: router-id %r is in use by process %s
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- ipv6 router ospf
- show ipv6 ospf

1.43 show ipv6 ospf

Function

Run the **show ipv6 ospf** command to display information of an OSPFv3 process.

Syntax

show ipv6 ospf [*process-id*]

Parameter Description

process-id: OSPFv3 process ID. The value range is from 1 to 65535.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays information of an OSPFv3 process.

```
Hostname> enable
Hostname# show ipv6 ospf
Routing Process "OSPFv3 (1)" with ID 1.1.1.1
Process uptime is 24 minutes
Enable two-way-maintain
SPF schedule delay 5 secs, Hold time between SPFs 10 secs
Initial LSA throttle delay 0 msecs
Minimum hold time for LSA throttle 5000 msecs
Maximum wait time for LSA throttle 5000 msecs
Lsa Transmit Pacing timer 40 msecs, 1 LS-Upd
Minimum LSA arrival 1000 msecs
Pacing lsa-group: 30 secs
Number of incomming current DD exchange neighbors 0/5
Number of outgoing current DD exchange neighbors 0/5
Number of external LSA 0. Checksum Sum 0x0000
Number of AS-Scoped Unknown LSA 0
Number of LSA originated 11
Number of LSA received 4
Log Neighbor Adjency Changes : Enabled
BFD enabled
Number of areas in this router is 2
Area BACKBONE(0)
Number of interfaces in this area is 1(1)
SPF algorithm executed 4 times
Number of LSA 3. Checksum Sum 0x1DDF1
Number of Unknown LSA 0
Area 0.0.0.1 (NSSA)
Number of interfaces in this area is 1(1)
SPF algorithm executed 5 times
Number of LSA 7. Checksum Sum 0x445FE
Number of Unknown LSA 0
```

Table 1-1Output Fields of the show ipv6 ospf Command

Field	Description
Routing Process "OSPFv3 (x)" with ID 1.1.1.1	OSPFv3 process ID and OSPFv3 router ID
Process uptime	Validation time of this OSPFv3 process (the process is invalid when the router ID is 0.0.0.0)
Enable two-way-maintain	Whether to enable two-way maintenance of OSPFv3
SPF schedule delay	Required delay time before calling the SPF computation when a topology change is received
SPF Hold time	Minimum holding time between two SPF computations
Initial LSA throttle delay	Minimum delay time of generating LSAs
Minimum hold time for LSA throttle	Minimum interval between two SPF computations
Maximum wait time for LSA throttle	Maximum interval between two SPF computations
Lsa Transmit Pacing timer	LSA group update frequency
Minimum LSA arrival	Minimum receiving delay time of LSAs
Pacing lsa-group	Group pace interval
Incomming current DD exchange neighbors	Number of neighbors in interaction. Incoming means that a neighbor enters the Exstart state for the first time.
Outgoing current DD exchange neighbors	Number of neighbors in interaction. Outgoing means that a neighbor returns from a higher state to the Exstart state for re-interaction.
Number of external LSA	Number of external LSAs stored in the database
External LSA Checksum Sum	Sum of checksums of external LSAs stored in the database
Number of AS-Scoped Unknown LSA	Number of unknown LSAs in the flooding scope
Number of LSA originated	Number of generated LSAs
Number of LSA received	Number of received LSAs
Log Neighbor Adjency Changes	Whether the neighbor state change recording is enabled
BFD enabled	Whether to associate OSPFv3 with BFD
Number of areas in this router	Number of areas on this router

Field	Description
Number of interfaces in this area	Number of interfaces in this area
SPF algorithm executed	SPF computation times
Number of LSA	Total number of LSAs in this area
Checksum Sum	Sum of the checksums of LSAs in this area
Number of Unknown LSA	Number of LSAs of unknown types received in this area
NSSA Translator State	Whether an NSSA LSA is translated to an external LSA. This field is valid only for the OSPFv3 process that is an ABR in the NSSA.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.44 show ipv6 ospf database

Function

Run the **show ipv6 ospf database** command to display the database information of an OSPFv3 process.

Syntax

show ipv6 ospf [*process-id*] **database** [**database-summary** | *lsa-type* [**adv-router** *router-id*]]

Parameter Description

process-id: OSPFv3 process ID. The value range is from 1 to 65535.

lsa-type: LSA type, including

NSSA-external-LSA, AS-external-LSAs, Link-LSAs, Inter-Area-Prefix-LSAs, Inter-Area-Router-LSAs, Intra-Area-Prefix-LSAs, Network-LSAs, and Router-LSAs.

If this parameter is not specified, all LSA information is displayed.

adv-route*r router-id*: Displays LSA information generated by a specified OSPFv3 neighbor.

database-summary: Displays the statistical information of each type of LSAs in the OSPFv3 LSDB.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the database information of an OSPFv3 process.

```
Hostname> enable
Hostname# show ipv6 ospf database
OSPFv3 Router with ID (1.1.1.1) (Process 1)
Link-LSA (Interface GigabitEthernet 0/1)
Link State ID   ADV Router    Age   Seq#        CkSum    Prefix
0.0.0.2         1.1.1.1       197   0x80000001  0x7cd8   0
0.0.0.5         2.2.2.2       206   0x80000001  0x8c86   0
Link-LSA (Interface Loopback 1)
Link State ID   ADV Router    Age   Seq#        CkSum    Prefix
0.0.64.1        1.1.1.1       82    0x80000001  0xb760   0
Router-LSA (Area 0.0.0.0)
Link State ID   ADV Router    Age   Seq#        CkSum    Link
0.0.0.0         1.1.1.1       17    0x80000006  0x62a1   1
0.0.0.0         2.2.2.2       156   0x80000003  0x8653   1
Network-LSA (Area 0.0.0.0)
Link State ID   ADV Router    Age   Seq#        CkSum
0.0.0.5         2.2.2.2       157   0x80000001  0xf8f6
Router-LSA (Area 0.0.0.1)
Link State ID   ADV Router    Age   Seq#        CkSum    Link
0.0.0.0         1.1.1.1       17    0x80000002  0x0529   0
Inter-Area-Prefix-LSA (Area 0.0.0.1)
Link State ID   ADV Router    Age   Seq#        CkSum
0.0.0.1         1.1.1.1       77    0x80000002  0x83b4
AS-external-LSA
Link State ID   ADV Router    Age   Seq#        CkSum
0.0.0.1         1.1.1.1       1     0x80000001  0x6035 E2
```

Table 1-1Output Fields of the show ipv6 ospf database Command

Field	Description
Link-LSA (Interface GigabitEthernet 0/1) Type-1 LSA—Router-LSA Type-2 LSA—Network-LSA Type-3 LSA—Inter-Area-Prefix-LSA Type-4 LSA—Inter-Area-Router-LSA Type-5 LSA—AS-External-LSA	Types of OSPFv3 Link-LSA

Field	Description
Type-7 LSA—NSSA-external-LSA Type-8 LSA—Link-LSA Type-9 LSA—Intra-Area-Prefix-LSA	
Link State ID	Link state ID of LSA
ADV Router	Advertising router of LSA
Age	LSA aging time
Seq#	LSA serial number
CkSum	LSA checksum
Prefix	Number of IPv6 address prefixes in Type-8 LSA
Link	Number of links in Type-1 LSA

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.45 show ipv6 ospf interface

Function

Run the **show ipv6 ospf interface** command to display the information of an OSPFv3 interface.

Syntax

show ipv6 ospf [*process-id*] **interface** [**brief** | *interface-type interface-number*]

Parameter Description

process-id: OSPFv3 process ID. The value range is from 1 to 65535.

brief: Displays the brief information of an interface.

interface-type interface-number: Interface type and interface number.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays information of an OSPFv3 interface.

```
Hostname> enable
Hostname# show ipv6 ospf interface
GigabitEthernet 0/1 is up, line protocol is up
Interface ID 2
IPv6 Prefixes
fe80::2d0:22ff:fe22:2223/64 (Link-Local Address)
OSPFv3 Process (1), Area 0.0.0.0, Instance ID 0
Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State BDR, Priority 1,
BFD enabled
Designated Router (ID) 2.2.2.2
Interface Address fe80::c800:eff:fe84:1c
Backup Designated Router (ID) 1.1.1.1
Interface Address fe80::2d0:22ff:fe22:2223
Timer interval configured,Hello 10,Dead 40,Wait 40,Retransmit 5
Hello due in 00:00:02
Neighbor Count is 1, Adjacent neighbor count is 1
Hello received 26 sent 26, DD received 5 sent 4
LS-Req received 1 sent 1, LS-Upd received 3 sent 6
LS-Ack received 6 sent 2, Discarded 0
```

Table 1-1Output Fields of the show ipv6 ospf interface Command

Field	Description
GigabitEthernet 0/1 is up, line protocol is up	Link and protocol state
Interface ID	Interface index
IPv6 Prefixes	IPv6 prefix information of an interface
OSPFv3 Process (1)	OSPFv3 process where an interface resides
Area	Area to which an interface belongs
Instance ID	Instance to which an interface belongs
Router ID	ID of an OSPFv3 router
Network Type	OSPFv3 network type
Cost	Cost of an OSPFv3 interface
Transmit Delay	Transmission delay of an OSPFv3 interface

Field	Description
State	DR/BDR state
Priority	Priority of an OSPFv3 interface
BFD enabled	Whether to associate OSPFv3 with BFD
Designated Router (ID)	ID for the DR of this interface
DR's Interface address	Interface address for the DR of this interface
Backup Designated Router (ID)	ID for the BDR of this interface
BDR's Interface address	Interface address for the BDR of this interface
Time intervals configured	Hello, Dead, Wait, and Retransmit time corresponding to this interface
Hello due in	Hello packet sending duration last time
Neighbor Count	Total number of neighbors
Adjacent neighbor count	Number of neighbors in full neighbor relationship
Hello received sent	Statistics of the received and sent hello packets
DD received send	Statistics of the received and sent DD packets
LS-Req received send	Statistics of the received and sent LS request packets
LS-Upd received send	Statistics of the received and sent LS update packets
LS-Ack received send	Statistics of the received and sent LS response packets
Discard	Statistics of the discarded OSPFv3 packets

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.46 show ipv6 ospf neighbor

Function

Run the **show ipv6 ospf neighbor** command to display neighbor information of an OSPFv3 process.

Syntax

show ipv6 ospf [*process-id*] **neighbor** [**detail** | *interface-type interface-number* [**detail**] | *neighbor-id* | **statistics**]

Parameter Description

process-id: OSPFv3 process ID. The value range is from 1 to 65535.

detail: Displays the neighbor details.

interface-type interface-number: Interface type and interface number.

neighbor-id: Route ID of a specified neighbor.

statistics: Displays the statistics of neighbors.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the brief information of an OSPFv3 neighbor.

```
Hostname> enable
Hostname# show ipv6 ospf neighbor
OSPFv3 Process (1) , 1 Neighbors, 1 is Full:
Neighbor ID  Pri  State     Dead Time   Interface         Instance ID
2.2.2.2      1    Full/DR   00:00:33    GigabitEthernet 0/1  0
Hostname# show ipv6 ospf neighbor detail
Neighbor 2.2.2.2, interface address fe80::c800:eff:fe84:1c
In the area 0.0.0.0 via interface GigabitEthernet 0/1
Neighbor priority is 1, State is Full, 6 state changes
DR is 2.2.2.2 BDR is 1.1.1.1
Options is 0x000013 (-|R|-|E|V6)
Dead timer due in 00:00:36
Database Summary List 0
Link State Request List 0
Link State Retransmission List 0
BFD session state up
```

Table 1-1Output Fields of the show ipv6 ospf neighbor Command

Field	Description
OSPFv3 Process (1), 1 Neighbors, 1 is Full:	Process ID, number of neighbors, and number of neighbors in full neighbor relationship
Neighbor ID	Router ID of a neighbor

Field	Description
Pri	Priority of a neighbor
State	Neighbor states, including Down—Initial status of a neighbor in a session Attempt—When the interface of a device in the NBMA qualified for DR election becomes valid, the neighbor state is reset to Attempt. This state is applicable to neighbors in the NBMA. Init—The neighbor receives a hello packet that does not contain the neighbor ID. 2-Way—The hello packet received from the neighbor contains the local router ID, indicating that 2-way communication has been established. Exstart—An active/standby relationship is established between a router and its neighbors and the sequence number of DD packets is determined, which is ready for DD packet exchange. Exchange—A router sends DD packets that describe local LSDB information to its neighbors. Loading—A router sends LSR packets to a neighbor to request the latest LSA. Full—A router establishes full adjacency relationship with neighbors. OSPF routers play the following roles in broadcast and NBMA networks: DR—A DR exists in only broadcast and NBMA networks. BDR—A BDR exists in only broadcast and NBMA networks. DRother—Indicates all other devices except the DR and BDR in broadcast and NBMA networks. In P2P and P2MP networks, the preceding roles do not exist, and this field is displayed as a hyphen (-).
Dead Time	Time before the neighbor enters the dead state
Instance ID	ID of a neighbor instance
Interface	Interface connected to neighbors
Interface address	Interface address of the neighbor router
In the area	Area that learns this neighbor
via interface	Interface that learns this neighbor
Neighbor priority	Priority value of the neighbor
State changes times	Change times of the neighbor state
DR	Interface address (namely, the DR field in the hello packet) of the DR elected by

Field	Description
	the neighbor router
BDR	Interface address (namely, the BDR field in the hello packet) of the BDR elected by the neighbor router
Options	Options for the hello packet
Dead Time due in	Time when the dead state of this neighbor is declared
Database Summary List	DD packet statistics of the neighbor
Link State Request List	LSR packet statistics of the neighbor
Link State Retransmission List	Retransmitted packet statistics of the neighbor
BFD session state up	BFD association state

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.47 show ipv6 ospf restart

Function

Run the **show ipv6 ospf restart** command to display the information related to OSPFv3 GR.

Syntax

show ipv6 ospf [*process-id*] **restart**

Parameter Description

process-id: OSPFv3 process ID. The value range is from 1 to 65535.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the current status of the restarter.

```
Hostname> enable
Hostname# show ipv6 ospf restart
Routing Process is ospf 1
Graceful-restart enabled
Restart grace period 120 secs
Current Restart status is plannedRestart
Current Restart remaining time 50 secs
Graceful-restart helper support enabled
```

Table 1-1Output Fields of the show ipv6 ospf restart Command

Field	Description
Routing Process is ospf	ID of a process that starts GR
Graceful-restart enabled	Whether to enable the GR function
Restart grace period	GR period
Current Restart status	Current GR status
Current Restart remaining time	Remaining GR time
Graceful-restart helper support enabled	Whether to support restart helper

The following example displays the current status of the restart helper.

```
Hostname> enable
Hostname# show ipv6 ospf restart
Routing Process is ospf 1
Neighbor 10.1.1.2, interface addr 10.1.1.2
In the area 0.0.0.0 via interface GigabitEthernet 6/0/0
Graceful-restart helper enabled
Current helper status is helping
Current helper remaining time 50 secs
```

Table 1-2Output Fields of the show ipv6 ospf restart Command

Field	Description
Neighbor	Router ID of the neighbor of the helper
interface addr	IP address of the interface corresponding to the helper
In the area	Area in which the helper resides
interface GigabitEthernet	Interface corresponding to the helper
Graceful-restart helper enabled	Whether to enable the helper function

Field	Description
Current helper status	Current helper status
Current helper remaining time	Remaining time of a router in the helper state

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.48 show ipv6 ospf route

Function

Run the **show ipv6 ospf route** command to display the routing information of OSPFv3.

Syntax

show ipv6 ospf [*process-id*] **route [count]**

Parameter Description

process-id: OSPFv3 process ID. The value range is from 1 to 65535.

count: Displays the number of OSPFv3 routes.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the routing information of OSPFv3.

```
Hostname> enable
Hostname# show ipv6 ospf route
OSPFv3 Process (1)
Codes: C - connected, D - Discard, B – Backup O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

       E1 - OSPF external type 1, E2 - OSPF external type 2Destination
Metric   Next-hop
```

```
E2 2001:DB8:1::/64   1/20     via fe80::c800:eff:fe84:1c, GigabitEthernet 0/1
B                             via fe80::c800:eff:fe84:1d, GigabitEthernet 0/2
O  2001:DB8:2::/64   11       via fe80::c800:eff:fe84:1c, GigabitEthernet 0/1,
Area 0.0.0.0
```

Table 1-1Output Fields of the show ipv6 ospf route Command

Field	Description
OSPFv3 Process (1)	OSPFv3 process ID
Destination	Type and destination network of OSPFv3 routes OSPFv3 supports the following four types of routes: **C**: Direct route **D**: Black-hole route **O**: Internal route of OSPFv3 **IA**: Inter-area route of OSPFv3 **N1**: NSSA external type 1 route of OSPFv3 **N2**: NSSA external type 2 route of OSPFv3 **E1**: External type 1 route of OSPFv3 **E2**: External type 2 route of OSPFv3
Metric	Cost of a route
Next-hop	Next hop of a route

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.49 show ipv6 ospf summary-prefix

Function

Run the **show ipv6 ospf summary-prefix** command to display external route summarization information of OSPFv3.

Syntax

show ipv6 ospf [*process-id*] **summary-prefix**

Parameter Description

process-id: OSPFv3 process ID. The value range is from 1 to 65535.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the external route summarization information of OSPFv3.

```
Hostname> enable
Hostname# show ipv6 ospf summary-prefix
OSPFv3 Process 1, Summary-prefix:
2001:1::/64, Metric 20, Type 2, Tag 0, Match count 5, advertise
```

Table 1-1Output Fields of the show ipv6 ospf summary-prefix Command

Field	Description
Summary-prefix	Prefix of a summarized route
Metric	Metric of a summarized route
Type	Type of a summarized route
Match count	Number of summarized routes
Advertise	Advertisement after summarization
Tag	Tag of a summarized route

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.50 show ipv6 ospf topology

Function

Run the **show ipv6 ospf topology** command to display the topological information of an OSPFv3 area.

Syntax

show ipv6 ospf [*process-id*] **topology** [**area** *area-id*]

Parameter Description

process-id: OSPFv3 process ID. The value range is from 1 to 65535.

area-id: Area ID, which can be a decimal integer or an IP address. The value range is from 0 to 4294967295.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the topological information of an OSPFv3 area.

```
Hostname> enable
Hostname# show ipv6 ospf topology
OSPFv3 Process (1)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID        Bits  Metric     Interface             Next-Hop(router/address)
1.1.1.1             B
2.2.2.2            EB  1          GigabitEthernet 0/6
2.2.2.2/fe80::21a:a9ff:fe41:5b06
OSPFv3 paths to Area (0.0.0.1) routers
Router ID        Bits  Metric     Interface             Next-Hop(router/address)
1.1.1.1           V B
2.2.2.2           VEB  1          GigabitEthernet 0/6
2.2.2.2/fe80::21a:a9ff:fe41:5b06
```

Table 1-1Output Fields of the show ipv6 ospf topology Command

Field	Description
OSPFv3 paths to Area	Topological information corresponding to an area
Router ID	Router ID of a node
Bits	Options for a node
Metric	Metric from this node to the root node
Interface	Outbound interface to this node
Next-Hop(router/address)	Next hop to this node

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.51 show ipv6 ospf virtual-links

Function

Run the **show ipv6 ospf virtual-links** command to display virtual link information of an OSPFv3 process.

Syntax

show ipv6 ospf [*process-id*] **virtual-links**

Parameter Description

process-id: OSPFv3 process ID. The value range is from 1 to 65535.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays virtual link information of OSPFv3.

```
Hostname> enable
Hostname# show ipv6 ospf virtual-links
Virtual Link VLINK1 to router 1.1.1.1 is up
  Transit area 0.0.0.1 via interface GigabitEthernet 0/1, instance ID 0
  Local address 2001::2/128
  Remote address 2001::1/128
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:08
Adajcency state Full
```

Table 1-1Output Fields of the show ipv6 ospf virtual-links Command

Field	Description
Virtual Link VLINK1 to router	Neighbor and neighbor state of a virtual link

Field	Description
Transit area	Transmission area of a virtual link
via interface	Interface associated with a virtual link
Local address	Address of the local interface
Remote address	Address of the peer interface
Transmit Delay	Transmission delay of a virtual link
State	Network type of a virtual link
Timer intervals configured	Timer of a virtual link, including Hello, Dead, and Retransmit
Hello due in	Hello packet sending interval
Adjacency state	Neighbor state of a virtual link

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.52 summary-prefix

Function

Run the **summary-prefix** command to configure a summarized route for the external routes of an OSPFv3 routing domain.

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

Route summarization is disabled by default.

Syntax

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

no summary-prefix *ipv6-prefix*/*prefix-length* [[**cost** | **tag**] * | **not-advertise**]

Parameter Description

ipv6-prefix/prefix-length: Range of IP addresses to be summarized.

cost *cost*: Configures a cost value of the summarized routes. The value range is from 0 to 16777214. The default metric value is the minimum cost value of the summarized routes.

tag *tag-value*: Specifies the tag value of the route that is redistributed to an OSPFv3 routing domain. The value range is from 0 to 4294967295.

not-advertise: Does not advertise this summarized route to neighbors. If this parameter is not specified, this summarized route is advertised.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

When routes are redistributed from other routing processes and injected to the OSPFv3 routing process, each route is advertised to the OSPFv3 routers using an external LSA. If the injected routes are a continuous address space, the ASBR can advertise only one summarized route to reduce the size of the routing table.

While **area range** summarizes the routes between OSPFv3 areas, **summary-prefix** summarizes external routes of the OSPFv3 routing domain.

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

Examples

The following example summarizes external routes of the OSPFv3 routing domain as 2001:DB8::/64 and advertises the routes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# summary-prefix 2001:db8::/64
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- ipv6 router ospf
- show ipv6 ospf summary-prefix

1.53 timers lsa arrival

Function

Run the **timers lsa arrival** command to configure the delay for receiving same LSAs.

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

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

Syntax

timers lsa arrival *arrival-time*

no timers lsa arrival

Parameter Description

arrival-time: Delay for receiving same LSAs, in milliseconds. The value range is from 0 to 600000.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

No processing is performed if the same LSAs are received within the specified time to avoid resource consumption.

Examples

The following example sets the delay for receiving the same LSAs to **2** seconds at least.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# timers lsa arrival 2000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- ipv6 router ospf
- show ipv6 ospf

1.54 timers pacing lsa-group

Function

Run the **timers pacing lsa-group** command to configure a group update time of LSAs.

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

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

Syntax

timers pacing lsa-group *update-time*

no timers pacing lsa-group

Parameter Description

update-time: Group update time of LSAs, in seconds. The value range is from 10 to 1800.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

Every LSA has a time to live (LSA age). When the LSA age reaches 1800s, the LSA age must be updated to prevent LSAs from being cleared because their age reaches the maximum time to live. If LSA update and aging computation are performed for every LSA, the device will consume a lot of CPU resources.

To use CPU resources effectively, you can refresh LSAs by group on the device. The interval of group refreshment is called group pacing interval. The group refreshment operation is to organize the LSAs generated within a group pacing interval into a group and refresh the group as a whole.

If the total number of LSAs does not change, a larger group pacing interval indicates that more LSAs need to be processed after timeout. To maintain the CPU stability, the number of LSAs to be processed upon each timeout cannot be too large. If the number of LSAs is large, you are advised to reduce the group pacing interval. For example, if there are 10,000 LSAs in the database, you can reduce the pacing interval; if there are 40 to 100 LSAs, you can set the pacing interval to 10-20 minutes.

Examples

The following example sets the LSA group refresh time to 120 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# timers pacing lsa-group 120
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 router ospf**
- **show ipv6 ospf**

1.55 timers pacing lsa-transmit

Function

Run the **timers pacing lsa-transmit** command to configure the LSA group sending interval.

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

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

Syntax

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

no timers pacing lsa-transmit

Parameter Description

transmit-time: LSA group sending interval, in milliseconds. The value range is from 10 to 1000.

transmit-count: Number of LS-UPD packets in each group. The value range is from 1 to 200.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

If the number of LSAs is large and the device load is heavy in an environment, properly configuring *transimit-time* and *transimit-count* can limit the number of LS-UPD packets flooded in the network.

If the CPU usage is not high and the network bandwidth load is not heavy, reducing the value of *transimit-time* and increasing the value of *transimit-count* can accelerate the environment convergence.

Examples

The following example sets the LSA group sending interval to **50** ms and the number of LS-UPD packets in each group to **20**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# timers pacing lsa-transmit 50 20
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- ipv6 router ospf
- show ipv6 ospf

1.56 timers spf

Function

Run the **timers spf** command to configure the delay time for SPF computation after an OSPFv3 process receives the topological change information and the interval between two SPF computations.

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

By default, the **timers spf** command does not take effect, and the delay for SPF computation is subject to the default configuration of the **timers throttle spf** command. Refer to the description of the **timers throttle spf** command.

Syntax

timers spf *spf-delay spf-holdtime*

no timers spf

Parameter Description

spf-delay: Delay for SPF computation, in seconds. After receiving the topological change information, the OSPF routing process must wait for the specified time before performing SPF computation. The value range is from 0 to 2147483647.

spf-holdtime: Interval between two SPF computations, in seconds. If the delay time expires but the interval between two SPF computations does not expire, SPF computation still cannot be performed. The value range is from 0 to 2147483647.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

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

Smaller values of *spf-delay* and *spf-holdtime* mean that the OSPF can adapt to topological changes more quickly. In other words, a shorter network convergence time means that more CPU time of the router will be occupied.

The configurations of **timers spf** and **timers throttle spf** are mutually overwritten.

Examples

The following example sets the delay time for SPF computation to **3** seconds after an OSPFv3 process receives the topological change information, and sets the interval between two SPF computations to **9** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 20
Hostname(config-router)# timers spf 3 9
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 router ospf**
- **show ipv6 ospf**

1.57 timers throttle lsa all

Function

Run the **timers throttle lsa all** command to configure an exponential backoff algorithm of LSA packet generation.

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

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

Syntax

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

no timers throttle lsa all

Parameter Description

delay-time: Minimum delay for LSA generation, in milliseconds. The first LSA in the database is always generated instantly. The value range is from 0 to 600000.

hold-time: Minimum interval between the first LSA update and the second LSA update, in milliseconds. The value range is from 0 to 600000.

max-wait-time: Maximum interval between two LSA updates when the LSA is updated continuously, in milliseconds. This interval is also used to determine whether the LSA is updated continuously. The value range is from 0 to 600000.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

If a high convergence requirement is raised when a link changes, you can set *delay-time* to a smaller value. You can also appropriately increase the values of the preceding parameters to reduce the CPU usage. When this command is used for configuration, the value of *hold-time* cannot be smaller than the value of *delay-time*, and the value of *max-wait-time* cannot be smaller than the value of *hold-time*.

Examples

The following example sets the minimum delay of LSA generation to **10** ms, the minimum interval between the first update and the second update to **1** second, and the maximum interval between two LSA updates to **5** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# timers throttle lsa all 10 1000 5000
```

Notifications

If the configured value of *max-wait-time* is smaller than that of *hold-time*, the following notification will be displayed:

```
% Warning: max-wait-time should be no less than hold-time, set to (5)
```

If the configured value of *hold-time* is smaller than that of *delay-time*, the following notification will be displayed:

```
% Warning: hold-time should be no less than delay-time, set to (5).
```

Common Errors

- The configured value of *hold-time* is smaller than that of *delay-time* or the configured value of *max-wait-time* is smaller than that of *hold-time*.

Platform Description

N/A

Related Commands

- **ipv6 router ospf**
- **show ipv6 ospf**

1.58 timers throttle route

Function

Run the **timers throttle route** command to configure the delay time for route computation when an OSPFv3 process receives changed inter-area and external LSAs.

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

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

Syntax

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

no timers throttle route { **ase** | **inter-area** }

Parameter Description

ase: Indicates external route computation.

ase-delay: Delay for external route computation, in milliseconds. When the OSPF process receives external LSA change information, the route computation triggered should be performed at least after the ase-delay for external route computation elapses. The value range is from 0 to 600000.

inter-area: Indicates inter-area route computation.

ia-delay: Delay for inter-area route computation, in milliseconds. When the OSPF process receives inter-area LSA change information, the route computation triggered should be performed at least after the ia-delay for inter-area route computation elapses. The value range is from 0 to 600000.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

If a strict requirement is raised for the network convergence time, use the default value.

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

Examples

The following example sets the delay for inter-area route computation to **1** second.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# timers throttle route inter-area 1000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 router ospf**

1.59 timers throttle spf

Function

Run the **timers throttle spf** command to configure the delay time for SPF computation when an OSPFv3 process receives topological change information, and the minimum and maximum intervals for two SPF computations.

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

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

Syntax

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

no timers throttle spf

Parameter Description

spf-delay: Delay for SPF computation, in milliseconds. When the OSPF process receives topological change information, the SPF computation triggered should be performed at least after the spf-delay for SPF computation elapses. The value range is from 1 to 600000.

spf-holdtime: Minimum interval between two SPF computations, in milliseconds. The value range is from 1 to 600000.

spf-max-waittime: Maximum interval between two SPF computations, in milliseconds. The value range is from 1 to 600000.

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

Here, *spf-delay* indicates the minimum time between the occurrence of a topology change and the start of SPF computation. *spf-holdtime* indicates the minimum interval between the first and second SPF computations. After that, the interval between two SPF computations must be at least twice of the previous interval. When the interval reaches *spf-max-waittime*, the interval cannot increase again. If the interval between two SPF computations already exceeds the required minimum value, the interval for SPF computation is computed starting from *spf-holdtime*.

You can set *spf-delay* and *spf-holdtime* to values smaller than the default values to accelerate topology convergence. The value of *spf-max-waittime* can be set to a larger value to reduce SPF computation. Flexible settings can be used based on stability of the network topology.

Compared with the **timers spf** command, this command supports more flexible settings to accelerate SPF computation convergence and further reduce the system resources consumed by SPF computation when the topology continuously changes. Therefore, you are advised to use the **timers throttle spf** command for configuration.

Notes:

- The value of *spf-holdtime* cannot be smaller than that of *spf-delay*; otherwise, the value of *spf-holdtime* will be automatically set to the value of *spf-delay*.
- The value of *spf-max-waittime* cannot be smaller than that of *spf-holdtime*; otherwise, *spf-max-waittime* will be automatically set to the value of *spf-holdtime*.
- The configurations of **timers throttle spf** and **timers spf** are mutually overwritten.
- When both **timers throttle spf** and **timers spf** are not configured, the default values of **timers throttle spf** prevail.

Examples

The following example sets the delay for SPF computation, hold time, and maximum interval for two SPF computations to 5 ms, 1000 ms, and 90000 ms, respectively. If the topology continuously changes, the delay for SPF computation is set to 5 ms, 1s, 3s, 7s, 15s, 31s, 63s, 89s, 179s, and (179+90)s..., respectively.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 20
Hostname(config-router)# timers spf 5 1000 90000
```

Notifications

If the configured value of *max-wait-time* is smaller than that of *hold-time*, the following notification will be displayed:

```
% Warning: max-wait-time should be no less than hold-time, set to (5).
```

If the configured value of *hold-time* is smaller than that of *delay-time*, the following notification will be displayed:

```
% Warning: hold-time should be no less than delay-time, set to (5).
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- ipv6 router ospf
- show ipv6 ospf

1.60 two-way-maintain

Function

Run the **two-way-maintain** command to enable the two-way maintenance function of OSPFv3.

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

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

Syntax

two-way-maintain

no two-way-maintain

Parameter Description

N/A

Command Modes

Routing process configuration mode

Default Level

14

Usage Guidelines

In a large network, a lot of packets may be sent or received, occupying too much CPU and memory. As a result, some packets are delayed or discarded. If the processing time of Hello packets exceeds the neighbor dead interval, the adjacency will be destroyed due to timeout. If the two-way maintenance function is enabled, in addition to the hello packets, the DD, LSU, LSR, and LSAck packets from a neighbor can also be used to maintain the bidirectional communication between neighbors when a large number of packets exist 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 an OSPF process.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 router ospf 1
Hostname(config-router)# no two-way-maintain
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 router ospf**
- **show ipv6 ospf**