O Commands

object

o specify an object for a tracked list, use the **object** command. To remove the object from the tracked list, use the **no** form of this command.

object **object-number** [**not**] [**weight** *weight-number*]
no **object** **object-number**

Syntax Description

not	(Optional) Negates the state of an object. **Note** The **not** keyword cannot be used in a weight or percentage threshold list. It can only be used in a Boolean list.
weight *weight-number*	(Optional) Specifies a threshold weight for each object.

Command Default

None

Command Modes

tracking configuration

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

You can configure an object track list that contains multiple tracked objects. A tracked list contains one or more objects.

The Boolean expression enables two types of calculation by using either “and” or “or” operators.

You can also configure an object track list that contains a percentage threshold.The percentage of up objects must exceed the configured track list up percent threshold before the track list is in an up state. For example, if the tracked list has three objects, and you configure an up threshold of 60%, two of the objects must be in the up state (66% of all objects) for the track list to be in the up state.

You can also configure an object track list that contains a weight threshold. A tracked list contains one or more objects. The combined weight of up objects must exceed the configured track list up weight threshold before the track list is in an up state. For example, if the tracked list has three objects with the default weight of 10 each, and you configure an up threshold of 15, two of the objects must be in the up state (combined weight of 20) for the track list to be in the up state.

This command does not require a license.

Examples

This example shows how to configure a track list with an up weight threshold of 30 and a down threshold of 10:

```
switch(config)# track 1 list threshold weight
switch(config-track)# threshold weight up 30 down 10
switch(config-track)# object 10 weight 15
switch(config-track)# object 20 weight 15
switch(config-track)# object 30
```

Related Commands

Command	Description
track list	Configures a track list for object tracking.

ospfv3 authentication ipsec

To enable authentication of OSPFv3 packets for a particular interface, use the **ospfv3 authentication ipsec** command at the interface level. To disable the authentication of OSPFv3 packets, use the **no** form of this command.

ospfv3 authentication ipsec spi *spi auth* [{**0** | **3** | **7**}] *key*
no ospfv3 authentication ipsec spi *spi*

Syntax Description

spi	Specifies the Security Policy Index.
spi	Value of **spi**. It ranges from 256 to 4294967295.
auth	Authentication algorithm. Its value can be md1 / sha1 / null.
key	Authentication password.
0	Specifies that the authentication password is unencrypted.
3	Specifies that the authentication password is 3DES encrypted.
7	Specifies that the authentication password is Cisco type 7 encrypted.

Command Default

The OSPFv3 packets are not authenticated by default.

Command Modes

Interface configuration (config-if).

Command History

Release	Modification
7.3(0)D1(1)	This command was introduced.

Usage Guidelines

Before running this command, ensure that you have enabled the authentication package with the **feature imp** command.

Examples

The following example shows how to authenticate OSPFv3 packets at the ethernet interface 2/1:

```
switch# configure terminal
switch(config)# feature imp
witch(config)# interface ethernet 2/1
switch(config-if)# ipv6 router ospfv3 1
switch(config-if)# ospfv3 authentication ipsec spi 301 md5 1234
```

Related Commands

Command	Description
area authentication ipsec	Enables authentication of the OSPFv3 packets for all interfaces under the area.
authentication ipsec	Enables authentication of the OSPFv3 packets at the router level.

ospfv3 esp at router level

To enable encryption of OSPFv3 packets on a per interface basis at router level, use below commands.

encryption ipsec spi <*spi_val*> **esp** { **3des [0|3|7] <key>** | **aes 128 [0|3|7] <key>** | **null** } **authentication** { **sha1 [0|3|7] <key>** | **null** }

To disable the encryption of OSPFv3 packets, use the **no** form of this command.

no encryption ipsec spi <*spi_val*> **esp** { **3des [0|3|7] <key>** | **aes 128 [0|3|7] <key>** | **null** } **authentication** { **sha1 [0|3|7] <key>** | **null** }

Syntax Description

Syntax	Description
spi	Specifies security policy index.
spi val	Value of **spi**. It ranges from 256 to 4294967295.
esp	Encryption algorithm. Its value can be 3des / aes / null.
authentication	Authentication algorithm. Its value can be sha1 / null.
0	Specifies an unencrypted password.
3	Specifies 3DES unencrypted password.
7	Specifies Cisco Type 7 encrypted password.
WORD	Specifies unencrypted (cleartext) password.

Note You cannot configure both *esp* and *auth* algorithms as null in one esp CLI.

Command Default

The OSPFv3 packets are not encrypted by default.

Command History

Release	Modification
8.4.4	This command was introduced.

ospfv3 esp at area level

To enable encryption of OSPFv3 packets on a per interface basis at area level, use below commands.

area *area_id* **encryption** {**disable** | **ipsec** **spi** *spi_val* **esp** { **3des** **[0 | 3 | 7]** *key* | **aes** **128** **[0 | 3 | 7]** *key* | **null** } **authentication** { **sha1** **[0 | 3 | 7]** *key* | **null** } }

To disable the encryption of OSPFv3 packets, use the **no** form of this command.

no area *area_id* **encryption** { **disable** | **ipsec** **spi** *spi_val* **esp** { **3des** **[0 | 3 | 7]** *key* | **aes** **128** **[0 | 3 | 7]** *key* | **null** } **authentication** { **sha1** **[0 | 3 | 7]** *key* | **null** } }

Syntax Description

Syntax	Description
area_id	Specifies area to which esp to be configured.
spi	Specifies security policy index.
disable	Disable encryption for the area.
spi_val	Value of **spi**. It ranges from 256 to 4294967295.
esp	Encryption algorithm. Its value can be 3des / aes / null.
authentication	Specifies authentication algorithm. Its value can be sha1 / null
0	Specifies an unencrypted password.
3	Specifies 3DES unencrypted password.
7	Specifies that the password is cisco type 7 encrypted password.
WORD	Specifies unencrypted (cleartext) password.

Command Default

The OSPFv3 packets are not encrypted by default.

Command History

Release	Modification
8.4.4	This command was introduced.

ospfv3 encryption at interface level

To enable encryption of OSPFv3 packets at interface level, use below commands.

ospfv3 encryption { **disable** | **ipsec spi** *spi_val* **esp** { **3des [0 | 3 | 7]** *key* | **aes 128 [0 | 3 | 7]** *key* | **null** } **authentication** { **sha1 [0 | 3 | 7]** *key* | **null** } }

Use below command to disable encryption of OSPFv3 packets at interface level.

no ospfv3 encryption { **disable** | **ipsec spi** *spi_val* **esp** { **3des [0 | 3 | 7]** *key* | **aes 128 [0 | 3 | 7]** *key* | **null** } **authentication** { **sha1 [0 | 3 | 7]** *key* | **null** } }

Syntax Description

Syntax	Description
spi	Specifies security policy index.
disable	Disables encryption for the Interface.
spi_val	Value of **spi**. It ranges from 256 to 4294967295.
esp	Encryption algorithm. Its value can be 3des / aes / null.
authentication	Authentication algorithm. Its value can be 3des/ sha1 / null.
0	Specifies an unencrypted password.
3	Specifies 3DES unencrypted password.
7	Specifies that the password is cisco type 7 encrypted password.
WORD	Specifies unencrypted (cleartext) password.

Note You cannot configure both *esp* and *auth* algorithms as null in one esp CLI.

Table 1: Password Length

Password	Description

AES 128	`0 - 32 HEX CHAR`
	`3 - 64 HEX CHAR`
	`7 - 66 HEX CHAR`
	`WORD- 32 HEX CHAR`

Password	Description
3DES	0 - 48 HEX CHAR 3 - 96 HEX CHAR 7 - 98 HEX CHAR WORD- 48 HEX CHAR
SHA1	0 - 40 HEX CHAR 3 - 80 HEX CHAR 7 - 82 HEX CHAR WORD- 40 HEX CHAR

Command Default

The OSPFv3 packets are not encrypted by default.

Command History

Release	Modification
8.4.4	This command was introduced.

Usage Guidelines

Before running this command, ensure that you configure **feature imp** and **feature ospfv3** commands.

Examples

The following example shows how to encrypt OSPFv3 packets at the ethernet interface 3/2:

```
switch (config)# feature ospfv3
switch (config)# feature imp
switch(config)# interface Ethernet3/2
switch(config-if)# ipv6 router ospfv3 1 area 0
switch(config-if)# ospfv3 encryption ipsec spi 40040 esp aes 128 0
123456789A123456789B123456789C12 authentication sha1 0
0DA293FA8B0BBC1AA4CC425FDB6784A723456789
switch (config-if)# sh running-config interface Ethernet3/2

Command: show running-config interface Ethernet3/2
Running configuration last done at: Mon Feb  1 05:39:38 2021
Time: Mon Feb  1 05:42:11 2021
version 8.4(4)
interface Ethernet3/2
 ospfv3 encryption ipsec spi 40040 esp aes 128 3
762bc328e3bdf235a526a5c4787faed5b590430ca971a52f60d848eb18a115b1 authentication sha1 3
1626937cb7784c9055f0b4c791721d1149c4d1c29b15a62365baee4f8997b69e62787a37d4c0b374
 ipv6 address 100:300:1:1::2/64
 ipv6 router ospfv3 1 area 0.0.0.0
 no shutdown
```

ospfv3 esp at virtual link level

To enable encryption of OSPFv3 packets on virtual link level using the following commands.

encryption ipsec spi *spi_val* **esp** { **3des [0 | 3 | 7]** *key* | **aes** { **128 [0 | 3 | 7]** *key* | **null** } **authentication** { **sha1 [0 | 3 | 7]** *key* | **null** } }

To disable the encryption of OSPFv3 packets, use the **no** form of this command.

no encryption ipsec spi *spi_val* **esp** { **3des [0 | 3 | 7]** *key* | **aes** { **128 [0 | 3 | 7]** *key* | **null** } **authentication** { **sha1 [0 | 3 | 7]** *key* | **null** } }

Syntax Description

Syntax	Description
spi	Specifies security policy index.
spi_val	Value of **spi**. It ranges from 256 to 4294967295.
esp	Encryption algorithm. Its value can be 3des / aes / null.
authentication	Authentication algorithm. Its value can be sha1 / null.
0	Specifies an unencrypted password.
3	Specifies 3DES unencrypted password.
7	Specifies that the password is cisco type 7 encrypted password.
WORD	Specifies unencrypted (cleartext) password.

Note You cannot configure both *esp* and *auth* algorithms as null in one esp CLI.

Command Default

The OSPFv3 packets are not encrypted by default.

Command History

Release	Modification
8.4.4	This command was introduced.

Usage Guidelines

Before running this command, ensure that you configure **feature imp** and **feature ospfv3** commands.

Examples

The following example shows how to encrypt OSPFv3 packets for virtual links:

```
switch (config)# feature ospfv3
switch (config)# feature imp
switch (config)# router ospfv3 1
switch (config-router)# area 0.0.0.1 virtual-link 44.40.1.1
switch (config-router-vlink)# encryption ipsec spi 10010 esp aes 128 3
2810136407eb188a4645b57f18df3b4f72fa9eab7eb1294770aa2ff708298064 authentication sha1
```

```
FEF91D1D46E01005CBE8F3A8FCDF14F534567890
switch (config-router-vlink)# exit
```

ospfv3 cost

To specify the cost of sending a packet on an interface, use the **ospfv3 cost** command. To reset the path cost to the default, use the **no** form of this command.

ospfv3 cost *interface-cost*
no ospfv3 cost *interface-cost*

Syntax Description

interface-cost	Unsigned integer value expressed as the link-state metric. The range is from 1 to 65535.

Command Default

Calculates the cost based on the reference bandwidth divided by the configured interface bandwidth. You can configure the reference bandwidth or it defaults to 40 Gb/s.

Command Modes

Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ospfv3 cost** command to configure the cost metric manually for each interface. This command overrides any settings for the reference bandwidth that you set using the auto-cost command in router configuration mode.

If this command is not used, the link cost is calculated using the following formula:

link cost = reference bandwidth / interface bandwidth

This command requires the Enterprise Services license.

Examples

This example shows how to configure the interface cost value to 65:

```
switch(config)# interface ethernet 1/2
switch(config-if)#ospfv3 cost 65
```

Related Commands

Command	Description
auto-cost (OSPFv3)	Specifies the reference bandwidth that OSPFv3 uses to calculate the link cost.

ospfv3 dead-interval

To set the interval during which at least one hello packet must be received from a neighbor before the router declares that neighbor as down, use the **ospfv3 dead-interval** command. To restore the default, use the **no** form of this command.

ospfv3 dead-interval *seconds*
no ospfv3 dead-interval

Syntax Description

seconds	Interval (in seconds) during which the router must receive at least one hello packet from a neighbor or that neighbor adjacency is removed from the local router and does not participate in routing. The range is from 1 to 65535. The value must be the same for all nodes on the network.

Command Default

The default for *seconds* is four times the interval set by the **ospfv3 hello-interval** command.

Command Modes

Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ospfv3 dead-interval** command to set the dead interval that OSPFv3 advertises in hello packets. This value must be the same for all networking devices on a specific network.

Configure a shorter dead interval to detect down neighbors faster and improve convergence. Very short dead intervals could cause routing instability.

Use the **show ospfv3 interface** command to verify the dead interval and hello interval.

This command requires the Enterprise Services license.

Examples

This example shows how to set the OSPFv3 dead interval to 20 seconds:

```
switch(config)# interface ethernet 1/2
switch(config-if)#ospfv3 dead-interval 20
```

Related Commands

Command	Description
ospfv3 hello-interval	Interval between hello packets that OSPFv3 sends on the interface.
show ospfv3 interface	Displays OSPFv3-related information.

ospfv3 hello-interval

To specify the interval between hello packets that Open Shortest Path First version 3 (OSPFv3) sends on the interface, use the **ospfv3 hello-interval** command. To return to the default, use the **no** form of this command.

ospfv3 hello-interval *seconds*
no ospfv3 hello-interval

Syntax Description

seconds	Specifies the interval (in seconds). The value must be the same for all nodes on a specific network. The range is from 1 to 65535.

Command Default

10 seconds

Command Modes

Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ospfv3 hello-interva**l command to set the rate at which OSPFv3 advertises hello packets. Shorter hello intervals allow OSPFv3 to detect topological changes faster. This value must be the same for all routers and access servers on a specific network.

This command requires the Enterprise Services license.

Examples

This example shows how to set the interval between hello packets to 15 seconds:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ospfv3 hello-interval 15
```

Related Commands

Command	Description
ospfv3 dead-interval	Sets the time period for which hello packets must not have been seen before neighbors declare the router as down.

ospfv3 mtu-ignore

To disable Open Shortest Path First version 3 (OSPFv3) maximum transmission unit (MTU) mismatch detection on received Database Descriptor (DBD) packets, use the **ospfv3 mtu-ignore** command. To return to the default, use the **no** form of this command.

ospfv3 mtu-ignore
no ospfv3 mtu-ignore

Syntax Description

This command has no arguments or keywords.

Command Default

OSPFv3 MTU mismatch detection is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ospfv3 mtu-ignore** command to disable MTU mismatch detection on an interface. By default, OSPFv3 checks whether neighbors are using the same MTU on a common interface. If the receiving MTU is higher than the IP MTU configured on the incoming interface, OSPFv3 does not establish adjacencies. Use the **ospfv3 mtu-ignore** command to disable this check and allow adjacencies when the MTU value differs between OSPFv3 neighbors.

This command requires the Enterprise Services license.

Examples

This example shows how to disable MTU mismatch detection on received DBD packets:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ospfv3 mtu-ignore
```

ospfv3 network

To configure the Open Shortest Path First version 3 (OSPFv3) network type to a type other than the default for an interface, use the **ospfv3 network** command. To return to the default, use the **no** form of this command.

ospfv3 network {**broadcast** | **point-to-point**}
no ospfv3 network

Syntax Description

broadcast	Sets the network type as broadcast.
point-to-point	Sets the network type as point-to-point.

Command Default

Depends on the network type.

Command Modes

Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The network type influences the behavior of the OSPF interface. OSPF network type is usually broadcast, which uses OSPF multicasting capabilities. Under this network type a designated router and backup designated router are elected. For point-to-point networks there are only two neighbors and multicast is not required. For routers on an interface to become neighbors the network type for all should match.

This command requires the Enterprise Services license.

Examples

This example shows how to set an OSPFv3 network as a broadcast network:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ipv6 address 2001:0DB8::1/8
switch(config-if)# ospfv3 network broadcast
```

ospfv3 passive-interface

To suppress Open Shortest Path First version 3 (OSPFv3) routing updates on an interface, use the **ospfv3 passive-interface** command. To return to the default, use the **no** form of this command.

ospfv3 passive-interface
no ospfv3 passive-interface

Syntax Description

This command has no keywords or arguments.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

If an interface is configured as passive-interface it does not participate in the OSPF protocol and will not establish adjacencies or send routing updates. However the interface is announced as part of the routing network.

This command requires the Enterprise Services license.

Examples

This example shows how to set an interface as passive:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ospfv3 passive-interface
```

ospfv3 priority

To set the router priority for an Open Shortest Path First version 3 (osPFv3) interface, use the **ospfv3 priority** command. To return to the default, use the **no** form of this command.

ospfv3 priority *number-value*
no ospfv3 priority *number-value*

Syntax Description

number-value	Number value that specifies the priority of the router. The range is from 0 to 255.

Command Default

Priority of 1

Command Modes

Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ospfv3 priority** command to set the router priority, which determines the designated router for this network. When two routers are attached to a network, both attempt to become the designated router. The router with the higher router priority takes precedence. If there is a tie, the router with the higher router ID takes precedence. A router with a router priority set to zero cannot become the designated router or backup designated router.

This command requires the Enterprise Services license.

Examples

This example shows how to set the router priority value to 4:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ospfv3 priority 4
```

Related Commands

Command	Description
ospfv3 network	Configures the OSPFv3 network type to a type other than the default for a given medium.

ospfv3 retransmit-interval

To specify the time between Open Shortest Path First version 3 (OSPFv3) link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface, use the **ospfv3 retransmit-interval** command. To return to the default, use the **no** form of this command.

ospfv3 retransmit-interval *seconds*
no ospfv3 retransmit-interval

Syntax Description

seconds	Time (in seconds) between retransmissions. The time must be greater than the expected round-trip delay between any two routers on the attached network. The range is from 1 to 65535 seconds. The default is 5 seconds.

Command Default

5 seconds

Command Modes

Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ospfv3 retransmit-interval** command to set the time between LSA retransmissions. When a router sends an LSA to its neighbor, it keeps the LSA until it receives an acknowledgment message from the neighbor. If the router receives no acknowledgment within the retransmit interval, the local router resends the LSA.

This command requires the Enterprise Services license.

Examples

This example shows how to set the retransmit interval value to 8 seconds:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ospfv3 retransmit-interval 8
```

ospfv3 shutdown

To shut down an Open Shortest Path First version 3 (osPFv3) interface, use the **ospfv3 shutdown** command. To return to the default, use the **no** form of this command.

ospfv3 shutdown
no ospfv3 shutdown

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ospfv3 shutdown** command to shut down OSPFv3 on this interface.

This command requires the Enterprise Services license.

Examples

This example shows how to shut down OSPFv3 on an interface:

```
switch(config)# interface ethernet 1/2
switch(config-if)#ospfv3 shutdown
```

ospfv3 transmit-delay

To set the estimated time required to send an Open Shortest Path First version 3 (OSPFv3) link-state update packet on the interface, use the **ospfv3 transmit-delay** command. To return to the default, use the **no** form of this command.

ospfv3 transmit-delay *seconds*
no ospfv3 transmit-delay

Syntax Description

seconds	Time (in seconds) required to send a link-state update. The range is from 1 to 450 seconds.

Command Default

1 second

Command Modes

Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ospfv3 transmit-delay** command to set the estimated time needed to send an LSA update packet. OSPFv3 increments the LSA age time by transmit delay amount before transmitting the LSA update. You should take into account the transmission and propagation delays for the interface when you set this value.

This command requires the Enterprise Services license.

Examples

This example shows how to set the transmit delay value to 8 seconds:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ospfv3 transmit-delay 8
```