IPv6 Commands: n to re

nai (proxy mobile IPv6)

To configure the Network Access Identifier (NAI) for the mobile node (MN) within the PMIPV6 domain, use the **nai** command in PMIPV6 domain configuration mode. To disable the NAI configuration, use the **no** form of this command.

nai [*user*] ***@realm***
no nai [*user*] ***@realm***

Syntax Description

user@realm	Fully qualified specific user address and realm. The @ symbol is required.
@realm	Any user address at a specific realm. The @ symbol is required.

Command Default

NAI for the MN is not specified.

Command Modes

PMIPV6 domain configuration (config-ipv6-pmipv6-domain)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.

Examples

The following example shows how to configure the NAI within the PMIPV6 domain:

```
Device(config)# ipv6 mobile pmipv6-domain dn1
Device(config-ipv6-pmipv6-domain)# nai example@example.com
Device(config-ipv6-pmipv6-domain-mn)#
```

Related Commands

Command	Description
ipv6 mobile pmipv6-domain	Configures the PMIPV6 domain.

neighbor override-capability-neg

To enable the IPv6 address family for a Border Gateway Protocol (BGP) neighbor that does not support capability negotiation, use the **neighbor override-capability-neg**command in address family configuration mode. To disable the IPv6 address family for a BGP neighbor that does not support capability negotiation, use the **no** form of this command.

neighbor {*peer-group-nameipv6-address*} **override-capability-neg**
no neighbor {*peer-group-nameipv6-address*} **override-capability-neg**

Syntax Description

peer-group-name	Name of a BGP peer group.
ipv6-address	IPv6 address of the BGP neighbor. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

Command Default

Capability negotiation is enabled.

Command Modes

Address family configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Capability negotiation is used to establish a connection between BGP-speaking peers. If one of the BGP peers does not support capability negotiation, the connection is automatically terminated. The **neighbor override-capability-neg**command overrides the capability negotiation process and enables BGP-speaking peers to establish a connection.

The **neighbor override-capability-neg**command is supported only in address family configuration mode for the IPv6 address family.

Examples

The following example enables the IPv6 address family for BGP neighbor 7000::2:

```
Router(config)# address-family ipv6
Router(config-router-af)# neighbor 7000::2 override-capability-neg
```

The following example enables the IPv6 address family for all neighbors in the BGP peer group named group1:

```
Router(config)# address-family ipv6
Router(config-router-af)# neighbor group1 override-capability-neg
```

Related Commands

Command	Description
address-family ipv6	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv6 address prefixes.

neighbor send-label

To enable a Border Gateway Protocol (BGP) router to send Multiprotocol Label Switching (MPLS) labels with BGP routes to a neighboring BGP router, use the **neighbor send-label** command in address family configuration mode or router configuration mode. To disable this feature, use the **no** form of this command.

neighbor {*ip-addressipv6-addresspeer-group-name*} **send-label** [**explicit-null**]
no neighbor {*ip-addressipv6-addresspeer-group-name*} **send-label** [**explicit-null**]

Syntax Description

ip-address	IP address of the neighboring router.
ipv6-address	IPv6 address of the neighboring router.
peer-group-name	Name of a BGP peer group.
send-label	Sends Network Layer Reachability Information (NLRI) and MPLS labels to this peer.
explicit-null	(Optional) Advertises the Explicit Null label.

Command Default

BGP routers distribute only BGP routes.

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
12.0(21)ST	This command was introduced.
12.0(22)S	This command was modified. The *ipv6-address* argument was added.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.1(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.
15.2(2)SNI	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

The **neighbor send-label** command enables a router to use BGP to distribute MPLS labels along with IPv4 routes to a peer router. You must issue this command on both the local and the neighboring router.

This command has the following restrictions:

- If a BGP session is running when you issue the **neighbor send-label** command, the BGP session flaps immediately after the command is issued.
- In router configuration mode, only IPv4 addresses are distributed.

Use the **neighbor send-label** command in address family configuration mode, to bind and advertise IPv6 prefix MPLS labels. Using this command in conjunction with the **mpls ipv6 source-interface** global configuration command allows IPv6 traffic to run over an IPv4 MPLS network without any software or hardware configuration changes in the backbone. Edge routers configured to run both IPv4 and IPv6 traffic forward IPv6 traffic using MPLS and multiprotocol internal BGP (MP-iBGP).

Cisco IOS software installs /32 routes for directly connected external BGP (eBGP) peers when the BGP session for such a peer comes up. The /32 routes are installed only when MPLS labels are exchanged between such peers. Directly connected eBGP peers exchange MPLS labels for:

- IP address families (IPv4 and IPv6) with the **neighbor send-label** command enabled for the peers
- VPN address families (VPNv4 and VPNv6)

A single BGP session can include multiple address families. If one of the families exchanges MPLS labels, the /32 neighbor route is installed for the connected peer.

Examples

The following example shows how to enable a router in autonomous system 65000 to send MPLS labels with BGP routes to the neighboring BGP router at 192.168.0.1:

```
Router(config)# router bgp 65000
Router(config-router)# neighbor 192.168.0.1 remote-as 65001
Router(config-router)# neighbor 192.168.0.1 send-label
```

The following example shows how to enable a router in the autonomous system 65000 to bind and advertise IPv6 prefix MPLS labels and send the labels with BGP routes to the neighboring BGP router at 192.168.99.70:

```
Router(config)# router bgp 65000
Router(config-router)# neighbor 192.168.99.70 remote-as 65000
Router(config-router)# address-family ipv6
Router(config-router-af)# neighbor 192.168.99.70 activate
Router(config-router-af)# neighbor 192.168.99.70 send-label
```

Related Commands

Command	Description
address-family ipv6	Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
neighbor activate	Enables the exchange of information with a neighboring router.
neighbor remote-as	Adds an entry to the BGP or multiprotocol BGP neighbor table.
mpls ipv6 source-interface	Specifies an IPv6 address of an interface to be used as the source address for locally generated IPv6 packets to be sent over an MPLS network.

neighbor translate-update

To enable customer-edge (CE) devices, which are not capable of multicast BGP (mBGP) routing, to participate in a multicast session, use the **neighbor translate-update** command in address-family configuration mode. To disable mBGP routing on CE devices, use the **no** form of the command.

neighbor {*ipv4-address ipv6-address*} **translate-update multicast** [**unicast**]
no neighbor {*ipv4-address ipv6-address*} **translate-update multicast** [**unicast**]

Syntax Description

ipv4-address	Specifies the multicast IPv4 address for the BGP neighbor.
ipv6-address	Specifies the multicast IPv6 address for the BGP neighbor.
multicast	Specifies multicast address prefixes.
unicast	(Optional) Specifies unicast address prefixes.

Command Modes

Address family configuration (config-router-af)

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.4(1)S	This command was modified. Support for translate-update was extended to VRF address-families.
Cisco IOS XE Release 3.11S	This command was modified. Support for translate-update was extended to VRF address-families.

Usage Guidelines

The **translate-update** keyword in the neighbor command enables CE devices, which cannot send BGP Reverse Path Forwarding (RPF) multicast routes, to advertise its routes to multicast VRF-Lite and multicast VPN (mVPN) for VPNv4 and VPNv6 neighbors. These routes are also advertised through IPv6 over IPv4 tunnel. The **translate-update** keyword is configured on the provider-edge (PE) devices for multicast routing to neighbor CE devices using the **address-family ipv4 vrf** or the **address-family ipv6 vrf** command. The PE devices translate the updates from unicast to multicast on CE devices and put them in the BGP VRF routing table of the PE devices, as multicast updates, for processing. If the optional keyword **unicast** is also configured, the updates that are not translated to multicast are also placed in the unicast queue of the PE devices and

populate the unicast BGP VRF table. The translation from unicast to multicast occurs from CE devices to PE devices only. Prefixes are only advertised from CE devices to the multicast neighbors of the PE devices.

Prior to configuring the translate-update feature, you must enable multicast VRF on the PE devices, along with an active VRF session with the CE devices.

Examples

The following example shows how to configure the translate-update feature for an IPv4 VRF address-family named v1 and BGP neighbor n2:

Note Peer-template configuration for BGP neighbor is not supported for this feature due to conflicts with the earlier versions of Cisco software.

```
Device> enable
Device# configure terminal
Device(config)# router bgp 65000
Device(config-router)# address-family ipv4 vrf v1
Device(config-router-af)# neighbor n2 peer-group
Device(config-router-af)# neighbor n2 remote-as 4
Device(config-router-af)# neighbor 10.1.1.1 peer-group n2
Device(config-router-af)# neighbor 10.1.1.1 activate
Device(config-router-af)# neighbor 10.1.1.1 translate-update multicast unicast
Device(config-router-af)# end
```

The following is sample output from the **show bgp vpnv4 multicast vrf** command. If the "State/PfxRcd" field displays "NoNeg", it indicates that the neighbor has a translate-update session:

```
Device# show bgp vpnv4 multicast vrf v1 summary

BGP router identifier 10.1.3.1, local AS number 65000
BGP table version is 8, main routing table version 8
7 network entries using 1792 bytes of memory
8 path entries using 960 bytes of memory
5/3 BGP path/bestpath attribute entries using 1280 bytes of memory
3 BGP AS-PATH entries using 88 bytes of memory
2 BGP extended community entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 4168 total bytes of memory
BGP activity 23/2 prefixes, 33/9 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.1.1.1        4            4       5      10        1    0    0 00:01:10 (NoNeg)

10.1.3.2        4            2      12      10        8    0    0 00:01:33
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family ipv6	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv6 address prefixes.

Command	Description
neighbor peer-group	Creates a BGP or multiprotocol BGP peer group.
neighbor remote-as	Adds an entry to a BGP or multiprotocol BGP neighbor table.
neighbor activate	Enables exchange of information with a BGP neighbor.
show bgp vpnv4 multicast	Displays Virtual Private Network Version 4 (VPNv4) multicast entries in a BGP table.

network (IPv6)

To configure the network source of the next hop to be used by the PE VPN, use the network command in router configuration mode. To disable the source, use the **no** form of this command.

network *ipv6-address/prefix-length*
no network *ipv6-address/prefix-length*

Syntax Description

ipv6-address	The IPv6 address to be used.
/ *prefix-length*	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Command Default

Next-hop network sources are not configured.

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The *ipv6-address* argument in this command configures the IPv6 network number.

Examples

The following example places the router in address family configuration mode and configures the network source to be used as the next hop:

```
Router(config)# router bgp 100
Router(config-router)# network 2001:DB8:100::1/128
```

Related Commands

Command	Description
address-family ipv6	Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
address-family vpnv6	Places the router in address family configuration mode for configuring routing sessions that use standard VPNv6 address prefixes.

nis address

To specify the network information service (NIS) address of an IPv6 server to be sent to the client, use the **nis address** command in DHCP for IPv6 pool configuration mode. To remove the NIS address, use the **no** form of this command.

nis address *ipv6-address*
no nis address *ipv6-address*

Syntax Description

ipv6-address	The NIS address of an IPv6 server to be sent to the client.

Command Default

No NIS address is specified.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

The Dynamic Host Configuration Protocol (DHCP) for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS server option provides a list of one or more IPv6 addresses of NIS servers available to send to the client. The client must view the list of NIS servers as an ordered list, and the server may list the NIS servers in the order of the server's preference.

The NIS server option code is 27. For more information on DHCP options and suboptions, see the "DHCPv6 Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to specify the NIS address of an IPv6 server:

```
nis address 23::1
```

Related Commands

Command	Description
import nis address	Imports the NIS server option to a DHCP for IPv6 client.
nis domain-name	Enables a server to convey a client's NIS domain name information to the client.

nis domain-name

To enable a server to convey a client's network information service (NIS) domain name information to the client, use the **nis domain-name**command in DHCP for IPv6 pool configuration mode. To remove the domain name, use the **no** form of this command.

nis domain-name *domain-name*
no nis domain-name *domain-name*

Syntax Description

domain-name	The domain name of an IPv6 server to be sent to the client.

Command Default

No NIS domain name is specified.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

The Dynamic Host Configuration Protocol (DHCP) for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS domain name option provides a NIS domain name for the client. Use the **nis domain-name** command to specify the client's NIS domain name that the server sends to the client.

The NIS domain name option code is 29. For more information on DHCP options and suboptions, see the "DHCPv6 Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to enable the IPv6 server to specify the NIS domain name of a client:

```
nis domain-name cisco1.com
```

Related Commands

Command	Description
import nis domain	Imports the NIS domain name option to a DHCP for IPv6 client.
nis address	Specifies the NIS address of an IPv6 server to be sent to the client.

nisp address

To specify the network information service plus (NIS+) address of an IPv6 server to be sent to the client, use the **nisp address** command in DHCP for IPv6 pool configuration mode. To remove the NIS+ address, use the **no** form of the command.

nisp address *ipv6-address*
no nisp address *ipv6-address*

Syntax Description

ipv6-address	The NIS+ address of an IPv6 server to be sent to the client.

Command Default

No NIS+ address is specified.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

The Dynamic Host Configuration Protocol (DHCP) for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS+ servers option provides a list of one or more IPv6 addresses of NIS+ servers available to send to the client. The client must view the list of NIS+ servers as an ordered list, and the server may list the NIS+ servers in the order of the server’s preference.

The NIS+ servers option code is 28. For more information on DHCP options and suboptions, see the "DHCPv6 Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to specify the NIS+ address of an IPv6 server:

```
nisp address 33::1
```

Related Commands

Command	Description
import nisp address	Imports the NIS+ servers option to a DHCP for IPv6 client.
nisp domain-name	Enables a server to convey a client’s NIS+ domain name information to the client.

nisp domain-name

To enable an IPv6 server to convey a client's network information service plus (NIS+) domain name information to the client, use the **nisp domain-name**command in DHCP for IPv6 pool configuration mode. To remove the domain name, use the **no** form of this command.

nisp domain-name *domain-name*
no nisp domain-name *domain-name*

Syntax Description

domain-name	The NIS+ domain name of an IPv6 server to be sent to the client.

Command Default

No NIS+ domain name is specified.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

The Dynamic Host Configuration Protocol (DHCP) for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS+ domain name option provides a NIS+ domain name for the client. Use the **nisp domain-name** command to enable a server to send the client its NIS+ domain name information.

The NIS+ domain name option code is 30. For more information on DHCP options and suboptions, see the "DHCPv6 Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to enable the IPv6 server to specify the NIS+ domain name of a client:

```
nisp domain-name cisco1.com
```

Related Commands

Command	Description
import nisp domain	Imports the NIS+ domain name option to a DHCP for IPv6 client.
nisp address	Specifies the NIS+ address of an IPv6 server to be sent to the client.

ospfv3 area

To enable Open Shortest Path First version 3 (OSPFv3) on an interface with the IPv4 or IPv6 address family (AF), use the **ospfv3 area** command in interface configuration mode. To disable OSPFv3 routing for interfaces defined, use the **no** form of this command.

ospfv3 *process-id* {**ipv4** | **ipv6**} **area** *area-ID* [**instance** *instance-id*]
no ospfv3 *process-id* {**ipv4** | **ipv6**} **area** *area-ID*

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
ipv4	IPv4 address family.
ipv6	IPv6 address family.
area-id	Area that is to be associated with the OSPFv3 interface.
instance *instance-id*	(Optional) Instance identifier. • When the **ipv4** keyword is used, the *instance-id* argument can be a value from 64 through 95. The default is 64. • When the **ipv6** keyword is used, the *instance-id* argument can be a value from 0 through 31. The default is 0.

Command Default

OSPFv3 is not enabled on the interface. The default instance ID for IPv4 is 64. The default instance ID for IPv6 is 0.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **ospfv3 area**command to enable OSPFv3 on an interface. This command enables you to configure two OSPFv3 instances on an interface-one IPv6 AF instance, and one IPv4 AF instance. You can configure only one process for each AF per interface.

Before you enable OSPFv3 on an interface using the **ospfv3 area** command, you must enable IPv6 on the interface, and you must enable IPv6 routing.

When the **ospfv3 area**command is configured for the IPv6 AF, it overwrites the **ipv6 ospf area** configuration if OSPFv3 was attached to the interface using the ipv6 ospf area command.

Examples

The following example enables OSPFv3 for the IPv4 AF on an interface:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 1 area 1 ipv4
```

ospfv3 authentication

To specify the authentication type for an Open Shortest Path First version 3 (OSPFv3) instance, use the **ospfv3 authentication**command in interface configuration mode. To remove this instance, use the **no** form of this command.

{**ospfv3 authentication ipsec** *spi* {**md5** | **sha1**} *key-encryption-type key* | **null**}
{**no ospfv3 authentication ipsec** *spi* {**md5** | **sha1**} *key-encryption-type key* | **null**}

Syntax Description

ipsec	Configures use of IP Security (IPsec) authentication.
spi *spi*	Security policy index (SPI) value. The *spi* value must be a number from 256 to 4294967295.
md5	Enables message digest 5 (MD5) authentication.
sha1	Enables Secure Hash Algorithm 1 (SHA-1) authentication.
key-encryption-type	One of the following values can be entered: • **0** --The key is not encrypted. • **7** --The key is encrypted.
key	Number used in the calculation of the message digest. • When MD5 authentication is used, the key must be 32 hex digits (16 bytes) long. • When SHA-1 authentication is used, the key must be 40 hex digits (20 bytes) long.
null	Used to override area authentication.

Command Default

No authentication is specified.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **ospfv3 authentication** command to specify the OSPFv3 authentication type on an interface. The **ospfv3 authentication** command cannot be configured per process. If the **ospfv3 authentication** command is used, it affects all OSPFv3 instances.

The user needs to ensure that the same policy (the SPI and the key) is configured on all of the interfaces on the link. SPI values may automatically be used by other client applications, such as tunnels.

The policy database is common to all client applications on a box. This means that two IPsec clients, such as OSPFv3 and a tunnel, cannot use the same SPI. Additionally, an SPI can be used only in one policy.

The **null** keyword is used to override existing area authentication. If area authentication is not configured, then it is not necessary to configure the interface with the **authentication null**command.

Examples

The following example specifies the authentication type for an OSPFv3 instance:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 authentication md5 0 275761340947681324733020312097 27
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 bfd

To enable Bidirectional Forwarding Detection (BFD) on an Open Shortest Path First version 3 (OSPFv3) interface, use the **ospfv3 bfd** command in interface configuration mode. To remove this instance, use the **no** form of this command.

ospfv3 [*process-id*] **bfd** [**disable**]
no ospfv3 [*process-id*] **bfd**

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
disable	(Optional) Disables BFD on the specified interface.

Command Default

BFD support for OSPFv3 is not enabled on the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **ospfv3 bfd** command to enable BFD on an interface. When the **ospfv3 bfd** command is entered with a process ID, it applies to that specific process only. This configuration takes precedence if the **ospfv3 bfd** command is enabled with no specified process ID.

If you have used the **bfd all-interfaces** command in router configuration mode to globally configure all OSPFv3 interfaces for an OSPFv3 process to use BFD, you can enter the **bfd** command in interface configuration mode with the **disable** keyword to disable BFD for a specific OSPFv3 interface.

Examples

The following example enables BFD on OSPFv3:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 bfd
```

Related Commands

Command	Description
bfd all-interfaces	Enables BFD for all interfaces for a BFD peer.
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 cost

To explicitly specify the cost of sending a packet on an Open Shortest Path First version 3 (OSPFv3) interface, use the ospfv3 **cost** command in interface configuration mode. To reset the interface cost to the default value, use the **no** form of this command.

ospfv3 [*process-id*] **cost** {*interface-cost* | **dynamic** [**default** *default-link-metric*] | **hysteresis** [*percent* | **threshold** *threshold-value*] | **weight** {**L2-factor** *percent* | **latency** *percent* | **resources** *percent* | **throughput** *percent*}
no ospfv3 [*process-id*] **cost**

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
interface-cost	Route cost of this interface. It can be a value in the range from 1 to 65535.
dynamic	Default value on VMI interfaces.
default	(Optional) Default link metric value.
default-link-metric	Specifies the default link metric value on this interface. It can be a value in the range from 0 to 65535.
hysteresis	(Optional) Hysteresis value for link-state advertisement (LSA) dampening.
percent	(Optional) The percentage of c
threshold *threshold-value*	(Optional) Cost change threshold at which hysteresis will be implemented. The threshold range is from 0 to 64k, and the default threshold value is 10k.
weight	(Optional) Amount of impact a variable has on the dynamic cost.
L2-factor *percent*	Quality weight of the Layer 2 link expressed as a percentage. The *percent* value can be in the range from 0 to 100. The default value is 100.
latency *percent*	Latency weight of the Layer 2 link, expressed as a percentage. The *percent* value can be in the range from 0 to 100. The default value is 100.
resources *percent*	Resources weight (such as battery life) of the router at the Layer 2 link, expressed as a percentage. The *percent* value can be in the range from 0 to 100. The default value is 100.
throughput *percent*	Throughput weight of the Layer 2 link, expressed as a percentage. The *percent* value can be in the range from 0 to 100. The default value is 100.

Command Default

Default cost is based on the bandwidth. Mobile Ad Hoc Network (MANET) interfaces are set to use dynamic costs. Non-MANET networks are set to use static costs.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **ospfv3 cost**command to specify the cost of sending a packet on an interface. When the **ospfv3 cost**command is configured with the *process-id* argument, it overwrites the **ipv6 ospf cost**configuration if OSPFv3 was attached to the interface using the ipv6 ospf area command. When the **ospfv3 cost**command is configured without the *process-id* argument, it is inherited on all instances running on the interface.

You can set the metric manually using the **ospfv3 cost** command, if you need to change the default. Using the **bandwidth** command changes the link cost as long as the **ospfv3 cost** command is not used. The link-state metric is advertised as the link cost in the router link advertisement.

The dynamic cost metric used for interfaces is computed based on the Layer 2 (L2) feedback to Layer 3 (L3). For a dynamic cost to have the same cost as a default cost, all parameters must equal zero.

Each Layer 2 feedback can contribute a cost in the range of 0 to 65535. To tune down this cost range, use the optional **weight** keyword in conjunction with the **throughput**, **resources**, **latency**, or **L2-factor** keyword. Each of these weights has a default value of 100% and can be configured in the range from 0 to 100. When 0 is configured for a specific weight, that weight does not contribute to the OSPFv3 cost.

Because cost components can change rapidly, you may need to dampen the amount of changes in order to reduce network-wide churn. Use the optional **hysteresis** keyword with the **threshold** *threshold-value* keyword and argument to set a cost change threshold. Any cost change below this threshold is ignored.

If you enable hysteresis without specifying the mode (percent or threshold), the default mode is threshold, and 10k as the default threshold value.

The higher the threshold or the percent value is set, the larger the change in link quality required to change the OSPFv3 route costs.

Mobile Ad Hoc Networks (MANET)

When the network type is set to MANET, the OSPF cost associated with an interface automatically sets to dynamic. All other network types, keep the interface cost, and you must enter the **ospfv3 cost dynamic** command to change the cost to dynamic.

If you do not specify a default dynamic cost with the **ospfv3 cost dynamic default** command, OSPF uses the interface cost until it receives link metric data.

Examples

The following example sets the interface cost value to 65:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 cost 65
```

The following example shows how to configure OSPFv3 instance 4 to use 30 as the default cost until link metric data arrives from dynamic costing:

```
Router(config)# interface ethernet 0/0
```

```
Router(config-if)# ospfv3 4 cost dynamic default 30
Router(config-if)# exit
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 database-filter

To filter outgoing link-state advertisements (LSAs) to an Open Shortest Path First version 3 (OSPFv3) interface, use the **database-filter**command in interface configuration mode. To restore the forwarding of LSAs to the interface, use the **no** form of this command.

ospfv3 [*process-id*] **database-filter** [{**all** | **disable**}]
no ospfv3 database-filter

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
all	(Optional) Filters all LSAs on the OSPFv3 interface.
disable	(Optional) Disables the LSA filter on the OSPFv3 interface.

Command Default

All outgoing LSAs are flooded to the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **ospfv3 database-filter**command to filter outgoing LSAs to an OSPFv3 interface. When the **ospfv3 database-filter**command is configured with the *process-id* argument, it overwrites the **ipv6 ospf database-filter** configuration if OSPFv3 was attached to the interface using the ipv6 ospf area command. When the **ospfv3 database-filter** command is configured without the *process-id* argument, it is inherited on all instances running on the interface.

Examples

The following example prevents flooding of OSPFv3 LSAs to networks reachable through Ethernet interface 0/0:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 database-filter
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 dead-interval

To set the time period for which hello packets must not be seen before neighbors declare the router down, use the ospfv3 **dead-interval**command in interface configuration mode. To return to the default time, use the **no** form of this command.

ospfv3 [*process-id*] **dead-interval** *seconds*
no ospfv3 [*process-id*] **dead-interval** *seconds*

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
seconds	Specifies the interval (in seconds). The value must be the same for all nodes on the network. The value can be from 1 through 65335 seconds.

Command Default

Four times the interval set by the **ospfv3 h ello-interval** command.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **ospfv3 dead-interval**command to set the time period for which hello packets must not be seen before neighbors declare the router down. When the **ospfv3 dead-interval**command is configured with the *process-id* argument, it overwrites the **ipv6 dead-interval**configuration if OSPFv3 was attached to the interface using the ipv6 ospf area command. When the **ospfv3 dead-interval**command is configured without the *process-id* argument, it is inherited on all instances running on the interface.

The interval is advertised in router hello packets. This value must be the same for all routers and access servers on a specific network.

If no hello-interval is specified, the default dead-interval is 120 seconds for Mobile Ad Hoc Networks (MANETs) and 40 seconds for all other network types.

Examples

The following example sets the OSPFv3 dead interval to 60 seconds:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 dead-interval 60
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 demand-circuit

To configure Open Shortest Path First version 3 (OSPFv3) to treat the interface as an OSPFv3 demand circuit, use the ospfv3 **demand-circuit** command in interface configuration mode. To remove the demand circuit designation from the interface, use the **no** form of this command.

ospfv3 [*process-id*] **demand-circuit** [**disable**] [**ignore**]
no ospfv3 demand-circuit

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
disable	(Optional) Disables the demand circuit on the specified OSPFv3 instance.
ignore	(Optional) Ignores requests from other routers to operate the link in demand-circuit mode.

Command Default

The circuit is not a demand circuit.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
Cisco IOS XE Release 3.8S	This command was modified. The **ignore** keyword was added.

Usage Guidelines

Use the **ospfv3 demand-circuit**command to configure OSPFv3 to treat the interface as an OSPFv3 demand circuit. When the **ospfv3 demand-circuit**command is configured with the *process-id* argument, it overwrites the **ipv6 ospf demand-circuit**configuration if OSPFv3 was attached to the interface using the ipv6 ospf area command. When the **ospfv3 demand-circuit**command is configured without the *process-id* argument, it is inherited on all instances running on the interface.

On point-to-point interfaces, only one end of the demand circuit must be configured with the **demand-circuit** command. Periodic hello messages are suppressed and periodic refreshes of link-state advertisements (LSAs) do not flood the demand circuit. This command allows the underlying data link layer to be closed when the topology is stable. In point-to-multipoint topology, only the multipoint end must configured with this command.

Examples

The following example configures an on-demand circuit on Ethernet interface 0/0:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 demand-circuit
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 encryption

To specify the encryption type for an Open Shortest Path First version 3 (OSPFv3) interface, use the **ospfv3 encryption** command in interface configuration mode. To remove the encryption type from an interface, use the **no** form of this command.

ospfv3 encryption {**ipsec spi** *spi* **esp** *encryption-algorithm key-encryption-type key authentication-algorithm key-encryption-type key* | **null**}
no ospfv3 encryption ipsec spi *spi*

Syntax Description

ipsec	Configures use of IP Security (IPsec) authentication.
spi *spi*	Security policy index (SPI) value. The *spi* value must be a number from 256 to 4294967295.
esp	Encapsulating security payload (ESP).
encryption-algorithm	Encryption algorithm to be used with ESP. The values can be any of the following: • **aes-cbc**--Enables AES-CBC encryption. • **3des**--Enables 3DES encryption. • **des**--Enables DES encryption. • **null**--ESP with no encryption.
key-encryption-type	One of two values can be entered: • **0** --The key is not encrypted. • **7** --The key is encrypted.
key	Number used in the calculation of the message digest. • When MD5 authentication is used, the key must be 32 hex digits (16 bytes) long. • When SHA-1 authentication is used, the key must be 40 hex digits (20 bytes) long.
authentication-algorithm	Encryption authentication algorithm to be used. The values can be one of the following: • **md5** --Enables message digest 5 (MD5). • **sha1** --Enables SHA-1.
null	Overrides area encryption.

Command Default

Authentication and encryption are not configured on an interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **ospfv3 encryption**command to specify the encryption type for an interface. The **ospfv3 encryption**command cannot be configured per process. If the **ospfv3 encryption**command is used, it affects all OSPFv3 instances.

The user needs to ensure that the same policy (the SPI and the key) is configured on all of the interfaces on the link. SPI values may automatically be used by other client applications, such as tunnels.

The policy database is common to all client applications on a box. This means that two IPSec clients, such as OSPFv3 and a tunnel, cannot use the same SPI. Additionally, an SPI can be used only in one policy.

The **null** keyword is used to override existing area encryption. If area encryption is not configured, then it is not necessary to configure the interface with the **encryption null**command.

Examples

The following example specifies the encryption type for Ethernet interface 0/0. The IPSec SPI value is 1001, ESP is used with no encryption, and the authentication algorithm is MD5.

```
Router(config)# interface ethernet 0/0
Router(config-if)# ospfv3 encryption ipsec spi 1001 esp null md5 0
 2757613409476813247330203120972 7
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 flood-reduction

To suppress the unnecessary flooding of link-state advertisements (LSAs) in stable topologies, use the **ospfv3 flood-reduction** command in interface configuration mode. To disable this feature, use the **no** form of this command.

ospfv3 [*process-id*] **flood-reduction** [**disable**]
no ospfv3 [*process-id*] **flood-reduction**

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the Open Shortest Path First version 3 (OSPFv3) routing process and can be a value from 1 through 65535.
disable	(Optional) Allows flood reduction to be disabled on the specified OSPFv3 interface.

Command Default

This command is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **ospfv3 flood-reduction**command to suppress unnecessary LSA flooding in stable topologies. When the **ospfv3 flood-reduction**command is configured with the *process-id* argument, it overwrites the **ipv6 ospf flood-reduction**configuration if OSPFv3 was attached to the interface using the ipv6 ospf flood-reduction command. When the **ospfv3 flood-reduction**command is configured without the *process-id* argument, it is inherited on all instances running on the interface.

All routers supporting the OSPFv3 demand circuit are compatible and can interact with routers supporting flooding reduction.

Examples

The following example suppresses the flooding of unnecessary LSAs on Ethernet interface 0/0:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 flood-reduction
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 hello-interval

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

ospfv3 [*process-id*] **hello-interval** *seconds*
no ospfv3 [*process-id*] **hello-interval** *seconds*

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
seconds	Specifies the interval (in seconds). The value must be the same for all nodes on a specific network.

Command Default

The default interval is 10 seconds when using Ethernet and 30 seconds when using nonbroadcast, such as Mobile Ad Hoc Networks (MANETs).

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **ospfv3 hello-interval**command to suppress unnecessary LSA flooding in stable topologies. When the **ospfv3 hello-interval**command is configured with the *process-id* argument, it overwrites the **ipv6 ospf hello-interval**configuration if OSPFv3 was attached to the interface using the ipv6 ospf area command. When the **ospfv3 hello-interval**command is configured without the *process-id* argument, it is inherited on all instances running on the interface.

The **hello-interval** value is advertised in the hello packets. The shorter the hello interval, the earlier topological changes will be detected, but more routing traffic will ensue. This value must be the same for all routers and access servers on a specific network.

Examples

The following example sets the interval between hello packets to 15 seconds:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 hello-interval 15
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 mtu-ignore

To disable Open Shortest Path First version 3 (OSPFv3) maximum transmission unit (MTU) mismatch detection on receiving database descriptor (DBD) packets, use the **ospfv3 mtu-ignore** command in interface configuration mode. To reset to default, use the **no** form of this command.

ospfv3 [*process-id*] **mtu-ignore** [**disable**]
no ospfv3 [*process-id*] **mtu-ignore**

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
disable	(Optional) Allows **mtu-ignore**to be disabled on the specified OSPFv3 interface.

Command Default

OSPFv3 MTU mismatch detection is enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **ospfv3 mtu-ignore**command to disable OSPFv3 MTU mismatch detection on receiving DBD packets. When the **ospfv3 mtu-ignore**command is configured with the *process-id* argument, it overwrites the **ipv6 ospf mtu-ignore**configuration if OSPFv3 was attached to the interface using the ipv6 ospf area command. When the **ospfv3 mtu-ignore**command is configured without the *process-id* argument, it is inherited on all instances running on the interface.

OSPFv3 checks whether neighbors are using the same MTU on a common interface. This check is performed when neighbors exchange DBD packets. If the receiving MTU in the DBD packet is higher then the IP MTU configured on the incoming interface, OSPFv3 adjacency will not be established.

Examples

The following example disables MTU mismatch detection on receiving DBD packets:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 mtu-ignore
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 network

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

ospfv3 [*process-id*] **network** {**broadcast** | **manet** | **non-broadcast** | {**point-to-multipoint** [**non-broadcast**] | **point-to-point**}}
no ospfv3 [*process-id*] **network** {**broadcast** | **manet** | **non-broadcast** | {**point-to-multipoint** [**non-broadcast**] | **point-to-point**}}

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
broadcast	Sets the network type to broadcast.
manet	Sets the network type to Mobile Ad Hoc Network (MANET).
non-broadcast	Sets the network type to nonbroadcast multiaccess (NBMA).
point-to-multipoint non-broadcast	Sets the network type to point-to-multipoint. The optional **non-broadcast** keyword sets the point-to-multipoint network to be nonbroadcast. If you use the **non-broadcast** keyword, the **neighbor** command is required.
point-to-point	Sets the network type to point-to-point.

Command Default

Default depends on the network type.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **ospfv3 network** command to configure an OSPFv3 network type to a type other than the default for a given medium. When the **ospfv3 network**command is configured with the *process-id* argument, it overwrites the **ipv6 ospf network**configuration if OSPFv3 was attached to the interface using the ipv6 ospf area command. When the **ospfv3 network**command is configured without the *process-id* argument, it is inherited on all instances running on the interface. .

MANET Networks

Use the **ospfv3 network manet** command to enable relaying and caching of LSA updates and LSA ACKs on the MANET interface. This results in a reduction of OSPF traffic and saves radio bandwidth.

By default, selective peering is disabled on MANET interfaces.

By default, the OSPFv3 dynamic cost timer is enabled for the MANET network type, as well as caching of LSAs and LSA ACKs received on the MANET interface. The following default values are applied for cache and timers:

LSA cache	Default = 1000 messages
LSA timer	Default = 10 minutes
LSA ACK cache	Default = 1000 messages
LSA ACK timer	Default = 5 minutes

Examples

The following example sets your OSPFv3 network as a broadcast network:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 network broadcast
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 priority

To set the router priority, which helps determine the designated router for this network, use the ospfv3 **priority** command in interface configuration mode. To return to the default value, use the **no** form of this command.

ospfv3 [*process-id*] **priority** *number-value*
no ospfv3 [*process-id*] **priority** *number-value*

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the Open Shortest Path First version 3 (OSPFv3) routing process and can be a value from 1 through 65535.
number-value	A number value that specifies the priority of the router. The range is from 0 to 255.

Command Default

The router priority is 1.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **ospfv3 priority**command to set the router priority, which helps determine the designated router for this network. When the **ospfv3 priority**command is configured with the *process-id* argument, it overwrites the **ipv6 ospf priority**configuration if OSPFv3 was attached to the interface using the ipv6 ospf area command. When the **ospfv3 priority**command is configured without the *process-id* argument, it is inherited on all instances running on the interface.

When two routers attached to a network both attempt to become the designated router, the one 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 is ineligible to become the designated router or backup designated router. Router priority is configured only for interfaces to multiaccess networks (in other words, not to point-to-point networks).

Examples

The following example sets the router priority value to 4:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 priority 4
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 retransmit-interval

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

ospfv3 [*process-id*] **retransmit-interval** *seconds*
no ospfv3 [*process-id*] **retransmit-interval** *seconds*

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
seconds	Time (in seconds) between retransmissions. It 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, and the default is 5 seconds.

Command Default

The default is 5 seconds.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **ospfv3 retransmit-interval**command to specify the time between LSA retransmissions for adjacencies belonging to the interface. When the **ospfv3 retransmit-interval**command is configured with the *process-id* argument, it overwrites the **ipv6 ospf retransmit-interval**configuration if OSPFv3 was attached to the interface using the ipv6 ospf area command. When the **ospfv3 retransmit-interval**command is configured without the *process-id* argument, it is inherited on all instances running on the interface.

When a router sends an LSA to its neighbor, it keeps the LSA until it receives back the acknowledgment message. If the router receives no acknowledgment, it will resend the LSA.

The setting of the restransmit-interval parameter should be conservative, or needless retransmission will result. The value should be larger for serial lines and virtual links.

Examples

The following example sets the retransmit interval value to 8 seconds:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 retransmit-interval 8
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 transmit-delay

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

ospfv3 [*process-id*] **transmit-delay** *seconds*
no ospfv3 [*process-id*] **transmit-delay** *seconds*

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the Open Shortest Path First version 3 (OSPFv3) routing process and can be a value from 1 through 65535.
seconds	Time (in seconds) required to send a link-state update. The range is from 1 to 65535 seconds. The default is 1 second.

Command Default

The default is 1 second.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **ospfv3 transmit-delay**command to set the estimated time required to send a link-state update packet on the interface. When the **ospfv3 transmit-delay**command is configured with the *process-id* argument, it overwrites the **ipv6 ospf transmit-delay**configuration if OSPFv3 was attached to the interface using the ipv6 ospf area command. When the **ospfv3 transmit-delay** command is configured without the *process-id* argument, it is inherited on all instances running on the interface.

Link-state advertisements (LSAs) in the update packet must have their ages incremented by the amount specified in the *seconds* argument before transmission. The value assigned should take into account the transmission and propagation delays for the interface.

If the delay is not added before transmission over a link, the time in which the LSA propagates over the link is not considered. This setting has more significance on very low-speed links.

Examples

The following example sets the retransmit delay value to 3 seconds:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 transmit-delay 3
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

other-config-flag

To verify the advertised “other” configuration parameter, use the **other-config-flag** command in RA guard policy configuration mode.

other-config-flag {**on** | **off**}

Syntax Description

on	Verification is enabled.
off	Verification is disabled.

Command Default

Verification is not enabled.

Command Modes

RA guard policy configuration
(config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **other-config-flag** command enables verification of the advertised "other" configuration parameter (or "O" flag). This flag could be set by an attacker to force hosts to retrieve other configuration information through a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server that may not be trustworthy.

Examples

The following example shows how the command defines a router advertisement (RA) guard policy name as raguard1, places the router in RA guard policy configuration mode, and enables O flag verification:

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# other-config-flag on
```

Related Commands

Command	Description
ipv6 nd raguard policy	Defines the RA guard policy name and enters RA guard policy configuration mode.

passive-interface (IPv6)

To disable sending routing updates on an interface, use the **passive-interface** command in router configuration mode. To reenable the sending of routing updates, use the **no** form of this command.

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

Syntax Description

default	(Optional) All interfaces become passive.
interface-type interface-number	(Optional) Interface type and number. For more information, use the question mark (**?**) online help function.

Command Default

No interfaces are passive. Routing updates are sent to all interfaces on which the routing protocol is enabled.

Command Modes

Router configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.4(6)T	Support for Enhanced Internal Gateway Routing Protocol (EIGRP) IPv6 was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

If you disable the sending of routing updates on an interface, the particular address prefix will continue to be advertised to other interfaces, and updates from other routers on that interface continue to be received and processed.

The **default** keyword sets all interfaces as passive by default. You can then configure individual interfaces where adjacencies are desired using the **no passive-interface** command. The **default** keyword is useful in Internet service provider (ISP) and large enterprise networks where many of the distribution routers have more than 200 interfaces.

OSPF for IPv6 routing information is neither sent nor received through the specified router interface. The specified interface address appears as a stub network in the OSPF for IPv6 domain.

For the Intermediate System-to-Intermediate System (IS-IS) protocol, this command instructs IS-IS to advertise the IP addresses for the specified interface without actually running IS-IS on that interface. The **no** form of this command for IS-IS disables advertising IP addresses for the specified address.

Examples

The following example sets all interfaces as passive, then activates Ethernet interface 0:

```
Router(config-router)# passive-interface default
Router(config-router)# no passive-interface ethernet0/0
```

passive-interface (OSPFv3)

To suppress sending routing updates on an interface when using an IPv4 Open Shortest Path First version 3 (OSPFv3) process, use the **passive-interface** command in router configuration mode. To reenable the sending of routing updates, use the **no** form of this command.

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

Syntax Description

default	(Optional) All interfaces become passive.
interface-type interface-number	(Optional) Interface type and number. For more information, use the question mark (**?**) online help function.

Command Default

No interfaces are passive. Routing updates are sent to all interfaces on which the routing protocol is enabled.

Command Modes

OSPFv3 router configuration mode (config-router)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

If you suppress the sending of routing updates on an interface, the particular address prefix will continue to be advertised to other interfaces, and updates from other routers on that interface continue to be received and processed.

The **default** keyword sets all interfaces as passive by default. You can then configure individual interfaces where adjacencies are desired using the **no passive-interface** command. The **default** keyword is useful in Internet service provider (ISP) and large enterprise networks where many of the distribution routers have more than 200 interfaces.

Examples

The following example sets all interfaces as passive, then activates Ethernet interface 0/0:

```
Router(config-router)# passive-interface default
Router(config-router)# no passive-interface ethernet0/0
```

Related Commands

Command	Description
default (OSPFv3)	Returns an OSPFv3 parameter to its default value.

Command	Description
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

peer default ipv6 address pool

To specify the pool from which client prefixes are assigned, use the **peer default ipv6 address pool** command in interface configuration mode. To disable a prior peer IPv6 address pooling configuration on an interface, or to remove the default address from your configuration, use the **no** form of this command.

peer default ipv6 address pool *pool-name*
no peer default ipv6 address pool

Syntax Description

pool-name	Name of a local address pool created using the **ipv6 local pool** command.

Command Default

The default pool name is **pool**.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS 12.2(13)T	This command was introduced.

Usage Guidelines

Note Ensure that PPP authentication is enabled on the interface.

This command applies to point-to-point interfaces that support PPP encapsulation. This command sets the address used on the remote (PC) side.

This command allows an administrator to configure all possible address pooling mechanisms on an interface-by-interface basis.

Examples

The following command specifies that the interface will use a local IPv6 address pool named pool3:

```
peer default ipv6 address pool pool3
```

In the following example, the pool1 pool is assigned to virtual template 1:

```
interface Virtual-Template1
 encapsulation ppp
 ipv6 enable
 no ipv6 nd suppress-ra
 peer default ipv6 address pool pool1
 ppp authentication chap
```

Related Commands

Command	Description
async dynamic address	Specifies dynamic asynchronous addressing versus default addressing.

Command	Description
encapsulation ppp	Enables PPP encapsulation.
ipv6 local pool	Configures a local pool of IPv6 addresses to be used when a remote peer connects to a point-to-point interface.
ppp	Starts an asynchronous connection using PPP.

permit (IPv6)

To set permit conditions for an IPv6 access list, use the **permit** command in IPv6 access list configuration mode. To remove the permit conditions, use the **no** form of this command.

permit *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**dest-option-type** [{*doh-numberdoh-type*}]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**hbh**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [{*mh-numbermh-type*}]] [**reflect** *name* [**timeout** *value*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]
no permit *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**dest-option-type** [{*doh-numberdoh-type*}]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**hbh**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [{*mh-numbermh-type*}]] [**reflect** *name* [**timeout** *value*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

Internet Control Message Protocol
permit icmp {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [{*icmp-type* [*icmp-code*]*icmp-message*}] [**dest-option-type** [{*doh-numberdoh-type*}]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**hbh**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [{*mh-numbermh-type*}]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

Transmission Control Protocol
permit tcp {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**ack**] [**dest-option-type** [{*doh-numberdoh-type*}]] [**dscp** *value*] [**established**] [**fin**] [**flow-label** *value*] [**fragments**] [**hbh**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [{*mh-numbermh-type*}]] [**neq** {*portprotocol*}] [**psh**] [**range** {*portprotocol*}] [**reflect** *name* [**timeout** *value*]] [**routing**] [**routing-type** *routing-number*] [**rst**] [**sequence** *value*] [**syn**] [**time-range** *name*] [**urg**]

User Datagram Protocol
permit udp {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**dest-option-type** [{*doh-numberdoh-type*}]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**hbh**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [{*mh-numbermh-type*}]] [**neq** {*portprotocol*}] [**range** {*portprotocol*}] [**reflect** *name* [**timeout** *value*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

Syntax Description

protocol	Name or number of an Internet protocol. It can be one of the keywords **ahp**, **esp**, **icmp**, **ipv6**, **pcp**, **sctp**, **tcp**, **udp**, or **hbh**, or an integer in the range from 0 to 255 representing an IPv6 protocol number.
source-ipv6-prefix/prefix-length	The source IPv6 network or class of networks about which to set permit conditions. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

any	An abbreviation for the IPv6 prefix ::/0.
host *source-ipv6-address*	The source IPv6 host address about which to set permit conditions. This *source-ipv6-address* argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
auth	Allows matching traffic against the presence of the authentication header in combination with any protocol.
operator [*port-number*]	(Optional) Specifies an operand that compares the source or destination ports of the specified protocol. Operands are **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range). If the operator is positioned after the *source-ipv6-prefix*/*prefix-length* argument, it must match the source port. If the operator is positioned after the *destination-ipv6-prefix*/*prefix-length* argument, it must match the destination port. The **range** operator requires two port numbers. All other operators require one port number. The optional *port-number* argument is a decimal number or the name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP port names can be used only when filtering TCP. UDP port names can be used only when filtering UDP.
destination-ipv6-prefix/ *prefix-length*	The destination IPv6 network or class of networks about which to set permit conditions. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
host *destination-ipv6-address*	The destination IPv6 host address about which to set permit conditions. This *destination-ipv6-address* argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
dest-option-type	(Optional) Matches IPv6 packets against the destination extension header within each IPv6 packet header.
doh-number	(Optional) Integer in the range from 0 to 255 representing an IPv6 destination option extension header.
doh-type	(Optional) Destination option header types. The possible destination option header type and its corresponding *doh-number* value are home-address—201.
dscp *value*	(Optional) Matches a differentiated services codepoint value against the traffic class value in the Traffic Class field of each IPv6 packet header. The acceptable range is from 0 to 63.
flow-label *value*	(Optional) Matches a flow label value against the flow label value in the Flow Label field of each IPv6 packet header. The acceptable range is from 0 to 1048575.

fragments	(Optional) Matches non-initial fragmented packets where the fragment extension header contains a non-zero fragment offset. The **fragments** keyword is an option only if the *operator* [*port-number*] arguments are not specified. When this keyword is used, it also matches when the first fragment does not have Layer 4 information.
hbh	(Optional) Matches IPv6 packets against the hop-by-hop extension header within each IPv6 packet header.
log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The message includes the access list name and sequence number, whether the packet was permitted; the protocol, whether it was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted in the prior 5-minute interval.
log-input	(Optional) Provides the same function as the **log** keyword, except that the logging message also includes the input interface.
mobility	(mobility) Matches IPv6 packets against the mobility extension header within each IPv6 packet header.
mobility-type	(Optional) Matches IPv6 packets against the mobility-type extension header within each IPv6 packet header. Either the *mh-number* or *mh-type* argument must be used with this keyword.
mh-number	(Optional) Integer in the range from 0 to 255 representing an IPv6 mobility header type.
mh-type	(Optional) Mobility header types. Possible mobility header types and their corresponding *mh-number* value are as follows: • 0—bind-refresh • 1—hoti • 2—coti • 3—hot • 4—cot • 5—bind-update • 6—bind-acknowledgment • 7—bind-error

reflect *name*	(Optional) Specifies a reflexive IPvì6 access list. Reflexive IPv6 access lists are created dynamically when an IPv6 packets matches a permit statement that contains the **reflect** keyword. The reflexive IPv6 access list mirrors the permit statement and times out automatically when no IPv6 packets match the permit statement. Reflexive IPv6 access lists can be applied to the TCP, UDP, SCTP, and ICMP for IPv6 packets.
timeout *value*	(Optional) Interval of idle time (in seconds) after which a reflexive IPv6 access list times out. The acceptable range is from 1 to 4294967295. The default is 180 seconds.
routing	(Optional) Matches source-routed packets against the routing extension header within each IPv6 packet header.
routing-type	(Optional) Matches IPv6 packets against the routing-type extension header within each IPv6 packet header. The *routing-number* argument must be used with this keyword.
routing-number	Integer in the range from 0 to 255 representing an IPv6 routing header type. Possible routing header types and their corresponding *routing-number* value are as follows: • 0—Standard IPv6 routing header • 2—Mobile IPv6 routing header
sequence *value*	(Optional) Specifies the sequence number for the access list statement. The acceptable range is from 1 to 4294967295.
time-range *name*	(Optional) Specifies the time range that applies to the permit statement. The name of the time range and its restrictions are specified by the **time-range** and **absolute** or **periodic** commands, respectively.
icmp-type	(Optional) Specifies an ICMP message type for filtering ICMP packets. ICMP packets can be filtered by ICMP message type. The ICMP message type can be a number from 0 to 255, some of which include the following predefined strings and their corresponding numeric values: • 144—dhaad-request • 145—dhaad-reply • 146—mpd-solicitation • 147—mpd-advertisement
icmp-code	(Optional) Specifies an ICMP message code for filtering ICMP packets. ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.
icmp-message	(Optional) Specifies an ICMP message name for filtering ICMP packets. ICMP packets can be filtered by an ICMP message name or ICMP message type and code. The possible names are listed in the “Usage Guidelines” section.

ack	(Optional) For the TCP protocol only: acknowledgment (ACK) bit set.
established	(Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the ACK or RST bits set. The nonmatching case is that of the initial TCP datagram to form a connection.
fin	(Optional) For the TCP protocol only: Fin bit set; no more data from sender.
neq {*port* | *protocol*}	(Optional) Matches only packets that are not on a given port number.
psh	(Optional) For the TCP protocol only: Push function bit set.
{**range** *port* | *protocol*}	(Optional) Matches only packets in the range of port numbers.
rst	(Optional) For the TCP protocol only: Reset bit set.
syn	(Optional) For the TCP protocol only: Synchronize bit set.
urg	(Optional) For the TCP protocol only: Urgent pointer bit set.

Command Default

No IPv6 access list is defined.

Command Modes

IPv6 access list configuration (config-ipv6-acl)#

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.4(2)T	The *icmp-type* argument was enhanced. The **dest-option-type**, **mobility**, **mobility-type**, and **routing-type** keywords were added. The *doh-number*, *doh-type*, *mh-number*, *mh-type*, and *routing-number* arguments were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 series routers.
12.4(20)T	The **auth** keyword was added.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
15.2(3)T	This command was modified. Support was added for the **hbh** keyword.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Release	Modification
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

The **permit** (IPv6) command is similar to the **permit** (IP) command, except that it is IPv6-specific.

Use the **permit** (IPv6) command following the **ipv6 access-list** command to define the conditions under which a packet passes the access list or to define the access list as a reflexive access list.

Specifying IPv6 for the *protocol* argument matches against the IPv6 header of the packet.

By default, the first statement in an access list is number 10, and the subsequent statements are incremented by 10.

You can add **permit**, **deny**, **remark**, or **evaluate** statements to an existing access list without retyping the entire list. To add a new statement anywhere other than at the end of the list, create a new statement with an appropriate entry number that falls between two existing entry numbers to indicate where it belongs.

In Cisco IOS Release 12.2(2)T or later releases, 12.0(21)ST, and 12.0(22)S, IPv6 access control lists (ACLs) are defined and their deny and permit conditions are set by using the **ipv6 access-list** command with the **deny** and **permit** keywords in global configuration mode. In Cisco IOS Release 12.0(23)S or later releases, IPv6 ACLs are defined by using the **ipv6 access-list** command in global configuration mode and their permit and deny conditions are set by using the **deny** and **permit** commands in IPv6 access list configuration mode. Refer to the **ipv6 access-list** command for more information on defining IPv6 ACLs.

Note In Cisco IOS Release 12.0(23)S or later releases, every IPv6 ACL has implicit **permit icmp any any nd-na**, **permit icmp any any nd-ns**, and **deny ipv6 any any** statements as its last match conditions. (The former two match conditions allow for ICMPv6 neighbor discovery.) An IPv6 ACL must contain at least one entry for the implicit **deny ipv6 any any** statement to take effect. The IPv6 neighbor discovery process makes use of the IPv6 network layer service; therefore, by default, IPv6 ACLs implicitly allow IPv6 neighbor discovery packets to be sent and received on an interface. In IPv4, the Address Resolution Protocol (ARP), which is equivalent to the IPv6 neighbor discovery process, makes use of a separate data link layer protocol; therefore, by default, IPv4 ACLs implicitly allow ARP packets to be sent and received on an interface.

Both the *source-ipv6-prefix*/*prefix-length* and *destination-ipv6-prefix*/*prefix-length* arguments are used for traffic filtering (the source prefix filters traffic based upon the traffic source; the destination prefix filters traffic based upon the traffic destination).

Note IPv6 prefix lists, not access lists, should be used for filtering routing protocol prefixes.

The **fragments** keyword is an option only if the *operator* [*port-number*] arguments are not specified.

The following is a list of ICMP message names:

- beyond-scope
- destination-unreachable

- echo-reply
- echo-request
- header
- hop-limit
- mld-query
- mld-reduction
- mld-report
- nd-na
- nd-ns
- next-header
- no-admin
- no-route
- packet-too-big
- parameter-option
- parameter-problem
- port-unreachable
- reassembly-timeout
- renum-command
- renum-result
- renum-seq-number
- router-advertisement
- router-renumbering
- router-solicitation
- time-exceeded
- unreachable

Defining Reflexive Access Lists

To define an IPv6 reflexive list, a form of session filtering, use the **reflect** keyword in the **permit** (IPv6) command. The **reflect** keyword creates an IPv6 reflexive access list and triggers the creation of entries in the reflexive access list. The **reflect** keyword must be an entry (condition statement) in an IPv6 access list.

Note For IPv6 reflexive access lists to work, you must nest the reflexive access list using the **evaluate** command.

If you are configuring IPv6 reflexive access lists for an external interface, the IPv6 access list should be one that is applied to outbound traffic.

If you are configuring an IPv6 reflexive access list for an internal interface, the IPv6 access list should be one that is applied to inbound traffic.

IPv6 sessions that originate from within your network are initiated with a packet exiting your network. When such a packet is evaluated against the statements in the IPv6 access list, the packet is also evaluated against the IPv6 reflexive permit entry.

As with all IPv6 access list entries, the order of entries is important, because they are evaluated in sequential order. When an IPv6 packet reaches the interface, it will be evaluated sequentially by each entry in the access list until a match occurs.

If the packet matches an entry prior to the reflexive permit entry, the packet will not be evaluated by the reflexive permit entry, and no temporary entry will be created for the reflexive access list (session filtering will not be triggered).

The packet will be evaluated by the reflexive permit entry if no other match occurs first. Then, if the packet matches the protocol specified in the reflexive permit entry, the packet is forwarded and a corresponding temporary entry is created in the reflexive access list (unless the corresponding entry already exists, indicating that the packet belongs to a session in progress). The temporary entry specifies criteria that permit traffic into your network only for the same session.

Characteristics of Reflexive Access List Entries

The **permit** (IPv6) command with the **reflect** keyword enables the creation of temporary entries in the same IPv6 reflexive access list that was defined by the **permit** (IPv6) command. The temporary entries are created when an IPv6 packet exiting your network matches the protocol specified in the **permit** (IPv6) command. (The packet "triggers" the creation of a temporary entry.) These entries have the following characteristics:

- The entry is a permit entry.
- The entry specifies the same IP upper-layer protocol as the original triggering packet.
- The entry specifies the same source and destination addresses as the original triggering packet, except that the addresses are swapped.
- If the original triggering packet is TCP or UDP, the entry specifies the same source and destination port numbers as the original packet, except that the port numbers are swapped.
- If the original triggering packet is a protocol other than TCP or UDP, port numbers do not apply, and other criteria are specified. For example, for ICMP, type numbers are used: The temporary entry specifies the same type number as the original packet (with only one exception: if the original ICMP packet is type 8, the returning ICMP packet must be type 0 to be matched).
- The entry inherits all the values of the original triggering packet, with exceptions only as noted in the previous four bullets.
- IPv6 traffic entering your internal network will be evaluated against the entry, until the entry expires. If an IPv6 packet matches the entry, the packet will be forwarded into your network.
- The entry will expire (be removed) after the last packet of the session is matched.
- If no packets belonging to the session are detected for a configured length of time (the timeout period), the entry will expire.

Examples

The following example configures two IPv6 access lists named OUTBOUND and INBOUND and applies both access lists to outbound and inbound traffic on Ethernet interface 0. The first and second permit entries in the OUTBOUND list permit all TCP and UDP packets from network 2001:ODB8:0300:0201::/64 to exit out of Ethernet interface 0. The entries also configure the temporary IPv6 reflexive access list named REFLECTOUT to filter returning (incoming) TCP and UDP packets on Ethernet interface 0. The first deny entry in the OUTBOUND list keeps all packets from the network FEC0:0:0:0201::/64 (packets that have the site-local prefix FEC0:0:0:0201 as the first 64 bits of their source IPv6 address) from exiting out of Ethernet interface 0. The third permit entry in the OUTBOUND list permits all ICMP packets to exit out of Ethernet interface 0.

The permit entry in the INBOUND list permits all ICMP packets to enter Ethernet interface 0. The **evaluate** command in the list applies the temporary IPv6 reflexive access list named REFLECTOUT to inbound TCP and UDP packets on Ethernet interface 0. When outgoing TCP or UDP packets are permitted on Ethernet interface 0 by the OUTBOUND list, the INBOUND list uses the REFLECTOUT list to match (evaluate) the returning (incoming) TCP and UDP packets. Refer to the **evaluate** command for more information on nesting IPv6 reflexive access lists within IPv6 ACLs.

```
ipv6 access-list OUTBOUND
 permit tcp 2001:0DB8:0300:0201::/64 any reflect REFLECTOUT
 permit udp 2001:0DB8:0300:0201::/64 any reflect REFLECTOUT
 deny FEC0:0:0:0201::/64 any
 permit icmp any any
ipv6 access-list INBOUND
 permit icmp any any
 evaluate REFLECTOUT
interface ethernet 0
 ipv6 traffic-filter OUTBOUND out
 ipv6 traffic-filter INBOUND in
```

Note Given that a **permit any any** statement is not included as the last entry in the OUTBOUND or INBOUND access list, only TCP, UDP, and ICMP packets will be permitted out of and in to Ethernet interface 0 (the implicit deny all condition at the end of the access list denies all other packet types on the interface).

The following example shows how to allow the matching of any UDP traffic. The authentication header may be present.

```
permit udp any any sequence 10
```

The following example shows how to allow the matching of only TCP traffic if the authentication header is also present.

```
permit tcp any any auth sequence 20
```

The following example shows how to allow the matching of any IPv6 traffic where the authentication header is present.

```
permit ahp any any sequence 30
```

Related Commands

Command	Description
deny (IPv6)	Sets deny conditions for an IPv6 access list.
evaluate (IPv6)	Nests an IPv6 reflexive access list within an IPv6 access list.
ipv6 access-list	Defines an IPv6 access list and enters IPv6 access list configuration mode.
ipv6 traffic-filter	Filters incoming or outgoing IPv6 traffic on an interface.
show ipv6 access-list	Displays the contents of all current IPv6 access lists.

permit link-local

To allow hardware bridging for all data traffic sourced by a link-local address, use the **permit link-local** command in source-guard policy configuration mode or switch integrated security features source-guard policy configuration mode. To disable this function, use the **no** form of this command.

permit link-local
no permit link-local

Syntax Description

This command has no arguments or keywords.

Command Default

This function is disabled.

Command Modes

Source-guard policy configuration (config-source-guard)

Command History

Release	Modification
15.0(2)SE	This command was introduced.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.

Usage Guidelines

Use the **permit link-local** command to allow hardware bridging for all data traffic sourced by a link-local address. This feature is used to reduce the number of ternary content addressable memory (TCAM) entries that are used. Because link-local addresses are valid only on the local link, they are not as critical to block as global addresses.

Use the **permit link-local** command after entering the **ipv6 source-guard policy** command to define an IPv6 source-guard policy name.

Examples

The following example shows how to allow hardware bridging for all data traffic sourced by a link-local address:

```
Device(config)# ipv6 source-guard policy mysgpolicy
Device(config-source-guard)# permit link-local
```

Related Commands

Command	Description
ipv6 source-guard policy	Defines an IPv6 source-guard policy name and enters source-guard policy configuration mode.

ping ipv6

To diagnose basic net work connectivity when using IPv6, use the **ping IPv6** command in user EXEC or privileged EXEC mode.

ping ipv6 *ipv6-address* [{**data** *hex-data-pattern* | **repeat** *repeat-count* | **size** *datagram-size* | **source** [{**async** | **bvi** | **ctunnel** | **dialer** | **ethernet** | **fastEthernet** | **gigabitEthernet** | **loopback** | **mfr** | **multilink** | **null** | **port-channel** | **tunnel** | **virtual-template***source-address* | **xtagatm**}] | **timeout** *seconds* | **verbose**}]

Syntax Description

ipv6-address	The address or hostname of the IPv6 host to be pinged. This address or hostname must be in the form documented in RFC 2373, where the address is specified in hexadecimal using 16-bit values between colons.
data	(Optional) Specifies the data pattern.
hex-data-pattern	(Optional) Range is from 0 to FFFF.
repeat	(Optional) Specifies the number of pings sent. The default is 5.
repeat-count	(Optional) Range is from 1 to 2147483647.
size	(Optional) Specifies the datagram size. Datagram size is the number of bytes in each ping.
datagram-size	(Optional) Range is from 48 to 18024.
source	(Optional) Specifies the source address or name.
async	(Optional) Asynchronous interface.
bvi	(Optional) Bridge-Group Virtual Interface.
ctunnel	(Optional) CTunnel interface.
dialer	(Optional) Dialer interface.
ethernet	(Optional) Ethernet IEEE 802.3.
fastEthernet	(Optional) FastEthernet IEEE 802.3.
gigabitEthernet	(Optional) GigabitEthernet IEEE 802.3z.
loopback	(Optional) Loopback interface.
mfr	(Optional) Multilink frame relay (MFR) bundle interface.
multilink	(Optional) Multilink-group interface.
null	(Optional) Null interface.
port-channel	(Optional) Ethernet channel of interfaces.
tunnel	(Optional) Tunnel interface.

virtual-template	(Optional) Virtual template interface.
source-address	(Optional) Source IPv6 address or name.
xtagatm	(Optional) Extended Tag ATM interface.
timeout	(Optional) Specifies the timeout interval in seconds. The default is 2 seconds.
seconds	(Optional) Range is from 0 to 3600.
verbose	(Optional) Displays the verbose output.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The user-level ping feature provides a basic ping facility for users that do not have system privileges. This feature allows the Cisco IOS software to perform the simple default ping functionality for a number of protocols.

The ping program sends an echo request packet to an address, then awaits a reply. Ping output can help you evaluate path-to-host reliability, delays over the path, and whether the host can be reached or is functioning.

If the system cannot map an address for a hostname, it returns an "%Unrecognized host or address, or protocol not running" message.

To abnormally terminate a ping session, type the escape sequence--by default, Ctrl-^ X. You type the default by simultaneously pressing and releasing the Ctrl, Shift, and 6 keys, and then pressing the X key.

Caution When the **timeout** keyword is used with the *seconds* argument set to 0, an immediate timeout occurs, which causes a flood ping. Use the **timeout 0** parameter with caution, because you may receive replies only from immediately adjacent routers depending on router and network use, distance to the remote device, and other factors.

The table below describes the characters displayed by the ping facility in IPv6.

Table 1: ping Test Characters (IPv6)

!	Each exclamation point indicates receipt of a reply.
.	Each period indicates that the network server timed out while waiting for a reply.
?	Unknown error.
@	Unreachable for unknown reason.
A	Administratively unreachable. Usually, this output indicates that an access list is blocking traffic.
B	Packet too big.
C	Alignment errors.
H	Host unreachable.
N	Network unreachable (beyond scope).
P	Port unreachable.
R	Parameter problem.
S	Source address failed ingress/egress policy.
T	Time exceeded.
U	No route to host.
X	Reject route to destination.

Note Not all protocols require hosts to support pings. For some protocols, the pings are Cisco-defined and are answered only by another Cisco router.

When the **ping ipv6** command is enabled, the router attempts to resolve hostnames into IPv6 addresses before trying to resolve them into IPv4 addresses, so if a hostname resolves to both an IPv6 and an IPv4 address and you specifically want to use the IPv4 address, use the **ping** (IPv4) command.

Examples

The following user EXEC example shows sample output for the **ping ipv6** command:

```
Router# ping ipv6 2001:0DB8::3/64
Target IPv6 address: 2001:0DB8::3/64
Repeat count [5]:
Datagram size [100]:48
Timeout in seconds [2]:
Extended commands? [no]: yes
UDP protocol? [no]:
Verbose? [no]:
Precedence [0]:
DSCP [0]:
Include hop by hop option? [no]:yes
Include destination option? [no]:y
% Using size of 64 to accommodate extension headers
```

```
Sweep range of sizes? [no]:y
Sweep min size [100]: 100
Sweep max size [18024]: 150
Sweep interval [1]: 5
Sending 55, [100..150]-byte ICMP Echos to 2001:0DB8::3/64, timeout is 2 seconds:
Success rate is 100 percent
round-trip min/avg/max = 2/5/10 ms
```

The table below describes the default **ping ipv6** fields shown in the display.

Table 2: ping ipv6 Field Descriptions

Field	Description
Target IPv6 address:	Prompts for the IPv6 address or host name of the destination node you plan to ping. Default: none.
Repeat count [5]:	Number of ping packets that will be sent to the destination address. Default: 5.
Datagram size [100]:	Size of the ping packet (in bytes). Default: 100 bytes.
Timeout in seconds [2]:	Timeout interval (in seconds). Default: 2.
Extended commands [no]:	Specifies whether a series of additional commands appears. Default: no. In an IPv6 dialog for the **ping IPv6** command, entering yes in the Extended commands field displays the UDP protocol?, Verbose, Priority, and Include extension headers? fields.
UDP protocol? [no]:	Specifies UDP packets or ICMPv6 packets. Default: no (ICMP packets are sent).
Verbose? [no]:	Enables verbose output.
Precedence [0]:	Sets precedence in the IPv6 header. The range is from 0 to 7.
DSCP [0]:	Sets Dynamic Host Configuration Protocol (DSCP) in the IPv6 header. The range is from 0 to 63. DSCP appears only if the precedence option is not set, because precedence and DSCP are two separate ways of viewing the same bits in the header.
Include hop by hop option? [no]:	The IPv6 hop-by-hop option is included in the outgoing echo request header, requiring the ping packet to be examined by each node along the path and therefore not be fast-switched or Cisco Express Forwarding-switched. This function may help with debugging network connectivity, especially switching problems. **Note** A Cisco router also includes the hop-by-hop option in the returned echo reply, so the packets should be process-switched rather than fast-switched or Cisco Express Forwarding-switched on the return path also. Non-Cisco routers likely do not have this option in their echo reply; therefore, if the echo request with hop-by-hop option arrives at the destination but the echo reply does not come back and the destination is not a Cisco router, a fast-path issue may exist in an intermediate router.

Field	Description
Include destination option? [no]:	Includes an IPv6 destination option in the outgoing echo request header.
Sweep range of sizes? [no]:	Allows you to vary the sizes of the echo packets being sent. This capability is useful for determining the minimum sizes of the maximum transmission units (MTUs) configured on the nodes along the path to the destination address. Packet fragmentation contributing to performance problems can then be reduced.
Sweep min size [100]: Sweep max size [18024]: Sweep interval [1]:	Options that appear if "Sweep range of sizes?" option is enabled. • Sweep min size--Defaults to the configured "Datagram size" parameter and will override that value if specified. • Sweep Interval--The size of the intervals between the "Sweep min size" and "Sweep max size" parameters. For example, min of 100 max of 150 with an interval of 5 means packets sent are of 100, 105, 110, ..., 150 bytes in size.
Sending 55, [100..150]-byte ICMP Echos to ...	Minimum and maximum sizes and interval as configured in "Sweep range of sizes" options. Sizes are reported if the ping fails (but not if it succeeds, unless the verbose option is enabled).
Success rate is 100 percent	Percentage of packets successfully echoed back to the router. Anything less than 80 percent is usually considered problematic.
round-trip min/avg/max = 2/5/10 ms	Round-trip minimum, average, and maximum time intervals for the protocol echo packets (in milliseconds).

platform ipv6 acl fragment hardware

To permit or deny fragments at hardware, use the **platform ipv6 acl fragment hardware** command in global configuration mode. To reset the IPv6 fragment handling to bridged mode, use the **no** form of this command.

platform ipv6 acl fragment hardware {**forward** | **drop**}
no platform ipv6 acl fragment hardware {**forward** | **drop**}

Syntax Description

forward	Forwards the IPv6 fragments in the hardware.
drop	Drops the IPv6 fragments in the hardware.

Command Default

The **no** form of this command is the default behavior.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.

Usage Guidelines

The PFC3A, PFC3B, and PFC3BXL are unable to handle IPv6 fragments in hardware, and all IPv6 fragments are handled in software. This could result in high CPU if your traffic includes a large amount of IPv6 fragments. This limitation is handled in the PFC3C hardware. The **platform ipv6 acl fragment hardware**command provides a software workaround for the PFC3A, PFC3B, and PFC3BXL by specifying either to permit or drop all IPv6 fragments in hardware.

Note When you enter the **drop** keyword, a small portion of the packets is leaked to the software (for ICMP message generation) and forwarded in software.

The **platform ipv6 acl fragment hardware** command overrides the following actions:

- Any ACE in the IPv6 filter (ACL) that contains the **fragment** keyword. If the ACE in the ACL contains the **fragment** keyword, the associated action (**permit** | **deny** | **log**) is not taken, and the action (**permit** | **drop**) specified by the **platform ipv6 acl fragment hardware** command is taken.
- Any IPv6 ACL that contains ACEs that implicitly permit IPv6 fragments; for example, permit ACEs that contain Layer 4 ports to implicitly permit fragments only.
- If the IPv6 fragment hits the implicit **deny any any** ACE added at the end of the ACL, the IPv6 fragment will not get hit.

Examples

This example shows how to forward the IPv6 fragments at hardware:

```
Router(config)#
platform ipv6 acl fragment hardware forward
```

This example shows how to drop the IPv6 fragments at hardware:

```
Router(config)#
platform ipv6 acl fragment hardware drop
```

platform ipv6 acl icmp optimize neighbor-discovery

To optimize ternary content addressable memory (TCAM) support for IPv6 access lists (ACLs), use the **platform ipv6 acl icmp optimize neighbor-discovery** command in global configuration mode. To disable optimization of TCAM support for IPv6 ACLs, use the **no** form of this command.

platform ipv6 acl icmp optimize neighbor-discovery
no platform ipv6 acl icmp optimize neighbor-discovery

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Note Use this command under the direction of the Cisco Technical Assistance Center only.

When you enable optimization of the TCAM support for IPv6 ACLs, the global Internet Control Message Protocol version 6 (ICMPv6) neighbor-discovery ACL at the top of the TCAM is programmed to permit all ICMPv6 neighbor-discovery packets. Enabling optimization prevents the addition of ICMPv6 access control entries (ACEs) at the end of every IPv6 security ACL, reducing the number of TCAM resources being used. Enabling this command reprograms IPv6 ACLs on all interfaces.

Note The ICMPv6 neighbor-discovery ACL at the top of the TCAM takes precedence over security ACLs for ICMP neighbor-discovery packets that you have configured, but has no effect if you have a bridge/deny that overlaps with the global ICMP ACL.

Examples

This example shows how to optimize TCAM support for IPv6 ACLs:

```
Router(config)# platform ipv6 acl icmp optimize neighbor-discovery
```

This example shows how to disable optimization of TCAM support for IPv6 ACLs:

```
Router(config)# no platform ipv6 acl icmp optimize neighbor-discovery
```

platform ipv6 acl punt extension-header

To enable processing of IPv6 packets with extension headers in software on the RP, use the **platform ipv6 acl punt extension-header**command in global configuration mode. To disable processing of IPv6 packets with extension headers in software on the RP, use the **no** form of this command.

platform ipv6 acl punt extension-header
no platform ipv6 acl punt extension-header

Syntax Description

This command has no arguments or keywords.

Command Default

IPv6 packets with extension headers are processed in software.

Command Modes

Global configuration mode

Command History

Release	Modification
12.2(33)SXH7	This command was introduced on the Supervisor Engine 720.
15.2(2)S	This command was introduced on the Cisco 7600 series routers.

Usage Guidelines

If your IPv6 traffic does not specify a Layer 4 protocol, software processing of IPv6 packets with extension headers is unnecessary. If your IPv6 traffic specifies a Layer 4 protocol, you can enter the **platform ipv6 acl punt extension-header** global configuration command to enable software processing of IPv6 packets with extension headers. On the Cisco 7600 series routers, this command is applicable only on the line cards that use Pinnacle as the port ASIC. Examples for such line cards include WS-X6548-GE-TX, WS-X6516A-GBIC, WS-X6516-GBIC, WS-X6148-GE-TX, and WS-X6816-GBIC.

Examples

This example shows how to enable processing of IPv6 packets with extension headers in software on the RP:

```
Router(config)# platform ipv6 acl punt extension-header
Router(config)#
```

This example shows how to disable processing of IPv6 packets with extension headers in software on the RP:

```
Router(config)# no platform ipv6 acl punt extension-header
Router(config)#
```

poison-reverse (IPv6 RIP)

To configure the poison reverse processing of IPv6 Routing Information Protocol (RIP) router updates, use the **poison-reverse**command in router configuration mode. To disable the poison reverse processing of IPv6 RIP updates, use the **no** form of this command.

poison-reverse
no poison-reverse

Syntax Description

This command has no keywords or arguments

Command Default

Poison reverse is not configured.

Command Modes

Router configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

This command configures poison reverse processing of IPv6 RIP router updates. When poison reverse is configured, routes learned via RIP are advertised out the interface over which they were learned, but with an unreachable metric.

If both poison reverse and split horizon are configured, then simple split horizon behavior (suppression of routes out of the interface over which they were learned) is replaced by poison reverse behavior.

Examples

The following example configures poison reverse processing for the IPv6 RIP routing process named cisco:

```
Router(config)# ipv6 router rip cisco
Router(config-rtr)# poison-reverse
```

Related Commands

Command	Description
split-horizon (IPv6 RIP)	Configures split horizon processing of IPv6 RIP router updates.

port (IPv6 RIP)

To configure a specified UDP port and multicast address for an IPv6 Routing Information Protocol (RIP) routing process, use the **port** command in RIP router configuration mode. To return the port number and multicast address to their default values, use the **no** form of this command.

port *port-number* **multicast-group** *multicast-address*
no port *port-number* **multicast-group** *multicast-address*

Syntax Description

port-number	UDP port number. The range is from 1 to 65535. The table in the "Usage Guidelines" section lists common UDP services and their port numbers.
multicast-group	Specifies a multicast group.
multicast-address	Address or hostname of the multicast group.

Command Default

UDP port 521; multicast address FF02::9

Command Modes

RIP router configuration (config-rtr-rip)

Command History

Release	Modification
Cisco IOS 12.2(2)T	This command was introduced.
Cisco IOS 12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
Cisco IOS 12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
Cisco IOS 12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
Cisco IOS 12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
Cisco IOS 12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
Cisco IOS 12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS 12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS 15.4(1)S	This command was deprecated.
Cisco IOS 15.4(1)T	This command was deprecated.

Usage Guidelines

Two IPv6 RIP routing processes cannot use the same UDP port. If two IPv6 RIP routing processes are configured on the same UDP port, the second process will not start until the configuration conflict is resolved. Two IPv6 RIP routing processes, though, can use the same multicast address. UDP services and port numbers are shown in the table below.

Table 3: Common UDP Services and Their Port Numbers

Service	Port
Domain Name System (DNS)	53
Network File System (NFS)	2049
remote-procedure call (RPC)	111
Simple Network Management Protocol (SNMP)	161
Trivial File Transfer Protocol (TFTP)	69

Examples

The following example configures UDP port 200 and multicast address FF02::9 for the IPv6 RIP routing process named cisco:

```
Device(config)# ipv6 router rip cisco
Device(config-rtr-rip)# port 200 multicast-group FF02::9
```

port (TACACS+)

To specify the TCP port to be used for TACACS+ connections, use the **port**command in TACACS+ server configuration mode. To remove the TCP port, use the **no** form of this command.

port [*number*]
no port [*number*]

Syntax Description

number	(Optional) Specifies the port where the TACACS+ server receives access-request packets. The range is from 1 to 65535.

Command Default

If no port is configured, port 49 is used.

Command Modes

TACACS+ server configuration (config-server-tacacs)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

TCP port 49 is used if the *number* argument is not used when using the **port** command.

Examples

The following example shows how to specify TCP port 12:

```
Router (config)# tacacs server server1
Router(config-server-tacacs)# port 12
```

Related Commands

Command	Description
tacacs server	Configures the TACACS+ server for IPv6 or IPv4 and enters TACACS+ server configuration mode.

ppp ipv6cp address unique

To verify if the IPv6 prefix delegation is unique using a PP-enabled interface, and to disconnect the session if the peer IPv6 prefix is duplicated, use the **ppp ipv6cp address unique**command in interface configuration mode. To disable the configuration, use the **no** form of this command.

ppp ipv6cp address unique
no ppp ipv6cp address unique

Syntax Description

This command has no arguments or keywords.

Command Default

Verification of the uniqueness of the IPv6 prefix delegation is not configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Examples

The following example shows how to verify whether the IPv6 prefix delegation is unique using a PPP-enabled interface, and to disconnect the session if the peer IPv6 prefix is duplicated:

```
Router> enable

Router# configure terminal
Router(config)# interface virtual-template 5
Router(config-if)# ppp ipv6cp address unique
```

ppp multilink

To enable Multilink PPP (MLP) on an interface and, optionally, to enable Bandwidth Allocation Control Protocol (BACP) and its Bandwidth Allocation Protocol (BAP) subset for dynamic bandwidth allocation, use the **ppp multilink** command in interface configuration mode. To disable Multilink PPP or, optionally, to disable only dynamic bandwidth allocation, use the **no** form of this command.

ppp multilink [**bap**]
no ppp multilink [**bap** [**required**]]

Cisco 10000 Series Router
ppp multilink
no ppp multilink

Syntax Description

bap	(Optional) Specifies bandwidth allocation control negotiation and dynamic allocation of bandwidth on a link.
required	(Optional) Enforces mandatory negotiation of BACP for the multilink bundle. The multilink bundle is disconnected if BACP is not negotiated.

Command Default

This command is disabled. When BACP is enabled, the defaults are to accept calls and to set the timeout pending at 30 seconds.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.1	This command was introduced.
12.0(23)SX	This command was implemented on the Cisco 10000 series router.
12.2(16)BX	This command was implemented on the ESR-PRE2.
12.2(31)SB 2	This command was integrated into Cisco IOS Release 12.2(31)SB 2.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.2(2)SNI	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

This command applies only to interfaces that use PPP encapsulation.

MLP and PPP reliable links do not work together.

When the **ppp multilink**command is used, the first channel will negotiate the appropriate Network Control Protocol (NCP) layers (such as the IP Control Protocol and IPX Control Protocol), but subsequent links will negotiate only the link control protocol and MLP. NCP layers do not get negotiated on these links, and it is normal to see these layers in a closed state.

This command with the **bap** keyword must be used before configuring any **ppp bap** commands and options. If the **bap required** option is configured and a reject of the options is received, the multilink bundle is torn down.

The **no** form of this command without the **bap** keyword disables both MLP and BACP on the interface.

The **dialer load-threshold** command enables a rotary group to bring up additional links and to add them to a multilink bundle.

Before Cisco IOS Release 11.1, the **dialer-load threshold 1** command kept a multilink bundle of any number of links connected indefinitely, and the **dialer-load threshold 2** command kept a multilink bundle of two links connected indefinitely. If you want a multilink bundle to be connected indefinitely, you must set a very high idle timer.

Note By default, after changing hostnames, an MLP member link does not undergo failure recovery automatically. You must use the **ppp chap hostname** command to define the MLP bundle name on an endpoint. If this command is not configured and the hostname is changed, then a link flap will not return the link back to the bundle.

Cisco 10000 Series Router

The ppp multilink command has no arguments or keywords.

Examples

The following partial example shows how to configure a dialer for MLP:

```
interface Dialer0
 ip address 10.0.0.2 255.0.0.0
 encapsulation ppp
 dialer in-band
 dialer idle-timeout 500
 dialer map ip 10.0.0.1 name atlanta broadcast 81012345678901
 dialer load-threshold 30 either
 dialer-group 1
 ppp authentication chap
 ppp multilink
```

Related Commands

Command	Description
compress	Configures compression for LAPB, PPP, and HDLC encapsulations.
dialer fast-idle (interface)	Specifies the idle time before the line is disconnected.
dialer-group	Controls access by configuring an interface to belong to a specific dialing group.
dialer load-threshold	Configures bandwidth on demand by setting the maximum load before the dialer places another call to a destination.
encapsulation ppp	Enables PPP encapsulation.
ppp authentication	Enables CHAP or PAP or both, and specifies the order in which CHAP and PAP authentication is selected on the interface.

Command	Description
ppp bap timeout	Specifies nondefault timeout values for PPP BAP pending actions and responses.
ppp chap hostname	Enables a router calling a collection of routers that do not support this command to configure a common CHAP secret password to use in response to challenges from an unknown peer.
ppp multilink fragment delay	Specifies a maximum time for the transmission of a packet fragment on a MLP bundle.
ppp multilink fragment disable	Disables packet fragmentation.
ppp multilink fragmentation	Sets the maximum number of fragments a packet will be segmented into before being sent over the bundle.
ppp multilink group	Restricts a physical link to joining only a designated multilink-group interface.
ppp multilink interleave	Enables MLP interleaving.
ppp multilink mrru	Configures the MRRU value negotiated on an MLP bundle.
ppp multilink slippage	Defines the constraints that set the MLP reorder buffer size.
show ppp bap	Displays the configuration settings and run-time status for a multilink bundle.

ppp ncp override local

To track attributes received in authorization from RADIUS, verify the permitted Network Control Program (NCP), reject the current NCP negotiation, and override the local dual-stack configuration, use the **ppp ncp override local**command in global configuration mode. To disable the configuration, use the **no** form of this command.

ppp ncp override local
no ppp ncp override local

Syntax Description

This command has no arguments or keywords.

Command Default

The tracking of attributes from RADIUS and the local configuration override are not enabled. The local configuration is used.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

Framed attributes are primarily used for address allocation. The RADIUS server maintains a pool of both IPv4 addresses and IPv6 prefixes. If IPv4 address or IPv6 prefix attributes are absent in the access-accept response from RADIUS, the **ppp ncp override local** command can be used to override local configuration.

Examples

The following example shows how to override the local IPv6 or IPv4 dual-stack configuration:

```
Router> enable

Router# configure terminal
Router(config)# ppp ncp override local
```

prc-interval (IPv6)

To configure the hold-down period between partial route calculations (PRCs), use the **p rc-interval**command in address family configuration mode. To restore the default interval, use the **no** form of this command.

prc-interval *seconds* [*initial-wait*] [*secondary-wait*]
no prc-interval *seconds*

Syntax Description

seconds	Minimum amount of time between PRCs, in seconds. It can be a number in the range 1 to 120. The default is 5 seconds.
initial-wait	(Optional) Length of time before the first PRC in milliseconds.
secondary-wait	(Optional) Minimum length of time between the first and second PRC in milliseconds.

Command Default

The default is 5 seconds.

Command Modes

Address family configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.6	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **prc-interval**command is used only in multitopology Intermediate System-to-Intermediate System (IS-IS).

The **prc-interval**command controls how often Cisco IOS software can perform a PRC. Increasing the PRC interval reduces the processor load of the router, but it could slow the convergence.

This command is analogous to the **spf-interval** command, which controls the hold-down period between shortest path first (SPF) calculations.

You can use the **prc-interval** (IPv6) command only when using the IS-IS multitopology for IPv6 feature.

Examples

The following example sets the PRC calculation interval to 20 seconds:

```
Router(config)# router isis
```

```
Router(config-router)# address-family ipv6
Router(config-router-af)# prc-interval 20
```

Related Commands

Command	Description
spf-interval (IPv6)	Controls how often Cisco IOS software performs the SPF calculation.

prefix-delegation

To specify a manually configured numeric prefix to be delegated to a specified client (and optionally a specified identity association for prefix delegation [IAPD] for that client), use the **prefix-delegation** command in DHCP for IPv6 pool configuration mode. To remove the prefix, use the **no** form of this command.

prefix-delegation *ipv6-prefix/prefix-length client-DUID* [**iaid** *iaid*] [*lifetime*]
no prefix-delegation *ipv6-prefix/prefix-length client-DUID* [**iaid** *iaid*]

Syntax Description

ipv6-prefix	(Optional) Specified IPv6 prefix. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/ *prefix-length*	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address).
client-DUID	The DHCP unique identifier (DUID) of the client to which the prefix is delegated.
iaid *iaid*	(Optional) Identity association identifier (IAID), which uniquely identifies an IAPD on the client.
lifetime	(Optional) Sets a length of time over which the requesting router is allowed to use the prefix. The following values can be used: • **valid-lifetime** --The length of time, in seconds, that the prefix remains valid for the requesting router to use. • **at** --Specifies absolute points in time where the prefix is no longer valid and no longer preferred. • **infinite** --Indicates an unlimited lifetime. • **preferred-lifetime** --The length of time, in seconds, that the prefix remains preferred for the requesting router to use. • *valid-month valid-date valid-year valid-time* --A fixed duration of time for hosts to remember router advertisements. The format to be used can be **oct 24 2003 11:45** or **24 oct 2003 11:45** • *preferred-month preferred-date preferred-year preferred-time*-- A fixed duration of time for hosts to remember router advertisements. The format to be used can be **oct 24 2003 11:45** or **24 oct 2003 11:45**.

Command Default

No manually configured prefix delegations exist.

Command Modes

DHCP for IPv6 pool configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

Administrators can manually configure a list of prefixes and associated preferred and valid lifetimes for an IAPD of a specific client that is identified by its DUID. This static binding of client and prefixes can be specified based on users' subscription to an ISP using the **prefix-delegation***prefix-length* command.

The *client-DUID* argument identifies the client to which the prefix is delegated. All the configured prefixes will be assigned to the specified IAPD of the client. The IAPD to which the prefix is assigned is identified by the **iaid** argument if the **iaid** keyword is configured. If the **iaid** keyword is not configured, the prefix will be assigned to the first IAPD from the client that does not have a static binding. This function is intended to make it convenient for administrators to manually configure prefixes for a client that only sends one IAPD in case it is not easy to know the iaid in advance.

When the delegating router receives a request from a client, it checks whether there is a static binding configured for the IAPD in the client's message. If one is present, the prefixes in the binding are returned to the client. If no such binding is found, the server attempts to assign prefixes for the client from other sources.

Optionally valid and preferred lifetimes can be specified for the prefixes assigned from this pool. Users should coordinate the specified lifetimes with the lifetimes on prefixes from the upstream delegating router if the prefixes were acquired from that router.

The **lifetime**keyword can be specified in one of two ways:

- A fixed duration that stays the same in consecutive advertisements.
- Absolute expiration time in the future so that advertised lifetime decrements in real time, which will result in a lifetime of 0 at the specified time in the future.

The specified length of time is between 60 and 4294967295 seconds or infinity if the **infinite** keyword is specified.

Examples

The following example configures an IAPD for a specified client:

```
prefix-delegation 2001:0DB8::/64 00030001000BBFAA2408
```

Related Commands

Command	Description
ipv6 dhcp pool	Configures a DHCP for IPv6 pool and enters DHCP for IPv6 pool configuration mode.
ipv6 local pool	Configures a local IPv6 prefix pool.
prefix-delegation pool	Specifies a named IPv6 local prefix pool from which prefixes are delegated to DHCP for IPv6 clients.
show ipv6 dhcp pool	Displays DHCP for IPv6 configuration pool information.

prefix-delegation aaa

To specify that prefixes are to be acquired from authorization, authentication, and accounting (AAA) servers, use the **prefix-delegation aaa**command in DHCP for IPv6 pool configuration mode. To disable this feature, use the **no** form of this command.

Cisco IOS Release 12.4(22)T and Earlier Releases and Cisco IOS Release 12.2(18)SXE, Cisco IOS XE Release 2.1, and Later Releases

prefix-delegation aaa [**method-list** *method-list* [**lifetime**] {{*valid-lifetime* | **infinite**} {*valid-lifetime* | **infinite**} | **at** {*date month year time* | *month date year time*} {*date month year time* | *month date year time*}}]

no prefix-delegation aaa method-list *method-list*

Cisco IOS Release 15.0(1)M and Later Releases

prefix-delegation aaa method-list {*method-list* | **default**} [{**lifetime** {*valid-lifetime* | **infinite**} {*preferred-lifetime* | **infinite**} | **at** {*date month year time* | *month date year time*} {*date month year time* | *month date year time*}}]

no prefix-delegation aaa method-list *method-list*

Syntax Description

method-list	(Optional) Indicates a method list to be defined.
method-list	Configuration type AAA authorization method list that defines how authorization will be performed.
default	Specifies the default method list, nvgened.
lifetime	(Optional) Configures prefix lifetimes.
valid-lifetime	The length of time that the prefix remains valid for the requesting router to use, in seconds. The range is from 60 to 4294967295. The default value is 2592000 seconds.
infinite	Indicates an unlimited lifetime.
preferred-lifetime	The length of time that the prefix remains preferred for the requesting router to use, in seconds. The range is from 60 to 4294967295. The default value is 604800 seconds.
at	Specifies absolute points in time where the prefix is no longer valid and no longer preferred.
date	The date for the valid lifetime to expire.
month	The month for the valid lifetime to expire.
year	The year for the valid lifetime to expire. The range is from 2003 to 2035.
time	The year for the valid lifetime to expire.

Command Default

The default time that the prefix remains valid is 2592000 seconds, and the default time that the prefix remains preferred for the requesting router to use is 604800 seconds.

Command Modes

DHCP for IPv6 pool configuration (config-dhcpv6)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.0(1)M	This command was modified. The **default** keyword was added and the command syntax was modified to show that **lifetime** can be configured only to a **method-list**.
Cisco IOS XE Release 2.5	This command was updated. It was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

In order for the Dynamic Host Configuration Protocol (DHCP) for IPv6 server to obtain prefixes from RADIUS servers, you must also configure the AAA client and Point-to-Point Protocol (PPP) on the router. For information on how to configure the AAA client and PPP, see the "Implementing ADSL and Deploying Dial Access for IPv6" module.

Use the **aaa authorization configuration default**, **aaa group server radius**, and **radius-server host** commands to specify a named list of authorization method and RADIUS servers to contact to acquire prefixes, and then apply that named list to the **prefix-delegation aaa** command.

Valid and preferred lifetimes can be specified for the prefixes assigned from AAA servers.

The **prefix-delegation aaa** and **prefix-delegation pool** commands are mutually exclusive in a pool.

Examples

The following example shows how to specify the use of a method list named list1:

```
Router> enable
Router# configure terminal
Router(config)# ipv6 dhcp pool name
Router(config-dhcpv6)# prefix-delegation aaa method-list list1
```

Related Commands

Command	Description
aaa authorization configuration default	Downloads static route configuration information from the AAA server using TACACS+ or RADIUS.
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
prefix-delegation pool	Specifies a named IPv6 local prefix pool from which prefixes are delegated to DHCP for IPv6 clients.
radius-server host	Specifies a RADIUS server host.
sip address	Configures a SIP server IPv6 address to be returned in the SIP server's IPv6 address list option to clients.

Command	Description
sip domain-name	Configures an SIP server domain name to be returned in the SIP server's domain name list option to clients.

prefix-delegation pool

To specify a named IPv6 local prefix pool from which prefixes are delegated to Dynamic Host Configuration Protocol (DHCP) for IPv6 clients, use the **prefix-delegation pool**command in DHCP for IPv6 pool configuration mode. To remove a named IPv6 local prefix pool, use the **no** form of this command.

prefix-delegation pool *poolname* [**lifetime** *valid-lifetime preferred-lifetime*]
no prefix-delegation pool *poolname*

Syntax Description

poolname	User-defined name for the local prefix pool. The pool name can be a symbolic string (such as "Engineering") or an integer (such as 0).
lifetime	(Optional) Used to set a length of time for the hosts to remember router advertisements. If the optional **lifetime** keyword is configured, both valid and preferred lifetimes must be configured.
valid-lifetime	The amount of time that the prefix remains valid for the requesting router to use. The following values can be used: • *seconds* --The length of time, in seconds, that the prefix remains valid for the requesting router to use. The range is from 60 through 4294967295. The *preferred-lifetime* value cannot exceed the *valid-lifetime* value. • **at** --Specifies absolute points in time where the prefix is no longer valid and no longer preferred. • **infinite** --Indicates an unlimited lifetime. • *valid-month valid-date valid-year valid-time* --A fixed duration of time for hosts to remember router advertisements. The format to be used can be **oct 24 2003 11:45** or **24 oct 2003 11:45**.
preferred-lifetime	The length of time, in seconds, that the prefix remains preferred for the requesting router to use. The following values can be used: • *seconds* --The length of time, in seconds, that the prefix remains valid for the requesting router to use. The range is from 60 through 4294967295. The *preferred-lifetime* value cannot exceed the *valid-lifetime* value. • **at** --Specifies absolute points in time where the prefix is no longer valid and no longer preferred. • **infinite** --Indicates an unlimited lifetime. • *preferred-month preferred-date preferred-year preferred-time*-- A fixed duration of time for hosts to remember router advertisements. The format to be used can be **oct 24 2003 11:45** or **24 oct 2003 11:45**

Command Default

No IPv6 local prefix pool is specified. Valid lifetime is 2592000 seconds (30 days). Preferred lifetime is 604800 seconds (7 days).

Command Modes

DHCP for IPv6 pool configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

The **prefix-delegation pool**command specifies a named IPv6 local prefix pool from which prefixes are delegated to clients. Use the **ipv6 local pool** command to configure the named IPv6 prefix pool.

Optionally, valid and preferred lifetimes can be specified for the prefixes assigned from this pool. Users should coordinate the specified lifetimes with the lifetimes on prefixes from the upstream delegating router if the prefixes were acquired from that router.

The **lifetime**keyword can be specified in one of two ways:

- A fixed duration that stays the same in consecutive advertisements.
- Absolute expiration time in the future so that advertised lifetime decrements in real time, which will result in a lifetime of 0 at the specified time in the future.

The specified length of time is from 60 to 4,294,967,295 seconds or infinity if the **infinite** keyword is specified.

The Cisco IOS DHCP for IPv6 server can assign prefixes dynamically from an IPv6 local prefix pool, which is configured using the **ipv6 local pool** command and associated with a DHCP for IPv6 configuration pool using the **prefix-delegation pool** command. When the server receives a prefix request from a client, it attempts to obtain unassigned prefixes, if any, from the pool.

After the client releases the previously assigned prefixes, the server will return the prefixes to the pool for reassignment to other clients.

Examples

The following example specifies that prefix requests should be satisfied from the pool called client-prefix-pool. The prefixes should be delegated with the valid lifetime set to 1800 seconds, and the preferred lifetime is set to 600 seconds:

```
prefix-delegation pool client-prefix-pool lifetime 1800 600
```

Related Commands

Command	Description
ipv6 dhcp pool	Configures a DHCP for IPv6 pool and enters DHCP for IPv6 pool configuration mode.
ipv6 local pool	Configures a local IPv6 prefix pool.
prefix-delegation	Specifies a manually configured numeric prefix that is to be delegated to a particular client's IAPD.
show ipv6 dhcp pool	Displays DHCP for IPv6 configuration pool information.

prefix-glean

To enable the device to glean prefixes from IPv6 router advertisements (RAs) or Dynamic Host Configuration Protocol (DHCP), use the **prefix-glean** command in IPv6 snooping configuration mode. To learn only prefixes gleaned in one of these protocols and exclude the other, use the **no** form of this command.

prefix-glean [**only**]
no prefix-glean [**only**]

Syntax Description

only	(Optional) Only prefixes are gleaned. Host addresses are not gleaned.

Command Default

Prefixes are not learned through RA or DHCP.

Command Modes

IPv6 snooping configuration (config-ipv6-snooping)

Command History

Release	Modification
15.0(2)SE	This command was introduced.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **prefix-glean** command enables the device to learn prefixes in RA and DHCP traffic.

Examples

The following example shows how to enable the device to learn prefixes:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# prefix-glean
```

Related Commands

Command	Description
ipv6 snooping attach-policy	Applies an IPv6 snooping policy to a target.
ipv6 snooping policy	Configures an IPv6 snooping policy and enters IPv6 snooping configuration mode.

protocol (IPv6)

To specify that addresses should be gleaned with Dynamic Host Configuration Protocol (DHCP) or Neighbor Discovery Protocol (NDP) or to associate the protocol with an IPv6 prefix list, use the **protocol** command. To disable address gleaning with DHCP or NDP, use the **no** form of the command.

protocol {**dhcp** | **ndp**} [{**prefix-list** *prefix-list-name*}]
no protocol {**dhcp** | **ndp**}

Syntax Description

dhcp	Specifies that addresses should be gleaned in Dynamic Host Configuration Protocol (DHCP) packets.
ndp	Specifies that addresses should be gleaned in Neighbor Discovery Protocol (NDP) packets.
prefix-list *prefix-list-name*	(Optional) Specifies that a prefix list of protected prefixes be used.

Command Default

Snooping and recovery are attempted using both DHCP and NDP. No prefix list is used, all address ranges are accepted.

Command Modes

IPv6 snooping configuration (config-ipv6-snooping)

Command History

Release	Modification
15.2(4)S	This command was introduced.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

If an address does not match the prefix list associated with DHCP or NDP, then control packets will be dropped and recovery of the binding table entry will not be attempted with that protocol.

- If a prefix list is specified, the prefix list applies to all flows for the specified protocol.
- If there is no prefix list specified, all protocols are supported by default. There is no check and all addresses are accepted.
- Using the **no protocol** {**dhcp** | **ndp**} command indicates that a protocol will not to be used for snooping or gleaning.
- However, if the **no protocol dhcp** command is used, DHCP can still be used for binding table recovery.
- The NDP prefix list should be a superset of the DHCP prefix list, as addresses obtained by DHCP must be confirmed by NDP later.
- When a prefix list is given and a protocol packet indicates an address that does not match the prefix list for that protocol, the packet is dropped (unless the security level is “glean”).

  This means that if the security level is "glean" all packets are gleaned - without checking the prefix-list. If the security level is "guard", then packets are checked againt the policy-configured prefix-list, to allow or deny it.

- Data glean can recover with DHCP and NDP, though destination guard will only recovery through DHCP.

Note Before you configure the **protocol** command, it is essential that you provide a value for the **ge** *ge-value* option when configuring a prefix list using the **ipv6 prefix-list** command.

Examples

The following example shows a valid configuration for an IPv6 prefix list ("abc") and shows that DHCP will be used to recover addresses that match the prefix list abc:

```
Device(config)# ipv6 prefix-list abc seq 5 permit 2001:DB8::/64 ge 128
!
Device(config-ipv6-snooping)# protocol dhcp prefix-list abc
```

Related Commands

Command	Description
ipv6 prefix-list	Creates an entry in an IPv6 prefix list.
ipv6 snooping policy	Enters IPv6 snooping configuration mode.

protocol ipv6 (ATM)

To map the IPv6 address of a remote node to the ATM permanent virtual circuit (PVC) used to reach the address, use the **protocol ipv6**command in ATM VC configuration mode. To remove the static map, use the **no** form of this command.

protocol ipv6 *ipv6-address* [[**no**] **broadcast**]
no protocol ipv6 *ipv6-address* [[**no**] **broadcast**]

Syntax Description

ipv6-address	Destination IPv6 (protocol) address that is being mapped to a PVC . This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
no broadcast	(Optional) Indicates whether the map entry should be used when IPv6 multicast packets (not broadcast packets) are sent to the interface. Pseudobroadcasting is supported. The [**no**] **broadcast** keywords in the **protocol ipv6** command take precedence over the **broadcast** command configured on the same ATM PVC.

Command Default

No mapping is defined.

Command Modes

ATM VC configuration (for an ATM PVC)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Examples

In the following example, two nodes named Cisco 1 and Cisco 2 are connected by a single PVC. The point-to-point subinterface ATM0.132 is used on both nodes to terminate the PVC; therefore, the mapping between the IPv6 addresses of both nodes and the PVC is implicit (no additional mappings are required).

Cisco 1 Configuration

```
interface ATM0
```

```
 no ip address
!
interface ATM0.132 point-to-point
 pvc 1/32
  encapsulation aal5snap
 !
 ipv6 address 2001:0DB8:2222::72/32
```

Cisco 2 Configuration

```
interface ATM0
 no ip address
!
interface ATM0.132 point-to-point
 pvc 1/32
  encapsulation aal5snap
 !
 ipv6 address 2001:0DB8:2222::45/32
```

In the following example, the same two nodes (Cisco 1 and Cisco 2) from the previous example are connected by the same PVC. In this example, however, the point-to-multipoint interface ATM0 is used on both nodes to terminate the PVC; therefore, explicit mappings are required between the link-local and global IPv6 addresses of interface ATM0 on both nodes and the PVC. Additionally, ATM pseudobroadcasts are enabled on the link-local address of interface ATM0 on both nodes.

Cisco 1 Configuration

```
interface ATM0
 no ip address
 pvc 1/32
  protocol ipv6 2001:0DB8:2222::45
  protocol ipv6 FE80::60:2FA4:8291:2 broadcast
  encapsulation aal5snap
 !
 ipv6 address 2001:0DB8:2222::72/32
```

Cisco 2 Configuration

```
interface ATM0
 no ip address
 pvc 1/32
  protocol ipv6 FE80::60:3E47:AC8:C broadcast
  protocol ipv6 2001:0DB8:2222::72
  encapsulation aal5snap
 !
 ipv6 address 2001:0DB8:2222::45/32
```

Related Commands

Command	Description
show atm map	Displays the list of all configured ATM static maps to remote hosts on an ATM network and on ATM bundle maps.

queue-depth (OSPFv3)

To configure the number of incoming packets that the IPv4 Open Shortest Path First version 3 (OSPFv3) process can keep in its queue, use the **queue-depth** command in OSPFv3 router configuration mode. To set the queue depth to its default value, use the **no** form of the command.

queue-depth {**hello** | **update**} {*queue-size* | **unlimited**}
no queue-depth {**hello** | **update**}

Syntax Description

hello	Specifies the queue depth of the OSPFv3 hello process.
update	Specifies the queue depth of the OSPFv3 router process queue.
queue-size	Maximum number of packets in the queue. The range is 1 to 2147483647.
unlimited	Specifies an infinite queue depth.

Command Default

If you do not set a queue size, the OSPFv3 hello process queue depth is unlimited and the OSPFv3 router process (update) queue depth is 200 packets.

Command Modes

OSPFv3 router configuration mode (config-router)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

All incoming OSPFv3 packets are initially enqueued in the hello queue. OSPFv3 hello packets are processed directly from this queue, while all other OSPFv3 packet types are subsequently enqueued in the update queue.

If you configure a router with many neighbors and a large database, use the **queue-depth** command to adjust the size of the hello and router queues. Otherwise, packets might be dropped because of queue limits, and OSPFv3 adjacencies may be lost.

Examples

The following example shows how to configure the OSPFv3 update queue to 1500 packets:

```
Router(config)# router ospfv3 1
Router(config-router)# queue-depth update 1500
```

Related Commands

Command	Description
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

redistribute (IPv6)

To redistribute IPv6 routes from one routing domain into another routing domain, use the **redistribute** command in address family configuration or router configuration mode. To disable redistribution, use the **no** form of this command.

redistribute source-protocol [*process-id*] [**include-connected** {**level-1** | **level-1-2** | **level-2**}] [*as-number*] [**metric** {*metric-value* | **transparent**}] [**metric-type** *type-value*] [**match** {**external** [{**1** | **2**}] | **internal** | **nssa-external** [{**1** | **2**}]}] [**tag** *tag-value*] [**route-map** *map-tag*]
no redistribute source-protocol [*process-id*] [**include-connected**] {**level-1** | **level-1-2** | **level-2**} [*as-number*] [**metric** {*metric-value* | **transparent**}] [**metric-type** *type-value*] [**match** {**external** [{**1** | **2**}] | **internal** | **nssa-external** [{**1** | **2**}]}] [**tag** *tag-value*] [**route-map** *map-tag*]

Syntax Description

source-protocol	Source protocol from which routes are being redistributed. It can be one of the following keywords: **bgp**, connected, **eigrp**, **isis**, **ospf**, **rip**, or **static**.
process-id	(Optional) For the **bgp** or **eigrp**keyword, the process ID is a Border Gateway Protocol (BGP) autonomous system number, which is a 16-bit decimal number. For the **isis**keyword, the process ID is an optional value that defines a meaningful name for a routing process. You can specify only one IS-IS process per router. Creating a name for a routing process means that you use names when configuring routing. For the **ospf** keyword, the process ID is the number assigned administratively when the Open Shortest Path First (OSPF) for IPv6 routing process is enabled. For the **rip**keyword, the process ID is an optional value that defines a meaningful name for an IPv6 Routing Information Protocol (RIP) routing process.
include-connected	(Optional) Allows the target protocol to redistribute routes learned by the source protocol and connected prefixes on those interfaces over which the source protocol is running.
level-1	Specifies that, for Intermediate System-to-Intermediate System (IS-IS), Level 1 routes are redistributed into other IP routing protocols independently.
level-1-2	Specifies that, for IS-IS, both Level 1 and Level 2 routes are redistributed into other IP routing protocols.
level-2	Specifies that, for IS-IS, Level 2 routes are redistributed into other IP routing protocols independently.
as-number	(Optional) Autonomous system number for the redistributed route.
metric *metric-value*	(Optional) When redistributing from one OSPF process to another OSPF process on the same router, the metric will be carried through from one process to the other if no metric value is specified. When redistributing other processes to an OSPF process, the default metric is 20 when no metric value is specified.
metric transparent	(Optional) Causes RIP to use the routing table metric for redistributed routes as the RIP metric.

metric-type *type-value*	(Optional) For OSPF, specifies the external link type associated with the default route advertised into the OSPF routing domain. It can be one of two values: • **1**—Type 1 external route • **2**—Type 2 external route If no value is specified for the **metric-type** keyword, the Cisco IOS software adopts a Type 2 external route. For IS-IS, the link type can be one of two values: • **internal**—IS-IS metric that is < 63. • **external**—IS-IS metric that is > 64 < 128. • **rib-metric-as-external**—Sets metric type to external and uses the RIB metric. • **rib-metric-as-internal**—Sets metric type to internal and uses the RIB metric. The default is **internal**.
match {**external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**]	(Optional) For OSPF, routes are redistributed into other routing domains using the match keyword. It is used with one of the following: • **external** [**1** | **2**] —Routes that are external to the autonomous system, but are imported into OSPF as Type 1 or Type 2 external routes. • **internal** —Routes that are internal to a specific autonomous system. • **nssa-external** [**1**| **2**]—Routes that are external to the autonomous system but are imported into OSPF, in a not so stubby area (NSSA), for IPv6 as Type 1 or Type 2 external routes.
tag *tag-value*	(Optional) Specifies the 32-bit decimal value attached to each external route. This is not used by OSPF itself. It may be used to communicate information between Autonomous System Boundary Routers (ASBRs). If none is specified, then the remote autonomous system number is used for routes from BGP and Exterior Gateway Protocol (EGP); for other protocols, zero (0) is used.
route-map	(Optional) Specifies the route map that should be checked to filter the importation of routes from this source routing protocol to the current routing protocol. If the route-map keyword is not specified, all routes are redistributed. If this keyword is specified, but no route map tags are listed, no routes will be imported.
map-tag	(Optional) Identifier of a configured route map.

Command Default

Route redistribution is disabled.

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.4(6)T	Support for Enhanced Internal Gateway Routing Protocol (EIGRP) IPv6 was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.
Cisco IOS XE Release 3.15S	This command was modified. The **rib-metric-as-external** and **rib-metric-as-internal** keywords were added.

Usage Guidelines

Changing or disabling any keyword will not affect the state of other keywords.

A router receiving an IPv6 IS-IS route with an internal metric will consider the cost of the route from itself to the redistributing router plus the advertised cost to reach the destination. An external metric considers only the advertised metric to reach the destination.

IS-IS will ignore any configured redistribution of routes configured with the **include-connected** keyword. IS-IS will advertise a prefix on an interface if either IS-IS is running over the interface or the interface is configured as passive.

Routes learned from IPv6 routing protocols can be redistributed into IPv6 IS-IS at Level 1 into an attached area or at Level 2. The **level-1-2** keyword allows both Level 1 and Level 2 routes in a single command.

For IPv6 RIP, use the **redistribute** command to advertise static routes as if they were directly connected routes.

Caution Advertising static routes as directly connected routes can cause routing loops if improperly configured.

Redistributed IPv6 RIP routing information should always be filtered by the **distribute-list prefix-list** router configuration command. Use of the **distribute-list prefix-list** command ensures that only those routes intended by the administrator are passed along to the receiving routing protocol.

Note The **metric** value specified in the **redistribute** command for IPv6 RIP supersedes the **metric** value specified using the **default-metric** command.

Note In IPv4, if you redistribute a protocol, by default you also redistribute the subnet on the interfaces over which the protocol is running. In IPv6 this is not the default behavior. To redistribute the subnet on the interfaces over which the protocol is running in IPv6, use the include-connected keyword. In IPv6 this functionality is not supported when the source protocol is BGP.

When the **no redistribute** command is configured, the parameter settings are ignored when the client protocol is IS-IS or EIGRP.

IS-IS redistribution will be removed completely when IS-IS level 1 and level 2 are removed by the user. IS-IS level settings can be configured using the redistribute command only.

The default redistribute type will be restored to OSPF when all route type values are removed by the user.

Examples

The following example configures IPv6 IS-IS to redistribute IPv6 BGP routes. The metric is specified as 5, and the metric type will be set to external, indicating that it has lower priority than internal metrics.

```
Router(config)# router isis
Router(config-router)# address-family ipv6
Router(config-router-af)# redistribute bgp 64500 metric 5 metric-type external
```

The following example redistributes IPv6 BGP routes into the IPv6 RIP routing process named cisco:

```
Router(config)# ipv6 router rip cisco
Router(config-router)# redistribute bgp 42
```

The following example redistributes IS-IS for IPv6 routes into the OSPF for IPv6 routing process 1:

```
Router(config)# ipv6 router ospf 1
Router(config-router)# redistribute isis 1 metric 32 metric-type 1 tag 85
```

In the following example, ospf 1 redistributes the prefixes 2001:1:1::/64 and 2001:99:1::/64 and any prefixes learned through rip 1:

```
interface ethernet0/0
 ipv6 address 2001:1:1::90/64
 ipv6 rip 1 enable
interface ethernet1/1
 ipv6 address 2001:99:1::90/64
 ipv6 rip 1 enable
interface ethernet2/0
 ipv6 address 2001:1:2::90/64
 ipv6 ospf 1 area 1
ipv6 router ospf 1
  redistribute rip 1 include-connected
```

The following configuration example and output show the no redistribute command parameters when the last route type value is removed:

```
Router(config-router)# redistribute rip process1 metric 7
Router(config-router)# do show run | include redistribute
 redistribute rip process1 metric 7
Router(config-router)# no redistribute rip process1 metric 7
```

```
Router(config-router)# do show run | include redistribute
 redistribute rip process1
Router(config-router)#
```

Related Commands

Command	Description
default-metric	Specifies a default metric for redistributed routes.
distribute-list prefix-list (IPv6 EIGRP)	Applies a prefix list to EIGRP for IPv6 routing updates that are received or sent on an interface.
distribute-list prefix-list (IPv6 RIP)	Applies a prefix list to IPv6 RIP routing updates that are received or sent on an interface.
redistribute isis (IPv6)	Redistributes IPv6 routes from one routing domain into another routing domain using IS-IS as both the target and source protocol.

redistribute (OSPFv3)

To redistribute IPv6 and IPv4 routes from one routing domain into another routing domain, use the **redistribute** command in IPv6 or IPv4 address family configuration mode. To disable redistribution, use the **no** form of this command.

redistribute source-protocol [*process-id*] [*options*]
no redistribute source-protocol [*process-id*] [*options*]

Syntax Description

source-protocol	Source protocol from which routes are being redistributed. It can be one of the following keywords: **bgp**, connected, **eigrp**, **isis**, **nd**, **nemo**, **ospfv3**, **ospf**, **rip**, or **static**.
process-id	(Optional) For the **bgp** or **eigrp** keyword, the process ID is a Border Gateway Protocol (BGP) autonomous system number, which is a 16-bit decimal number. For the **isis** keyword, the process ID is an optional value that defines a meaningful name for a routing process. You can specify only one IS-IS process per router. Creating a name for a routing process means that you use names when configuring routing. For the **ospfv3** keyword, the process ID is the number assigned administratively when the Open Shortest Path First version 3 (OSPFv3) routing process is enabled. For the **rip** keyword, the process ID is an optional value that defines a meaningful name for an IPv6 Routing Information Protocol (RIP) routing process.
options	(Optional) The range of available options depends on the protocol. In OSPFv3, it includes the **nssa-only** keyword, which you can use to restrict external distributions to the not-so-stubby area (NSSA).

Command Default

Default redistribute type is OSPFv3.

Command Modes

IPv6 address family configuration (config-router-af)
IPv4 address family configuration (config-router-af)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.2(4)S	This command was modified. The **nssa-only** keyword was added.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Changing or disabling any keyword will not affect the state of other keywords.

For the IPv6 address family (AF), the **ospf** option refers to an OSPFv3 process. For the IPv4 address family, the **ospfv3** option specifies an OSPFv3 process, and the **ospf** option refers to an OSPFv2 process.

A router receiving an IPv6 IS-IS route with an internal metric will consider the cost of the route from itself to the redistributing router plus the advertised cost to reach the destination. An external metric considers only the advertised metric to reach the destination.

IS-IS will ignore any configured redistribution of routes configured with the include-connected keyword. IS-IS will advertise a prefix on an interface if either IS-IS is running over the interface or the interface is configured as passive.

Routes learned from IPv6 routing protocols can be redistributed into IPv6 IS-IS at Level 1 into an attached area or at Level 2. The **level-1-2** keyword allows both Level 1 and Level 2 routes in a single command.

For IPv6 RIP, use the **redistribute**command to advertise static routes as if they were directly connected routes.

Caution Advertising static routes as directly connected routes can cause routing loops if improperly configured.

Redistributed IPv6 RIP routing information should always be filtered by the **distribute-list prefix-list**router configuration command. Use of the **distribute-list prefix-list**command ensures that only those routes intended by the administrator are passed along to the receiving routing protocol.

Note The **metric** value specified in the **redistribute** command for IPv6 RIP supersedes the **metric** value specified using the **default-metric** command.

Note In IPv4, if you redistribute a protocol, by default you also redistribute the subnet on the interfaces over which the protocol is running. In IPv6, this is not the default behavior. To redistribute the subnet on the interfaces over which the protocol is running in IPv6, use the include-connected keyword. In IPv6, this functionality is not supported when the source protocol is BGP.

When the no redistribute command is configured, the parameter settings are ignored when the client protocol is IS-IS or EIGRP.

IS-IS redistribution will be removed completely when IS-IS level 1 and level 2 are removed by the user. IS-IS level settings can be configured using the redistribute command only.

The default redistribute type will be restored to OSPFv3 when all route type values are removed by the user.

Specify the **nssa-only** keyword to clear the propagate bit (P-bit) when external routes are redistributed into a NSSA. Doing so prevents corresponding NSSA external link state advertisements (LSAs) being translated into other areas.

Related Commands

Command	Description
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

redistribute isis (IPv6)

To redistribute IPv6 routes from one routing domain into another routing domain using Intermediate System-to-Intermediate System (IS-IS) as both the target and source protocol, use the **redistribute isis** command in address family configuration mode. To disable redistribution, use the **no** form of this command.

redistribute isis [*process-id*] {**level-1** | **level-2**} **into** {**level-1** | **level-2**} {**distribute-list** *list-name* | **route-map** *map-tag*}
no redistribute isis [*process-id*] {**level-1** | **level-2**} **into** {**level-1** | **level-2**} {**distribute-list** *list-name* | **route-map***map-tag*}

Syntax Description

process-id	(Optional) A *tag* value that defines a meaningful name for a routing process. You can specify only one IS-IS process per router. Creating a name for a routing process means that you use names when configuring routing.
level-1	Specifies that IS-IS Level 1 routes are redistributed into other IP routing protocols independently.
level-2	Specifies that IS-IS Level 2 routes are redistributed into other IP routing protocols independently.
into	Distributes IS-IS Level 1 or Level 2 routes into Level 1 or Level 2 in another IS-IS instance.
distribute-list	Specifies the distribute list used for the redistributed route.
list-name	Specifies the name of the distribute list for the redistributed route.
route-map *map-tag*	(Optional) Specifies the name of a route map that controls the IS-IS redistribution. You can specify either a distribute list or a route map, but not both.

Command Default

Route redistribution is disabled. No process ID is defined.

Command Modes

Address family configuration (config-router-af)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
Cisco IOS XE Release 2.4	This command was introduced on Cisco ASR 1000 Aggregation Services Routers.
Cisco IOS XE Release 3.6S	This command was modified. Support for the **route-map** keyword was introduced.

Usage Guidelines

Changing or disabling any keyword will not affect the state of other keywords.

A router receiving an IPv6 IS-IS route with an internal metric will consider the cost of the route from itself to the redistributing router plus the advertised cost to reach the destination. An external metric considers only the advertised metric to reach the destination.

IS-IS will ignore any configured redistribution of routes configured with the connected keyword. IS-IS will advertise a prefix on an interface if either IS-IS is running over the interface or the interface is configured as passive.

Routes learned from IPv6 routing protocols can be redistributed into IPv6 IS-IS at Level 1 into an attached area or at Level 2. The **level-1-2** keyword allows both Level 1 and Level 2 routes in a single command.

Examples

The following example shows how to redistribute only Level-1 routes with tag 100 to Level 2:

```
router isis
address-family ipv6
redistribute isis level-1 into level-2 route-map match-tag
route-map match-tag
match tag 100
```

Related Commands

Command	Description
default-metric	Specifies a default metric for redistributed routes.
ipv6 route priority high	Assigns a high priority to an IS-IS IPv6 prefix.
isis ipv6 tag	Configures an administrative tag value that will be associated with an IPv6 address prefix and applied to an IS-IS LSP.
metric-style wide	Configures a router running IS-IS so that it generates and accepts only new-style type, length, and value.
redistribute (IPv6)	Redistributes IPv6 routes from one routing domain into another routing domain.
show isis database verbose	Displays details about the IS-IS link-state database, including the route tag.
summary-prefix (IPv6 IS-IS)	Creates aggregate IPv6 prefixes for IS-IS.

register (mobile router)

To con trol the registration parameters of the IPv6 mobile router, use the **register** command in mobile router configuration mode or IPv6 mobile router configuration mode. To return the registration parameters to their default settings, use the **no** form of this command.

register {**extend expire** *seconds* **retry** *number* **interval** *seconds* | **lifetime** *seconds* | **retransmit initial milliseconds maximum milliseconds retry number**}
no register {**extend expire** *seconds* **retry** *number* **interval** *seconds* | **lifetime** *seconds* | **retransmit initial milliseconds maximum milliseconds retry number**}

Syntax Description

extend	Reregisters before the lifetime expires.
expire *seconds*	Specifies the time (in seconds) in which to send a registration request before expiration. In IPv4, the range is from 1 to 3600; the default is 120. In IPv6, the range is from 1 to 600.
retry *number*	Specifies the number of times the mobile router retries sending a registration request if no reply is received. In both IPv4 and IPv6, the range is from 0 to 10; the default is 3. A value of 0 means no retry. The mobile router stops sending registration requests after the maximum number of retries is attempted.
interval *seconds*	Specifies the time (in seconds) that the mobile router waits before sending another registration request if no reply is received. In IPv4, the range is from 1 to 3600; the default is 10. In IPv6, the range is from 1 to 60.
lifetime *seconds*	Specifies the requested lifetime (in seconds) of each registration. The shortest value between the configured lifetime and the foreign agent advertised registration lifetime is used. In IPv4, the range is from 3 to 65534; the default is 65534 (infinity). In IPv6, the range is from 4 to 262143; the default is 262143 (infinity). This default ensures that the advertised lifetime is used, excluding infinity.
retransmit initial *milliseconds*	Specifies the wait period (in milliseconds) before sending a retransmission the first time no reply is received from the foreign agent. In IPv4, the range is from 10 to 10000 milliseconds (10 seconds); the default is 1000 milliseconds (1 second). In IPv6, the range is from 1000 to 256000.
maximum *milliseconds* **retry** *number*	Specifies the maximum wait period (in milliseconds) before retransmission of a registration request. In IPv4, the range is 10 to 10000 (10 seconds); the default is 5000 milliseconds (5 seconds). In IPv6, the maximum range is from 1000 to 256000. In IPv6, the retry number range is from 0 to 10. Each successive retransmission timeout period is twice the previous period, if the previous period was less than the maximum value. Retransmission stops after the maximum number of retries.

Command Default

The registration parameters of the IPv6 mobile router are used.

Command Modes

Mobile router configuration
IPv6 mobile router configuration (IPv6-mobile-router)

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.4(20)T	Support for IPv6 was added.

Usage Guidelines

The **register lifetime***seconds*command configures the lifetime that the mobile router requests in a registration request. The home agent also has lifetimes that are set. If the registration request from a mobile router has a greater lifetime than the registration reply from the home agent, the lifetime set on the home agent will be used for the registration. If the registration request lifetime from the mobile router is less than the registration reply from the home agent, the lifetime set on the mobile router will be used. Thus, the smaller lifetime between the home agent and mobile router is used for registration.

Examples

The following example specifies a registration lifetime of 600 seconds:

```
ip mobile router
 address 10.1.1.10 255.255.255.0
 home-agent 10.1.1.20
 register lifetime 600
```

Related Commands

Command	Description
ipv6 mobile router	Enables IPv6 NEMO functionality on the router and places the router in IPv6 mobile router mode.
show ip mobile router	Displays configuration information and monitoring statistics about the mobile router.
show ip mobile router registration	Displays the pending and accepted registrations of the mobile router.

remark (IPv6)

To write a helpful comment (remark) for an entry in an IPv6 access list, use the **remark**command in IPv6 access list configuration mode. To remove the remark, use the **no** form of this command.

remark *text-string*
no remark *text-string*

Syntax Description

text-string	Comment that describes the access list entry, up to 100 characters long.

Command Default

IPv6 access list entries have no remarks.

Command Modes

IPv6 access list configuration

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **remark** (IPv6) command is similar to the **remark** (IP) command, except that it is IPv6-specific.

The remark can be up to 100 characters long; anything longer is truncated.

Examples

The following example configures a remark for the IPv6 access list named TELNETTING. The remark is specific to not letting the Marketing subnet use outbound Telnet.

```
ipv6 access-list TELNETTING
 remark Do not allow Marketing subnet to telnet out
 deny tcp 2001:0DB8:0300:0201::/64 any eq telnet
```

Related Commands

Command	Description
ipv6 access-list	Defines an IPv6 access list and enters IPv6 access list configuration mode.
show ipv6 access-list	Displays the contents of all current IPv6 access lists.